UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

WALBER JOSÉ ADRIANO SILVA

INVESTIGAÇÃO EMPÍRICA SOBRE A PERCEPÇÃO DA SEGURANÇA DA INFORMAÇÃO PELOS USUÁRIOS DE UMA UNIVERSIDADE PÚBLICA BASEADA NA ANÁLISE FATORIAL EXPLORATÓRIA

João Pessoa
2011

WALBER JOSÉ ADRIANO SILVA

INVESTIGAÇÃO EMPÍRICA SOBRE A PERCEPÇÃO DA SEGURANÇA DA INFORMAÇÃO PELOS USUÁRIOS DE UMA UNIVERSIDADE PÚBLICA BASEADA NA ANÁLISE FATORIAL EXPLORATÓRIA

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Universidade Federal da Paraíba para obtenção do título de Mestre em Informática.

Área de concentração: Computação distribuída

Orientador:

Prof. Dr. Gustavo Henrique Matos Bezerra Motta

Co-Orientador:

Prof. Dr. Lucídio dos Anjos Formiga Cabral

João Pessoa

2011

Agradecimentos

Agradeço a Deus pelo amor incondicional e meu refúgio nos momentos mais difíceis de minha vida.

Aos meus pais, Socorro e Leandro, e ao meu irmão Thiago, que acreditaram e tornaram possível a oportunidade da educação.

Ao professor e amigo Gustavo Henrique Matos Bezerra Motta pelos conhecimentos, paciência, compreensão e conselhos sábios durante a minha graduação e pós-graduação.

Ao Programa de Pós-Graduação em Informática pelo esforço na formação de mestres na área.

Ao corpo de funcionários do CERES-UFRN pela atenção e compreensão durante minha participação no curso do PPGI.

A minha colega de trabalho Idelmárcia Dantas, pela contribuição na elaboração e validação do questionário.

Ao meu colega de trabalho Francisco Anderson Freire Pereira pela ajuda na divulgação do Convite de divulgação do questionário *on-line* no CERES.

Agradeço aos professores, alunos e técnicos administrativos que de boa vontade se dispuseram a responder ao questionário da pesquisa.

À Mary Campêlo de Oliveira pelo companheirismo e amor na minha nova fase da vida.

À colega de trabalho Maria de Fátima Lucimara Santos Nobrega pela assistência e atenção.

À direção do CERES pela oportunidade de conciliar as atividades do mestrado e o trabalho.

À professora Célia Maria de Medeiros pelas valiosas informações na elaboração na escrita da dissertação, através do curso “Língua Portuguesa como apoio à pesquisa: questões que orientam a produção textual de gêneros acadêmicos”.

Ao médico e amigo Laercio Bragante de Araújo pelo incentivo aos estudos.

Ao ex-colega e amigo Gustavo Cavalcanti por ensinar a grande vontade de viver (in memoriam).

Aos meus avôs e avó materna (in memoriam).

Agradeço ainda a todos que generosamente contribuíram com tempo e atenção durante as etapas dessa dissertação.

Seja você quem for, seja qual for à posição social que você tenha na vida, a mais alta ou a mais baixa, tenha sempre como meta muita força, muita determinação e sempre faça tudo com muito amor e com muita fé em Deus, que um dia você chega lá. De alguma maneira você chega lá.

Ayrton Senna da Silva

Resumo

SILVA, W. J. A. INVESTIGAÇÃO EMPÍRICA SOBRE PERCEPÇÃO DA SEGURANÇA DA INFORMAÇÃO PELOS USUÁRIOS DE UMA UNIVERSIDADE PÚBLICA BASEADA NA ANÁLISE FATORIAL EXPLORATÓRIA. 2011. 178 p. Dissertação (Mestrado) – Programa de Pós-Graduação em Informática, Departamento de Informática, Universidade Federal da Paraíba, João Pessoa, 2011.

O presente trabalho sobre segurança da informação no âmbito acadêmico objetiva analisar a percepção dos usuários da infraestrutura de TI de uma universidade pública sobre os fatores que envolvem a segurança da informação. Através de um questionário quantitativo on-line, exploram-se oito fatores relativos à segurança da informação, que foram retirados da literatura revisada, com especial atenção para os trabalhos qualitativos na área. São eles: 1. Apoio da administração; 2. Atribuição de responsabilidade; 3. Ambiente de liberdade acadêmica; 4. Cultura da segurança; 5. Prioridade da segurança; 6. Participação nas atividades de segurança; 7. Programas de conscientização; 8. Comunicação. Após a coleta de dados, total de 122 casos, o método de análise fatorial exploratória foi aplicado buscando aceitar ou rejeitar as hipóteses do trabalho. O trabalho estendeu outras pesquisas sobre segurança da informação e indica que o apoio da administração é o fator mais importante para explicar a percepção da segurança da informação num ambiente universitário público. Políticas de segurança da informação neste tipo de organização devem levar este fator em consideração durante a sua elaboração.

Palavras-chave: política de segurança, universidades públicas, usuários, análise fatorial exploratória.

Abstract

SILVA, W. J. A. EMPIRICAL RESEARCH ON PERCEPTION OF INFORMATION SECURITY FOR USERS OF A PUBLIC UNIVERSITY BASED ON EXPLORATORY FACTORIAL ANALYSIS. 2011. 178 p. Dissertation (Masters) – Programa de Pós-Graduação em Informática, Departamento de Informática, Universidade Federal da Paraíba, João Pessoa, 2010.

The present work on information security in the academic area, aims to analyze the users' perception of IT infrastructure of a public university on the factors involved in information security. Through a quantitative questionnaire online, eight factors related to information security were explored, which were taken from the literature reviewed, with special attention to the qualitative work in the area. They are: 1. Administration's support; 2. Assignment of responsibility;3. Environment of academic freedom; 4. Safety culture; 5. Priority of security; 6. Participation in safety activities; 7. Awareness programs; 8. Communication. After collecting data, total of 122 cases, the method of exploratory factor analysis for multivariate analysis of data was applied to accept or reject the hypothesis of the work. The work has extended other research on information security and indicates that the administration's support is the most important factor to explain the perception of information security in a public university environment. Information security policies in this organization should take this factor into account during its preparation.

Keywords: Security policies, public universities, users, exploratory factor analyze.

Lista de ilustrações

Lista de gráficos

Lista de equações

Lista de tabelas

Lista de abreviaturas e siglas

ABNT: Associação Brasileira de Normas Técnicas;

AF: Análise fatorial;

AFE: Análise fatorial exploratória;

CERES: Centro de Ensino Superior do Seridó;

KMO: Kaiser-Meyer-Olkin;

MSA: Measure of Sampling Adequacy;

PHP: Hypertext Preprocessor;

SPSS: Statistical Package for the Social Sciences;

TI: Tecnologia da Informação;

TIC: Tecnologia da Informação e Comunicação;

RH: Recursos Humanos;

UFRN: Universidade Federal do Rio Grande do Norte.

Sumário

Capítulo

1

Introdução

"Não quero ser um gênio, já tenho problemas suficientes ao tentar ser um homem."

Albert Einstein

É evidente a necessidade de segurança da informação nos dias atuais. São crescentes as ameaças à segurança, como indicado pelos índices de incidentes reportados pelas organizações (REDE NACIONAL DE ENSINO E PESQUISA, 2010). Estas não estão livres de terem sua infraestrutura de rede e de computadores comprometidas ou exploradas.

É fato comum encontrar a segurança da informação tendo sua atenção maior na adoção de novos hardwares e softwares. Esta visão puramente técnica revela sua fragilidade quando se analisam os resultados das perdas provenientes de falhas na segurança da informação (WHITMAN, 2003). Hoje, sabe-se que o sucesso da segurança da informação é proveniente do apoio da alta gerência (MACHADO, 2008) e de uma abordagem sócio-organizacional (ALBRECHTSEN, 2007).

Neste cenário, surgem as normas internacionais de segurança, guias que estabelecem um conjunto de diretrizes, controles[1] e boas práticas a serem seguidas. As normas foram escritas e direcionadas para as organizações alcançarem uma melhor gestão da segurança da informação, através da adoção de um processo contínuo, onde se define um conjunto de diretrizes e controles a serem implantados, procurando-se a proteção e manutenção dos ativos e o retorno dos investimentos.

Para a gestão da segurança da informação, as normas internacionais de segurança identificam pontos importantes, com destaque para a política de segurança, que estabelece a filosofia de proteção dos ativos da organização. Entretanto, as normas focam no que uma política de segurança da informação deve conter, e pouco direcionam à escrita de uma política de segurança efetiva que leve em conta a cultura da organização (HÖNE; ELOFF, 2002). Vale lembrar que as normas têm um cunho internacional sendo assim, abrangentes. Elas foram criadas com a percepção de que cada implantação deverá considerar as leis, as limitações e problemas organizacionais no país onde a organização se encontra. Assim, as organizações precisam escrever suas políticas de segurança levando em consideração a cultura e as características locais, adaptando, quando for necessário, as normas às suas necessidades.

Uma dificuldade que surge durante a elaboração de uma política de segurança é que nem sempre o que precisa ser protegido é tangível. A reputação de uma instituição é um exemplo disto. Então, numa vasta gama do que é preciso ser protegido, deve-se tomar cuidado em não se perder nos pormenores dos elementos a serem protegidos, o que poderá promover o insucesso da política de segurança. Assim, é importante que, na política de segurança, faça-se presente apenas aquilo que realmente necessita ser protegido.

---

[1] Controles [de segurança]: são implementações em hardware, software ou algum processo, que visam reduzir os riscos a um nível aceitável (Norma ABNT NBR ISO/IEC 17799:2005, página xi)

Portanto, é preciso levar em consideração que os ambientes organizacionais possuem suas peculiaridades e isso aumenta o desafio no estabelecimento de uma política de segurança. Um exemplo destas organizações são os ambientes encontrados nas universidades públicas. Elas respondem por uma grande infraestrutura de conectividade e um grande parque computacional do país, e no caso de comprometimento da rede e dos computadores eles poderão ser usados para deflagrar crimes cibernéticos.

O desafio é encontrar respostas para alcançar o alinhamento e o equilíbrio da implantação de controles no que deve ser protegido e expresso na política de segurança, e assim, atingir os objetivos da universidade, como a criação e disseminação do conhecimento; o provimento de serviços; a justiça, equidade e diversidade no acesso à educação; a autonomia institucional; a liberdade acadêmica e intelectual; a promoção da ética, da integridade e da responsabilidade (OBLINGER, 2003).

A harmonia entre a liberdade acadêmica e as restrições de segurança não pode ser imposto. A comunidade acadêmica precisa ser consultada para que o interesse dela seja preservado. Afinal, será ela quem irá julgar e determinar a efetividade da implantação de controles de segurança.

Analisando as universidades públicas, elas possuem uma população transiente, composta por sua grande maioria de discentes, e o corpo de servidores (onde se incluem os docentes e os técnico-administrativos). Este público pode ser considerado a grande parte dos usuários de um ambiente acadêmico comum, encontrado nas universidades públicas do país.

Também é pertinente observar que a cultura acadêmica tende a favorecer a tolerância, o anonimato e a experimentação (OBLINGER, 2003) por parte dos seus usuários. Essas características devem refletir na elaboração de uma política de segurança, onde é preciso identificar os agentes transgressores e fazer presente os meca-

nismos de segurança de maneira a procurar uma rápida resposta a incidentes, protegendo assim, os ativos[2] da instituição.

A segurança da informação, indicada por uma política de segurança, não deveria intencionalmente (ou não intencionalmente) comprometer os princípios da academia. As práticas de segurança devem suportar um comportamento aceitável dos usuários; a liberdade acadêmica e intelectual; possibilitar o debate e averiguação de assuntos sensíveis e polêmicos; respeitar leis municipais, estaduais e federais; promover equidade, diversidade e acesso à informação, a justiça, a ética, a integridade e a responsabilidade da comunidade acadêmica. Portanto, sem a segurança da informação, não é possível ter a privacidade, confidencialidade e integridade que os usuários necessitam, culminando com o comprometimento dos princípios e valores da universidade (OBLINGER, 2003).

Estes valores e princípios foram conquistados ao longo dos tempos pela comunidade acadêmica e cada instituição é livre para estipular os seus. Mas, muitas vezes, os controles de segurança vão de encontro a esses valores e princípios. Então, é preciso que uma política de segurança para este ambiente reflita os reais interesses da instituição e assim, acomode a real intenção da segurança que não é limitar as instituições, mas sim, auxiliá-las a alcançar seus propósitos mais nobres.

Além desse desafio, é válido indicar que no presente momento existem novos investimentos em infraestrutura e o aumento das vagas de ingresso nas universidades públicas federais (BRASIL, 2010). Como indicado por Chang e Ho, (2006), a mudança de cenário causa desafios para a segurança da informação nas organizações. Observa-se que os recursos são alocados conforme a demanda, mas, a segurança da informação não é uma questão puramente tecnológica (SOLMS, 2001). Uma segurança baseada em produtos e tecnologias sozinha não pode proteger a instituição (CHANG;

---

[2] Ativo: qualquer coisa que tenha valor para a organização. [ISO/IEC 13335-1:2004]

HO, 2006; MUNLEY, 2004). Gerenciar a segurança da informação não é uma questão de quantidade, mas sim, de qualidade. Baker e Wallace (2007) destacam que o ambiente acadêmico possui controles de segurança de baixa qualidade comparado com outros tipos de organizações. Quando uma organização identifica apropriadamente os seus pontos de falhas, ela pode efetivamente gerenciar os riscos de segurança, e assim, implementar controles mais efetivos.

No ambiente universitário, identificar esses pontos não é uma atividade trivial pelas características de liberdade requisitadas pelos usuários da academia. Eles, os usuários, geralmente, são rotulados como as fontes de mazelas para a segurança das organizações (MITNICK; SIMON, 2003), mas por outro lado, são a razão de ser delas. Assim, especificamente, os usuários de um campus têm papel importante na contribuição da segurança da informação, pois eles precisam estar envolvidos, já que além do fator técnico, a segurança da informação engloba os fatores organizacionais e sociais (BAKER; WALLACE, 2007), também. É um fator social, pois envolve as pessoas e como elas se relacionam no ambiente de trabalho. E também um fator organizacional porque a segurança depende da característica da organização, como, por exemplo, o apoio da administração e a atribuição de responsabilidades para com a segurança da informação.

Logo, faz-se necessário reduzir a complexidade no processo de elaboração de políticas de segurança da informação através da consulta dos usuários sobre o que eles percebem como sendo os fatores mais importantes para a segurança da informação, além de elaborar políticas de segurança considerando tais fatores.

Como consideração final, é pertinente indicar que existem poucos trabalhos empíricos[3] na área de segurança da informação, como relatado por Machado (2008). Werling, Hawkey e Beznosov (2008) ressaltam que mais pesquisas na área devem ser

---

[3] "Uma investigação empírica é uma investigação em que se fazem observações para compreender melhor o fenómeno (sic) a estudar" (HILL e HILL, 2005, p.19).

realizadas para buscar testar teorias emergentes sobre a efetividade das políticas de segurança nas organizações, em especial as universidades. Até onde foi pesquisado, a literatura carece de um trabalho empírico que explore a percepção da segurança da informação dos usuários que aborde os três tipos de usuários no ambiente acadêmico, professores, alunos e técnicos-administrativos.

Portanto, é importante investigar, através de uma pesquisa empírica, a percepção da segurança da informação dos usuários numa universidade pública. Este trabalho de pesquisa vem a contribuir para a implantação de políticas de segurança eficazes. Com as contribuições de trabalhos como este, a adoção de políticas de segurança terá menos dificuldades de aceitação por parte da comunidade acadêmica. Portanto, é fundamental analisar a percepção do usuário na segurança da informação em uma universidade pública, para o estabelecimento de políticas de segurança, de controles, de guias e de procedimentos mais efetivos.

1.1 Objetivo

O objetivo geral deste trabalho é realizar uma investigação visando descobrir os fatores mais importantes para explicar a eficácia de políticas de segurança no âmbito de uma universidade pública, através da análise da percepção da segurança da informação dos usuários. Para alcançar tal objetivo, é necessário que se cumpram os seguintes objetivos específicos:

- Levantar bibliografia dos trabalhos existentes na área afim, reconhecendo dados secundários à segurança da informação e conseqüentemente sobre os elementos que compõe a percepção do usuário sobre a segurança da informação;
- Caracterizar a percepção do usuário com relação ao seu papel como agente em prol da segurança da informação no âmbito de uma universidade pública;
- Formular as hipóteses sobre os elementos que descrevam a percepção do usuário;

- Realizar um estudo empírico, com a aplicação de um questionário junto aos usuários;
- Computar os dados coletados através da análise fatorial exploratória, visando à identificação dos fatores mais importantes, a fim de confirmar ou refutar as hipóteses do trabalho;
- Propor recomendações que norteiem a elaboração de políticas de segurança da informação em universidades públicas, com base nos resultados obtidos.

1.2 Justificativa

A realização deste estudo busca investigar a percepção dos usuários de uma universidade pública sobre a segurança da informação através de uma pesquisa quantitativa. A pesquisa baseia-se na análise de respostas obtidas nos questionários aplicados aos usuários de uma universidade pública sobre os fatores encontrados no ambiente universitário que envolvem a segurança da informação.

É notório que, no cenário atual, as universidades públicas estão recebendo recursos financeiros sem precedentes, o que resulta na realização de investimentos, inclusive expansão, nos diversos setores das instituições de ensino superior do país (BRASIL, 2010). Com este fato, emerge a questão do que é preciso ser feito para realizar a proteção dos ativos resultantes destes investimentos.

Sem o devido tratamento à segurança da informação, as universidades públicas sofrerão limitações para o seu crescimento. Por exemplo, as políticas de segurança vigentes podem não refletir mais a necessidade de proteção dos ativos, e com isso, as novas ameaças a segurança da organização não serão contempladas.

Ademais, os processos de negócio das universidades estão migrando para a informatização (por exemplo, sistemas de acadêmicos, que realizam gerenciamento de matrículas e notas de alunos, sistemas administrativos, sistemas de recursos humanos, entre outros). Manter a segurança destes sistemas, hoje, é vital para o funcionamento normal da instituição, pois numa situação de indisponibilidade destes siste-

mas, implicará em transtornos e má qualidade no atendimento à população, perda de investimentos (perda de prazos de editais para projetos de pesquisa), e até processos judiciais contra a instituição.

Portanto, as políticas de segurança da informação devem refletir o momento atual, necessitando-se o estabelecimento de medidas que não tornem as políticas de segurança complexas, com o objetivo de ter a efetividade da segurança da informação nesse tipo de organização. Assim, será pesquisada a percepção dos usuários de uma universidade pública sobre a segurança da informação, de sorte que a computação e análise dos dados desta pesquisa auxiliem a expandir o conhecimento sobre os problemas relativos à segurança da informação no âmbito de uma universidade pública e, se possível, tentar ajudar a solucioná-los.

1.3 Organização do Trabalho

O trabalho está organizado nos seguintes capítulos:

- **Capítulo 2: revisão da literatura.** Compila os artigos relevantes ao tema do trabalho. Essa revisão busca extrair de estudos empíricos qualitativos e quantitativos o fundamental teórico para embasar a investigação quantitativa sobre os fatores que permeiam a percepção do usuário sobre a segurança da informação, com foco especial no âmbito das universidades;
- **Capítulo 3: fundamentação teórica.** Embasa os principais conceitos sobre investigação por questionário e a teoria da análise fatorial exploratória, que será utilizada para testar as hipóteses do trabalho;
- **Capítulo 4: desenho do estudo.** Descreve a metodologia do estudo, bem como as hipóteses do trabalho. Também é exposto o questionário quantitativo que visa coletar os dados que corroborem ou refutem as hipóteses do trabalho;
- **Capítulo 5: resultados.** Apresenta os resultados numéricos, em tabelas, gráficos de barras, com as estatísticas descritivas e estatísticas indutivas;

- **Capítulo 6: discussão.** Realiza uma análise crítica dos resultados obtidos utilizando a literatura revisada;

- **Capítulo 7: considerações finais.** Enuncia as conclusões da dissertação. Em seguida, destaca as contribuições do trabalho para a área de conhecimento em questão. É finalizado com sugestões para trabalhos futuros.

Capítulo

2

Revisão da Literatura

> "Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas."
>
> *Provérbio Japonês*

A revisão da literatura busca extrair os fatores que permeiam a percepção dos usuários sobre a segurança da informação, em específico, os usuários que utilizam a infra-estrutura de TI de instituições de ensino superior. Esses fatores podem ser diversos e, como classificados por Werling, Hawkey e Beznosov (2009), são caracterizados como de caráter humano, organizacional ou tecnológico.

É importante observar que a percepção do usuário sobre a segurança da informação pode ser analisada por várias facetas, por exemplo, pela descrição do seu comportamento e motivação. Assim, limitou-se a análise apenas a fatores percebidos pelos usuários, e então, não se adentrando no mérito das teorias e modelos comportamentais e motivacionais, como indicado por Sipone (2001) e estudado por Gonzales e Sawicka (2002) e Silva e Stein (2007).

Entendem-se os fatores humanos como aqueles relacionados com a cognição ao nível individual, associado à cultura e à interação com outras pessoas. Os fatores organizacionais são compreendidos como os aspectos que estão relacionados com a estrutura da organização e seus processos de negócio[4]. Já os fatores tecnológicos, relacionam-se com as soluções técnicas e estão associados aos algoritmos, aplicações, equipamentos e protocolos (WERLING, HAWKEY e BEZNOSOV 2009).

Apesar do presente trabalho não esgotar os fatores encontrados no ambiente acadêmico sobre a percepção dos usuários acerca da segurança da informação, é importante ater-se a poucos fatores, justificado pelo fato do questionário necessitar ter um tamanho factível para ser colocado em prática.

Com estas ressalvas, o restante do capítulo está organizado nas seguintes seções: 2.1 Políticas de Segurança, principais ideias sobre a importância de uma política de segurança numa organização; 2.2 Usuários de uma universidade pública brasileira, apresenta o perfil típico dos usuários dos recursos computacionais de uma universidade pública brasileira; 2.3 Trabalhos relacionados, apresenta os trabalhos na literatura que são destaques para este tipo de investigação; 2.4 Fatores a serem pesquisados, levanta os fatores que foram julgados pertinentes para a pesquisa; o capítulo é encerrado com a seção 2.5 Considerações finais.

2.1 Políticas de Segurança

A informação é um ativo que fornece vantagens nos processos de negócios das organizações e deve ser protegida. Para que isso ocorra, é importante identificar os riscos a que a informação está submetida. Por exemplo, no caso onde as informações de contas dos usuários estejam centralizadas em apenas um único servidor de rede,

---

[4] "Processos de negócio referem-se aos métodos exclusivos segundo os quais o trabalho é organizado, coordenado e focado para produzir um produto ou serviço de valor" (LAUDON, K.; LAUDON, J. 2004, p. 6).

uma falha crítica pode inviabilizar a disponibilidade das informações de contas. Logo, identificar os riscos e ter a ciência do impacto que a sua ocorrência pode causar à instituição é uma tarefa fundamental para saber o que deve ser protegido.

Assim, surge a política de segurança da informação. Nela, a instituição explicita o que será protegido e quais as restrições e descrições que os controles devam obedecer para implementar a política. Entretanto, as restrições e descrições não devem entrar nos méritos de como esta proteção será feita (BARMAN, 2001). As descrições são de alto nível e devem ser baseadas numa análise/avaliação de riscos da organização. Como indicado na seção 5 da norma brasileira que traz o código de prática para a gestão da segurança da informação, o objetivo da política de segurança para a organização é:

> Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 8)

Logo, sem uma política de segurança, uma organização não saberá o que proteger, nem os riscos existentes ou potenciais. Portanto, o esforço deverá recair sobre uma preocupação global da segurança da informação e não em pontos específicos, por exemplo, a configuração de um *firewall*, muitas vezes em desalinho com os objetivos organizacionais.

Os objetivos da política de segurança precisam ser definidos sobre o que será protegido e o porquê da proteção. Para tal, é preciso saber quais sistemas, ativos e processos são importantes para cumprimento do objetivo da organização. E os usuários são de fundamental importância. Afinal, são os usuários que operam e mantêm os ativos da organização.

2.2 Usuários de uma universidade pública brasileira

Os usuários de uma universidade pública são peculiares, e diferem dos usuários de universidades privadas e outros tipos de organizações. Por exemplo, na uni-

versidade pública, a maior parte dos usuários, alunos, possui um vínculo muito curto com a instituição (entre 4 a 5 anos, tempo médio de um curso de graduação). Outros usuários têm vínculos mais longos com a instituição. Eles são os professores e funcionários (docentes e técnicos administrativos, respectivamente) gozam de estabilidade do emprego. Essa rigidez dos recursos humanos, por exemplo, impossibilita a substituição de funcionários responsáveis pela segurança da TIC que são improdutivos e não capacitados, por outros que podem exercer melhor as funções de segurança requeridas pela universidade pública.

Além disso, nas universidades públicas, existe um ambiente de liberdade acadêmica onde os usuários promovem a expansão do conhecimento humano, a averiguação e discussão de assuntos sensíveis e polêmicos que requer, para tal, o livre acesso à informação e à sua criação.

As universidades privadas, que tem o ambiente organizacional similar das universidades públicas, também diferem da universidade pública em sua essência. Nas universidades privadas, apesar de poder ter as três vertentes de ensino, pesquisa e extensão, elas objetivam o lucro, porque é o meio que as sustentam. Isso já não ocorre nas universidades públicas, onde a formação acadêmica é a razão de sua existência.

Com essas observações, a definição de usuário, no ambiente acadêmico, será a mesma que indicada por Albrechtsen (2006, p. 276, tradução nossa): “Um usuário pode ser caracterizado como uma pessoa com acesso legítimo para os sistemas de informação da organização”.

Segundo Albrechtsen (2006), os usuários desempenham um papel ativo na segurança, pois eles podem prevenir incidentes, proteger os recursos materiais (por exemplo, computadores) e não materiais (exemplo, imagem da instituição) da organização, além de reagir quando incidentes de segurança ocorrem. Assim, os usuários podem contribuir com várias ações de segurança no dia a dia, como evitar usar sof-

twares sem licença, ser cautelosos na abertura de anexo em e-mails, indicar brechas de segurança, ter cautela ao usar a internet, manter as atualizações de segurança em dia (quando aplicável), utilizar senhas de qualidade[5], entre outras.

Observando, os usuários das universidades públicas brasileiras são compostos por alunos (ou discentes), professores (os docentes) e funcionários (técnicos administrativos), basicamente. Os alunos têm acesso aos recursos computacionais somente após se submeterem a um processo de seleção para ingresso a universidade (processo de ingresso usual). Isto ocorre através de esforço pessoal e intelectual. Na universidade é senso comum que este usuário irá se comportar visando uma formação que lhe forneça subsídios para o desenvolvimento de uma carreira profissional.

Já os professores utilizam a infraestrutura da universidade para desenvolver suas atividades de ensino, pesquisa e extensão que trazem benefícios tanto para eles quanto para a sociedade. Ter um comportamento no sentido de comprometer a infraestrutura da universidade irá de encontro aos meios que lhes sustentam.

E os funcionários desejam exercer suas atividades de maneira mais rápida e de modo a evitar a sobrecarga de trabalho (o que causaria improdutividade). Caso a infra-estrutura computacional e a rede da universidade sejam comprometidas, estes terão dificuldades de realizar suas atividades.

Portanto, os usuários não têm interesse nem se empenham, a princípio, em comprometer a infraestrutura da universidade, tendo em vista que isto não lhes trará benefícios. Entretanto, os usuários podem ter um comportamento contrário ao desejável (SASSE, BROSTOFF, WEIRICH, 2001), não importando o quão boa seja a tecnologia de segurança utilizada (SOLMS, 2001). Sendo assim, é necessário consultá-

---

[5] Uma senha de qualidade ocorre quando são fáceis de lembrar; não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa; não vulneráveis ataque de dicionário; isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos.

los para saber o que eles percebem como sendo os fatores, na instituição, fundamentais para a efetividade da segurança e assim, investir os esforços nestes fatores.

2.3 Trabalhos relacionados

Nesta seção, são abordados alguns trabalhos relacionados às áreas que são de interesse do trabalho. Eles serão guias para a identificação dos fatores a serem pesquisados. Assim, a seção está organizada com as seguintes subsecções:

- 2.3.1 Resenha 1, aborda o artigo "Erros humanos e violações na segurança da informação e de computadores: o ponto de vista dos administradores de rede e especialistas em segurança" (KRAMER; CARAYON, 2007, tradução nossa);
- 2.3.2 Resenha 2, se tem o artigo "Fatores organizacionais para a efetividade da implementação da gestão da segurança da informação" (CHANG; HO, 2006, tradução nossa);
- 2.3.3 Resenha 3, artigo "Humano, organizacional e tecnológico – desafios para implementação da segurança da TI nas organizações" (WERLING; HAWKEY; BEZNOSOV, 2009, tradução nossa);
- 2.3.4 Resenha 4, dissertação de Machado (2008) "Um estudo empírico sobre a influência de fatores organizacionais na percepção da efetividade da segurança da informação em universidades públicas."

2.3.1 Resenha 1

Este artigo (KRAMER; CARAYON, 2007) buscou descrever os erros e violações cometidas por usuários finais de laboratórios de computadores no ambiente universitário, pela percepção de administradores de rede e especialistas de segurança. Com a participação de 16 entrevistados, elaborou-se um *framework* que explora os fatores humanos e organizacionais. O *framework* inclui uma taxonomia de erros humanos que busca descrever as condições do ambiente de trabalho que contribuem para dificultar a segurança da informação e de computadores.

É relevante na pesquisa, a indicação de que os administradores de rede tendem a perceber os erros criados pelos usuários finais como sendo mais intencionais do que não intencionais. A justificativa para tal é que, primeiro, geralmente, os administradores de rede não entendem as reais necessidades dos usuários finais no uso da rede. Segundo, políticas de segurança e procedimentos elaborados por administradores de rede não acomodam tais necessidades, fazendo com que os usuários finais menosprezem ou burlem as regras criadas.

Ademais, os administradores de rede indicam que os erros criados por eles (administradores), são mais não intencionais do que intencionais. Isto é resultado do fato de que o conhecimento e entendimento da rede estão associados às tarefas e procedimentos diários realizados.

Especialistas em segurança e administradores de rede relatam que fatores como a falta de recursos humanos para monitoramento e gerenciamento da rede, a falta de tempo, sobrecarga de trabalho, inconsistência na prioridade da segurança e falha de comunicação, contribuem para a introdução de erros nos sistemas e na rede da organização.

2.3.2 Resenha 2

O objetivo deste trabalho (CHANG; HO, 2006) foi examinar a influência dos fatores organizacionais para a efetividade da implementação do padrão de segurança da informação BS7799[6]. O modelo de pesquisa foi formulado baseado na revisão da literatura e o estudo empírico foi conduzido para mostrar como os fatores organizacionais influenciam as organizações na adoção do padrão em diferentes tipos de organização.

---

[6] A norma internacional BS7799 foi atualizada e equivalente, agora, a norma brasileira ABNT NBR ISO/IEC 27002 para a gestão da segurança da informação.

A coleta de dados ocorreu com a utilização de questionário. As organizações envolvidas na pesquisa foram companhias de vários segmentos da indústria (saúde, financeira, educação, etc.). O público alvo eram gerentes *seniors* destas organizações, ou equivalentes, que tinham experiência/conhecimento em TI.

A conclusão do estudo mostra que existem impactos significantes dos fatores organizacionais para efetividade da implementação da gestão da segurança da informação. Os fatores indicados como significantes pelo estudo incluem: a competência de TI dos gestores de negócio; o ambiente incerto das organizações (mudança de legislação, competidores de mercado, economia, entre outros); o tipo de indústria (organizações educacionais, financeiras, entre outras) e o tamanho da organização.

2.3.3 Resenha 3

Este trabalho (WERLING; HAWKEY; BEZNOSOV, 2009) empírico de pesquisa e de análise qualitativa buscou extrair uma lista de fatores sobre os desafios práticos enfrentados nas organizações (em especial, do tipo acadêmico) para a segurança da TI, bem como o relacionamento entre estes fatores.

O público alvo da pesquisa constituiu-se de respondentes envolvidos com a segurança da TI em suas organizações, do meio acadêmico, governamental e privado (17 organizações no total). Foram coletados dados de 36 entrevistados.

Os dados validaram e estenderam outros estudos que abordam os desafios da segurança da TI. Nos questionários, perguntou-se sobre as atividades, ferramentas e desafios enfrentados pelos profissionais de TI. Dois pesquisadores foram alocados para realizar as entrevistas e, assim, reduzindo-se as chances de enviesamento nas respostas. As entrevistas foram analisadas através da técnica descrição qualitativa, com comparação restrita e análise indutiva de dados. Além disso, os resultados obtidos foram organizados por tipos de desafios identificados pelos participantes. Cada tipo sofreu uma classificação, conforme listagem abaixo:

- Humano

    - *Falta de treinamento em segurança;*
    - *Falta de cultura em segurança;*
    - *Diferentes percepções de risco;*
    - *Problemas de segurança (comunicação).*
- Organizacional
    - *Estimação de risco;*
    - *Ambiente aberto e liberdade acadêmica;*
    - *Falta de orçamento;*
    - *Baixa prioridade da segurança;*
    - *Horários apertados;*
    - *Interações com outras organizações;*
    - *Distribuição do gerenciamento de TI;*
    - *Controle de acesso.*
- Tecnológico
    - *Complexidade técnica;*
    - *Vulnerabilidades (sistemas/aplicações);*
    - *Acesso móvel.*

Após essa organização, foi executada uma análise cruzada desses desafios, descritos pelos participantes, considerando o tipo de organização e a função do entrevistado. Isso resultou na elaboração do esquema da Figura 1. Nele, existem as associações entre os fatores que desafiam a TI nas organizações. As setas unidirecionais indicam fatores que afetam outros, enquanto as setas bi-direcionais são associação entre os fatores.

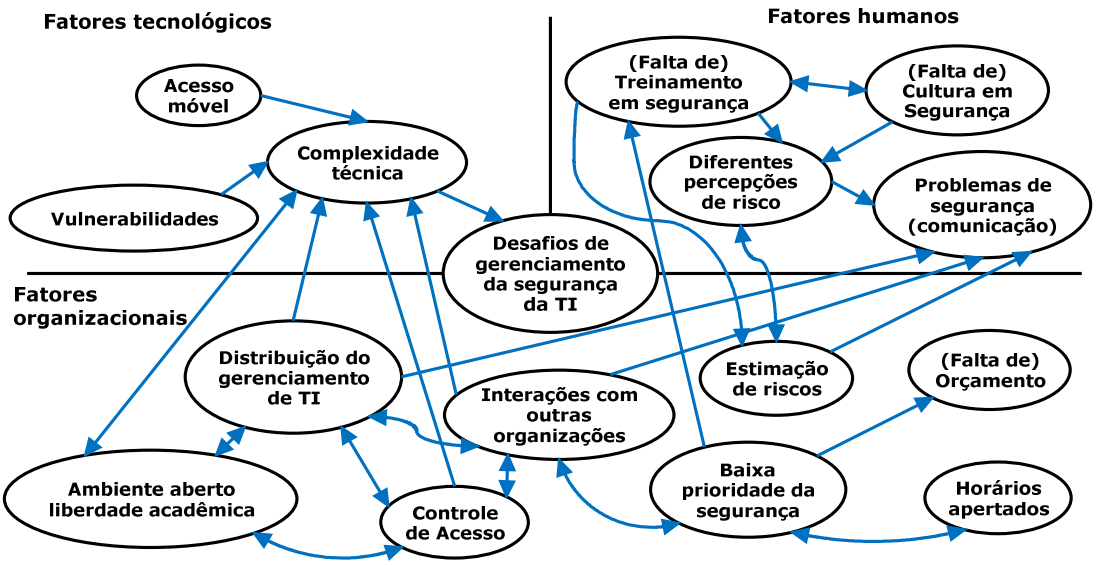

Figura 1 Esquema elaborado por Werlinger, Hawkey e Beznosov (2009, p.14) descrevendo o framework dos desafios da gestão da segurança da informação. Os autores concluem que este esquema, baseado em dados empíricos, deve ser guia para mais pesquisas sobre políticas de segurança para organizações que enfrentam os desafios da segurança da TI.

2.3.4 Resenha 4

Machado (2008) realizou um estudo empírico sobre a influência de fatores organizacionais na percepção da efetividade da segurança da informação nas universidades públicas do país. Ele teve como público alvo as pessoas que direta ou indiretamente estavam envolvidos com a área de segurança da informação nas universidades.

Assim, foram aplicados dois questionários um qualitativo e o outro quantitativo. O qualitativo obteve 23 casos e buscou fomentar a identificação de fatores organizacionais para o ambiente acadêmico, os quais foram utilizados para elaborar o questionário quantitativo. Então, de posse dos fatores selecionados, 10 fatores ao todo, o questionário quantitativo obteve respostas de 75 casos. O objetivo do questionário quantitativo era identificar aqueles fatores que mais contribuíam para a percepção da segurança da informação em universidades públicas.

Através da aplicação da técnica estatística da análise fatorial exploratória, Machado (2008) encontrou e concluiu que o fator apoio da administração é o que mais

contribui para explicar a segurança da informação na visão dos envolvidos diretamente ou indiretamente com a segurança da informação nas universidades públicas brasileiras. Entretanto, ele não trabalhou outros usuários como professores, alunos e técnicos administrativos (que não tenham funções associadas à segurança da informação).

2.4 Fatores a serem pesquisados

Pelos trabalhos pesquisados na literatura, há indícios de fatores importantes que influenciam a segurança da informação no âmbito de uma universidade. Por considerar a existência de fatores mais relevantes do que outros, buscou-se limitar àqueles que apresentam relevância ao tipo de organização e ao tipo de pesquisa que será realizada. Este julgamento teve como fonte a literatura, em especial estudos qualitativos, e a observação e experiência pessoal no ambiente de trabalho na universidade.

Foi possível debruçar-se sobre questões relevantes à percepção da segurança da informação dos usuários. Assim, os fatores selecionados a serem pesquisados são (as seções seguintes trazem mais informações sobre cada fator):

- Apoio da administração;
- Atribuição de responsabilidade;
- Ambiente de liberdade acadêmica;
- Cultura da segurança;
- Prioridade da segurança
- Participação na segurança;
- Programas de conscientização;
- Comunicação.

Outros fatores são encontrados na literatura são os seguintes: controle de acesso a dados sensíveis; ambientes abertos de TI; estimação de risco; falta de orça-

mento; elevada rotatividade dos usuários; ambientes de TI heterogêneos; autonomia administrativa das unidades organizacionais; relevância da política de segurança da informação; cumprimento da política de segurança da informação; rigidez imposta à gestão de recursos humanos. Eles não foram considerados na pesquisa porque, apesar de serem importantes, apenas um número limitado de fatores devem ser utilizados no questionário para não torná-lo enfadonho e longo, o que consequentemente reduz o número de respondentes.

As seções seguintes abordam cada fator a ser explorado na pesquisa. Além da descrição da importância e definição de cada fator, há uma explanação sobre o porquê de sua escolha, tendo como base a literatura revisada e uma maior atenção aos estudos qualitativos.

2.4.1 Apoio da administração

O apoio da administração é essencial para a efetividade de políticas de segurança numa organização. Segundo Barman (2001, p. 9, tradução nossa), "[...] se a gerência falhar em abençoar estes documentos, a eficácia desses será limitada."

Entretanto, Machado (2008) conclui que as pessoas que trabalham com segurança da informação nas universidades públicas do país não percebem o devido apoio que os dirigentes deveriam fornecer à segurança da informação.

Assim, conforme Chang e Ho (2006) acharam, a segurança da informação é primeiramente um problema gerencial da organização. A competência em TI dos gestores influencia positivamente o correto gerenciamento da segurança da informação. Ou seja, quanto maior o apoio da administração mais efetiva é a segurança na organização.

Na Norma brasileira ABNT ISO/IEC 27002, também há o indicativo do apoio da administração. O controle 6.1.1 comprometimento da direção com a segurança da informação, solicita que:

> Convém que a direção apóie ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p.10)

A recomendação da norma é que a administração se envolva na formulação, na análise e na aprovação da política de segurança.

Assim, será investigado no ambiente acadêmico se os usuários percebem o apoio da administração para com a segurança da informação. Do ponto de vista deste trabalho, buscar-se-á perguntar aos usuários se eles percebem a importância do apoio da administração sobre questões de segurança da informação, como um meio para tornar a segurança da informação mais efetiva na universidade.

2.4.2 Atribuição de responsabilidade

Muitos usuários consideram ser atribuição exclusiva da instituição a importância da segurança da informação (DOURISH et al., 2004). Desta forma, eles ficam livres da responsabilidade de proteger as máquinas e ter ações zelosas para com a segurança. Albrechtsen (2007) relata a entrevista de um usuário, que trabalha em um banco (acredita-se que os usuários da academia também possuam tal opinião), onde indica que o tratamento da segurança é responsabilidade dos profissionais na área. Assim,

> Segurança da informação não é o meu trabalho. Eu tenho que me concentrar nas minhas próprias atividades, e confiar que a segurança do sistema está no lugar [...] Bjorn(43), masculino, banco. (ALBRECHTSEN, 2007,p. 281, tradução nossa).

Apesar ter como público alvo os usuários de um banco e de uma companhia de TI, acredita-se que a percepção da atribuição de responsabilidades, no âmbito acadêmico, seja semelhante à evidenciada no estudo de Albrechtsen (2007). E essa transcrição corrobora com o estudo de Kraemer e Carayon (2007), onde os administradores de rede de uma universidade vêem que os usuários finais divergem dos pro-

cedimentos de segurança, como por exemplo, não serem cautelosos na abertura de anexos enviados por *e-mail*.

A norma brasileira ABNT ISO/IEC 27002, referencia a necessidade de atribuição explícita de responsabilidade para a segurança da informação. O controle 6.1.3 (atribuição de responsabilidades para a segurança da informação) indica que "Convém que todas as responsabilidades pela segurança da informação estejam claramente definidas." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 11,). Além do mais, como uma forma de implantar este controle, a norma solicita que essa atribuição de responsabilidade esteja em conformidade com a política de segurança da informação.

Na pesquisa qualitativa de Werlinger, Hawkey e Beznosov (2009), envolvendo usuários da academia, foi observado que os participantes indicaram a distribuição de responsabilidades da TI como sendo um problema nas unidades organizacionais e, particularmente, no ambiente acadêmico.

O que se quer investigar é se os usuários observam que a atribuição da responsabilidade, na instituição, é um fator importante para a efetividade da segurança da informação.

2.4.3 Ambiente de liberdade acadêmica

Na academia existe um ambiente que fomenta a produção científica e a disseminação do conhecimento. O acesso à informação é questão chave para tal. Entretanto, os mecanismos de segurança (como por exemplo, acesso por senhas, *firewalls*, detector de intrusão, *antivírus*, entre outros) podem ser vistos como um motivo de censura. Impor regras restritivas de segurança pode tornar o ambiente infértil para o livre desenvolvimento de pesquisas.

Conforme pesquisa realizada por Kraemer e Carayon (2007), um administrador de rede de uma universidade expôs a necessidade de introdução de regras no *firewall* da instituição para tornar o acesso mais permissivo:

> Nós temos que ter. Nós temos que colocar buracos para que as pessoas possam desempenhar suas atividades. [...] nós temos que colocar buracos nos **firewalls** para que eles possam executar os processos de ... Isso é uma coisa que você não irá querer provavelmente nunca fazer numa rede pública, normal. Mas ... nosso **firewall** tende a ser como um queijo suíço.[...] (KRAEMER; CARAYON, 2007, p. 148, tradução nossa)

Outra citação do mesmo estudo revela o requisito de liberdade acadêmica na rede da instituição: "[...] E, você sabe, você coloca na rede normal, nós temos aqueles canais abertos para o *firewall* porque são necessários para pesquisa." (KRAEMER; CARAYON, 2007, p. 148)

Machado (2008) indica que a liberdade acadêmica pode ser um fator que explica a segurança da informação no ambiente acadêmico, entretanto, ele não conseguiu confirmar nem refutar essa hipótese. Desta forma, o presente estudo buscará saber se os usuários percebem a importância que o ambiente de liberdade acadêmica para a segurança.

2.4.4 Cultura da segurança

A cultura da segurança pode ser caracterizada como os aspectos da filosofia que direta ou indiretamente afetam o ambiente da segurança da informação na organização (KRAEMER; CARYON, 2007). Ou como Munley (2004, p. 3, tradução nossa) define "Cultura pode simplesmente ser definida como as atitudes e comportamentos de um grupo de indivíduos". Conforme entrevista realizada por Kraemer e Caryon (2007), um especialista da segurança indicou a necessidade da cultura da segurança: "Um dos maiores obstáculos para a segurança de toda a organização é a cultura organizacional [...]" (KRAEMER; CARYON, 2007, p. 150)

No mesmo estudo, um administrador de rede, de uma instituição acadêmica, relata:

> A melhor maneira de levar as pessoas a colaborar para a segurança deve ser deixar inativo [por exemplo, um servidor] por alguns dias porque alguém invadiu as máquinas, e alguém perdeu todas as pesquisas que estavam fazendo. E, então, todos gostam de segurança. Então, nós estamos tipo aleijado (sic) pelo fato de que temos sido bem sucedidos nisso. (KRAEMER; CARYON, 2007, p. 151, tradução nossa)

Como sugere Machado (2008), o fator cultura organizacional está diretamente direcionado com a segurança da informação. No estudo, afirma-se que há uma influência significativa entre o apoio da cúpula de administrativa e a percepção da segurança da informação mediada pela cultura de segurança (MACHADO, 2008, p. 23 apud KNAPP et al., 2005).

Por fim, Munley (2004) destaca que a maior fonte de vulnerabilidade ainda vem das pessoas, pois são elas quem tem acesso ou conhecimento sobre o negócio e os dados na organização. Com um questionário quantitativo, a presente pesquisa buscará investigar a percepção dos usuários sobre a cultura da segurança, também.

2.4.5 Prioridade da segurança [7]

Este fator é identificado pelo estudo de Werling, Hawkey e Beznosov (2009). Ele aponta que a segurança da informação parece não praticável quando a organização não reconhece a segurança como sendo uma prioridade.

Albrechtsen (2006) indica que a sobrecarga de atividades atribuídas aos usuários cria um conflito de interesses entre as atividades desempenhadas na instituição e a segurança da informação. Apesar de Albrechtsen (2006) ter como público alvo os usuários de um banco e de uma companhia de TI, acredita-se que a percepção da pri-

---

[7] A justificativa para o não uso do termo baixa prioridade, termo utilizado no artigo Werling, Hawkey e Beznosov (2009), é por causa do tipo de estudo a ser realizado. A escala do estudo quantitativo será relativa, ou seja, não há um marco de referência absoluto. Será utilizada a escala de intervalo (especificamente a Escala de Likert) na aplicação do questionário. Esta escala tem como característica o valor <<zero>> da escala é arbitrário, ou seja, não é possível fazer uma inferência sobre os valores na escala. Por exemplo, não é possível afirmar que, após a computação dos dados, o apoio da administração é duas vezes, ou qualquer que seja a intensidade, mais importante que outro fator.

oridade da segurança seja um fator que influencia a segurança da informação na academia, também. Em uma das entrevistas um respondente do banco relata,

> Nós somos mensurados por vendas. Nosso salário depende disto, bônus e coisas como estas. Segurança da informação definitivamente é uma segunda ou terceira prioridade. Se nós tivermos que usar metade de uma hora extra em segurança da informação por dia – isto simplesmente não funciona! Harvard, 29, masculino, banco. (ALBRECHTSEN, 2007,p. 281 e 282, tradução nossa).

A segurança aparenta ser um obstáculo em diferentes formas (por exemplo, a solicitação do reinício da máquina após uma atualização, ou solicitando a aceitação de um certificado auto-assinado no acesso web). E assim, para os usuários finais, a segurança acaba não sendo uma preocupação primária (PAUL et al.,2004). Geralmente, a segurança da informação é percebida como uma atividade que não está no fluxo normal de trabalho dos usuários, ou seja, é uma atividade extra que deve ser realizada. Caso os usuários percebam que as ações de segurança não fazem parte do núcleo do processo de negócio da instituição, então a segurança será marginalizada e consequentemente sofrerá prejuízos.

Além disso, Kraemer e Caryon (2007) relatam que os administradores de rede de um laboratório acadêmico indicam que os usuários finais, do laboratório, contribuem para a ocorrência de violações de segurança:

> [...] nós deveríamos ser os mais vorazes em esforços para a segurança, mas estamos paralisados pelo fato que nossa gente, que nós estamos tentando proteger, não quer ser protegida, eles não vêem isto como importante [...] (KRAEMER; CARYON, 2007, p. 148, tradução nossa)

Pelo exposto, o questionário quantitativo indaga aos usuários se eles percebem que a prioridade da segurança é um fator importante para explicar a segurança, ou seja, se a prioridade da segurança é evidenciada por eles. Quanto mais baixa for à prioridade maior serão as dificuldades com a segurança.

2.4.6 Participação na segurança da informação

Albrechtsen (2006) indica que os usuários consideram uma abordagem que os envolva como sendo um meio mais efetivo para aumentar os conhecimentos em segu-

rança e torná-los mais cientes com relação à importância da segurança da informação. Desta maneira, o quão mais envolvido estiver os usuários, mais efetiva será a segurança.

> O Departamento Gestor de Segurança deveria nos fornecer mais informações sobre a segurança da informação e sobre eles mesmos [...] Envolver-nos é a melhor maneira de comunicação. Eles têm que ser visíveis para nós. Então nós iremos nos tornar mais interessados em segurança da informação também [...] Bente (53), feminino, Companhia de TI. (ALBRECHTSEN, 2007, p.283)

Portanto, a participação na solução dos problemas de segurança aparenta ser um fator para o sucesso da segurança da informação na organização. A investigação empírica sobre a percepção da segurança da informação busca a extrair da comunidade acadêmica a percepção do seu envolvimento/participação na segurança da informação como fator importante para explicar a segurança da informação.

2.4.7 Programas de conscientização

Paul et al. (2004) indica que as abordagens de relacionar a segurança e a usabilidade por meio da tecnologia, utilizando implementações que visem à transparência dos controles de segurança trazem problemas, pois não permite que os usuários percebam a segurança da informação no ambiente computacional em que estão. Desta maneira, quando algo inesperado acontece ou quando se faz necessária a solução de algum problema, os usuários não conseguem identificar o problema com sendo relacionado à segurança.

Ademais, Kraemer e Carayon (2007) indicam que o engano dos usuários finais ou a falta de conhecimento em segurança da informação e de computadores são fatores que norteiam a percepção dos usuários finais.

No texto da norma brasileira ABNT ISO/IEC 27002, o treinamento em segurança da informação é descrito no controle 8.2.2 (conscientização, educação e treinamento em segurança da informação):

> Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros, recebam treinamento apropriados em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 28)

É importante lembrar que nas universidades com grande quantidade de usuários ingressantes, a maioria composta por discentes, é muito difícil realizar programas extensos de conscientização e de treinamentos. Como indicado por Siponen (2001), o objetivo da conscientização para a segurança é tornar os usuários intrinsecamente comprometidos com os objetivos da segurança para a organização. Tornar os usuários agentes conscientes é o desafio.

Logo, o presente estudo pesquisa se os usuários acadêmicos percebem a importância dos programas de conscientização da segurança como fonte para explicar a efetividade da segurança da informação na instituição.

2.4.8 Comunicação

Kraemer e Carayon (2007) definem comunicação como sendo as interações entre os membros da instituição. Eles apontam que a comunicação é um dos fatores organizacionais que, quando falha, causa vulnerabilidades de segurança. Numa das entrevistas do estudo, um administrador de rede relata a falha de comunicação que ocorre entre eles:

> Isto [falta de comunicação] é provavelmente algo que nós deveríamos falar sobre. Agora que você mencionou, nós provavelmente deveremos conversar sobre o que deve ser monitorado. Porque há uma lista do que são específicos para os sistemas, como uma trilha de erros, etc, ... (KRAEMER; CARYON, 2007, p. 148, tradução nossa)

Num estudo sobre segurança de senhas, Adams e Sasse (1999) indicam que a comunicação insuficiente entre os projetistas de sistemas e os usuários produzem falhas em projetos de software. Esse estudo mostra que os usuários não são suficientemente informados sobre problemas de segurança. Como conseqüência, os usuários preenchem esse vazio através da construção de seus próprios modelos, muitas vezes de maneira imprecisa, e percepções sobre as ameaças de segurança.

Werlinger, Hawkey e Beznosov (2009) indicam que comunicações e interações efetivas são requeridas para alcançar um entendimento mútuo sobre os riscos de segurança entre diferentes interessados. Na universidade, os usuários precisam ser comunicados sobre as ameaças, vulnerabilidades, regras de uso, políticas e conjunto de boas práticas de segurança.

Assim, uma consulta aos usuários de uma universidade pública, busca ter ciência se eles percebem a comunicação como sendo um fator relevante para o sucesso da segurança da informação. Quanto mais precária for à comunicação com os usuários, mais ineficaz será a segurança na instituição.

2.5 Considerações finais

Neste capítulo, foram apresentadas as principais ideias sobre a importância da política de segurança numa organização, o perfil dos usuários de uma universidade pública brasileira, o que há de relevante na literatura para este tipo de pesquisa e alguns fatores, extraídos da literatura, que são promissores para investigação. Estes fatores foram justificados com estudos qualitativos ou com trabalhos relacionados, para compor o questionário quantitativo (descrito no próximo capítulo).

Capítulo

3

Fundamentação teórica

"A sabedoria só nos chega quando não precisamos mais dela."

Che Guevara

A fundamentação teórica tem o intuito de embasar os conceitos que permeiam a elaboração de uma investigação empírica por questionário e a análise fatorial.

O capítulo é dividido na seguinte maneira: 3.1 Investigação por questionário, aborda as principais características de uma investigação por questionário; 3.2 Análise fatorial, indica as definições da técnica e como aplicá-la; 3.3 Considerações finais, resume os principais pontos do capítulo.

3.1 Investigação por questionário

Ao elaborar uma investigação empírica, baseada na observação, através da aplicação de um questionário, o pesquisador deve considerar várias questões. Entre elas, pode-se pensar nas contribuições para a área de investigação, as escolhas das hipóteses a serem testadas, a maneira como se dará a coleta de dados e os métodos para análise dos dados (HILL, M.; HILL, A., 2005).

Sendo assim, a revisão da literatura tem papel importante. No nosso caso, o capítulo 2, revisão da literatura, revela a necessidade de investigar os usuários de uma universidade pública sobre fatores que ajudem a explicar a segurança da informação. Ademais, dentre estes os fatores, saber quais fatores são percebidos como mais importantes auxiliará e será guia para elaborar políticas de segurança da informação mais efetivas neste tipo de organização (MACHADO, 2008).

Ademais, quando se realiza uma investigação empírica, a grande quantidade de fatores pode se tornar um problema. Então, é importante que os métodos de análise de dados, utilizados pelo pesquisador, busque reduzir o conjunto de fatores abordados, visando à redução dessa complexidade. No campo da estatística existe a teoria da análise fatorial como opção na busca de reduzir um conjunto de dados. Esta redução ocorre através de uma análise da estrutura de interdependência, relacionamento, entre os dados (maiores detalhes dessa técnica serão fornecidos na seção 3.2 Análise fatorial, página 39).

Entretanto, para que estes métodos estatísticos possam ser aplicados aos dados, outros problemas precisam ser abordados. Dentre eles estão o Universo da investigação, a escala a ser utilizada nos itens do questionário, a quantidade necessária de questionários completos para tornar os dados confiáveis, e, como medir indiretamente a percepção dos usuários através dos fatores sobre segurança da informação (HILL, M.; HILL, A., 2005).

3.1.1 Universo do estudo

Uma investigação empírica pressupõe uma coleta de dados fornecidos por entidades chamadas de casos (os casos também podem ser entendidos como o conjunto de respostas fornecidas pelos respondentes ao questionário). Os casos atribuem medidas (ou observações) através de respostas sobre os itens (perguntas ou afirmações) de um questionário. O conjunto total de casos sobre os quais se pretende inferir conclusões é denominado de População ou Universo (HILL, M.; HILL, A., 2005).

A dificuldade em consultar o Universo causa a necessidade de restringir a pesquisa apenas a uma parte do Universo. Esta parte dos casos que compõe o Universo chama-se amostra.

Com relação a uma amostra, para que as conclusões de um estudo possam ser extrapoladas ao Universo é necessário que a amostra seja representativa do Universo. Ser representativa significa que ela contempla as mesmas características encontradas no Universo.

Então, para que os resultados encontrados sobre amostras sejam extensivas ao Universo, Hill, M. e Hill, A. (2005) indicam que duas opções podem ser adotadas. Ou há a escolha de um Universo pequeno de estudo (mas suficiente para aplicação da análise estatística planejada) ou se realiza a escolha de uma amostra representativa do Universo (o tamanho da amostra deverá usar métodos formais de amostragem). Em ambos os casos, é fundamental definir o Universo a ser estudado.

3.1.2 Tamanho da amostra

A pesquisa se debruça sobre a investigação de quais fatores são observados como mais importantes para explicar a percepção em segurança da informação no âmbito da universidade pelos usuários, utilizando a técnica da análise fatorial exploratória. Assim, o foco com relação ao tamanho da amostra será sobre a análise fatorial -AF.

Segundo Hair, Jr. et al (2009), é infactível realizar a AF com menos de 50 observações (casos), e é preferível usar 100 ou mais. Como recomendação, o mínimo é ter pelo menos cinco vezes mais observações que o número de variáveis (as variáveis recebem os valores atribuídos às respostas dos itens) a serem utilizadas e o recomendável é ter uma proporção de pelo menos dez para um. A maior proporção de casos por variável busca minimizar as chances de determinar fatores específicos de uma amostra, com pouca generalidade.

Costello e Osborne (2005) alertam para os pesquisadores que a AF é um procedimento de amostras grande, assim, quanto mais amostras, melhores são os resultados.

3.1.3 Questionário para medir uma variável dependente

"É muito fácil elaborar um questionário, mas não é fácil elaborar um **bom** questionário" (HILL, M.; HILL, A., 2005, p.83). Ou seja, não é fácil elaborar um questionário que forneça dados que permitam testar as hipóteses da investigação. E escrever um questionário no qual meça uma variável dependente é igualmente complicado. Para se entender o porquê, vamos à definição de variável dependente. Uma variável dependente refere-se a:

> "(...) uma variável que não pode ser observada nem medida directamente (sic) mas que pode ser definida a partir de um conjunto de outras variáveis (possíveis de serem observadas ou medidas) que medem qualquer coisa em comum (...)" (HILL, M.; HILL, A., 2005, p.135)

A Figura 2 ilustra a definição de variável dependente. Nela é possível notar que a variável dependente é difícil de ser observada ou mensurada. Entretanto, pode-se compor a variável dependente através de outras variáveis, as chamadas variáveis componentes. Elas são mais fáceis de serem observadas e mensuradas, pois são mais específicas que as variáveis dependentes.

Um exemplo adaptado do livro "*Investigação por Questionário*" de Hill e Hill (2005, p.136) irá auxiliar no entendimento da natureza da variável dependente. Suponha que o diretor de recursos humanos da universidade esteja interessado em medir a Satisfação Global de cada funcionário no setor de RH. Através de uma única pergunta, em um questionário, dirigida aos funcionários ele poderia medir a satisfação no trabalho. Logo, é fácil perceber que a Satisfação Global não é uma variável dependente.

Figura 2 Esquema mostrando que a variável dependente, de difícil observação e mensuração, é composta por variáveis componentes, que são mais fáceis de mensurar e observar.

Entretanto, o diretor pode pensar uma maneira mais confiável e viável de obter dados sobre a satisfação global dos funcionários, tratando a satisfação global como uma variável dependente. Assim, ele poderia definir um conjunto de variáveis mais específicas, por exemplo: 1. Satisfação com o trabalho que o funcionário desempenha; 2. Satisfação com o salário; 3. Satisfação com a equipe de trabalho; 4. Satisfação com o chefe do setor; 5. Satisfação com o ambiente de trabalho; 6. Satisfação com os administradores da universidade. Estes seis tipos de satisfação tendem a estar correlacionados uns com os outros e isto indica que todos eles medem alguma coisa em comum, a variável dependente satisfação global no trabalho.

De maneira análoga, é possível medir a percepção dos usuários sobre a segurança da informação, variável dependente, apenas com uma única pergunta dirigida aos usuários, ou colocá-la em um questionário, sobre o assunto. Portanto, isto indica que a percepção sobre segurança, também, não é uma variável dependente. Entretanto, Hill, M. e Hill, A. (2005) indicam que uma maneira mais confiável e válida de obter a medição dessa percepção é tratando ela como uma variável dependente e definila por um conjunto de outras variáveis mais específicas, as variáveis componentes (mais fáceis de mensurar ou observar).

Com isto, Hill, M. e Hill, A. (2005) indicam duas etapas para construir um questionário que meça uma variável dependente: através da seleção de itens apropriados e da adequação do questionário.

Na primeira etapa, deve-se definir o conjunto de variáveis componentes, com o auxílio de teorias disponíveis e estudos sobre o tema. Então, após a definição deste conjunto, é preciso escrever entre 4 e 6 itens (perguntas ou afirmações) para cada variável dependente. Os itens de uma variável componente são perguntas (ou afirmações) formuladas de modo distinto, mas que essencialmente têm a mesma semântica, de modo que se possa excluir posteriormente da análise perguntas mal formuladas ou enviesadas, após uma análise de confiabilidade. Os itens são mensurados através de respostas fechadas que utilizam alguma escala, como, por exemplo, escala de Likert. Em seguida, aplica-se o questionário a uma amostra de pelo menos 100 pessoas, obtendo os valores de respostas de cada pessoa para cada item. Então, verifica-se a confiabilidade, descartando aqueles que não são adequados.

Na segunda etapa, examina-se duas características da variável dependente: validade e confiabilidade.

A validade busca confirmar que a medição da variável dependente é a mesma que o pesquisador quer medir (HILL, M.; HILL, A., 2005). Há três tipos de validade: validade de conteúdo, validade teórica e validade prática (não será abordado este tipo de validação. O leitor interessado poderá consultar o capítulo 7 de Hill e Hill (2005) para maiores informações).

A validade de conteúdo envolve descrever, baseada na literatura, as componentes da variável dependente. Para cada componente, escreve-se uma lista dos aspectos relevantes (a literatura ajuda na especificação desses aspectos). São os aspectos de cada componente aqueles medidos no questionário. Quando o investigador tiver uma amostra relativamente representativa dos itens que descrevem as variáveis componentes, através dos aspectos delas, ele irá ter validade de conteúdo para a variável dependente. Não é possível calcular um valor numérico para a validade de conteúdo (HILL, M.; HILL, A., 2005).

A validade teórica de refere à busca de que a variável dependente concorde com outras medidas da mesma variável já conhecida na literatura (HILL, M.; HILL, A., 2005). Ou seja, o pesquisador utiliza outros estudos sobre a variável dependente para validar os questionários da sua pesquisa.

Com relação à confiabilidade do questionário, ela está condicionada à repetição e consistência das medidas empíricas coletadas (CAMARGO, 1996). Um mecanismo comumente utilizado para testar a confiabilidade interna de um questionário é o coeficiente de Alfa de Cronbach[8] (HORA, MONTEIRO e ARICA, 2010). O coeficiente mede as associações existentes entre as respostas dos itens relativos a uma mesma variável componente que foram fornecidos pelos respondentes do questionário (HORA e MONTEIRO, 2010).

Entretanto, para usar o Alfa de Cronbach, é necessário ter as seguintes premissas: os itens possuem um mesmo aspecto; os itens devem ser respondidos por uma amostra heterogênea (se as respostas forem muito parecidas o Alfa será próximo de zero); a escala utilizada já deve estar validada.

Após o cálculo, o valor do coeficiente é utilizado para classificar a confiabilidade interna do questionário. A Tabela 1 mostra a classificação para cada valor do coeficiente.

A faixa de valores do coeficiente de Alfa de Cronbach é apenas interpretada no intervalo compreendido de 0 a 1. Valores negativos do Alfa são considerados como zero, ou seja, sem confiança (HORA e MONTEIRO, 2010).

[8] O coeficiente de Alfa de Cronbach foi desenvolvido por Lee J. Cronbach em 1951.

Valor do coeficiente de Alfa de Cronbach	Classificação
> 0,9	Excelente
>0,8 e ≤0,9	Bom
>0,7 e ≤0,8	Razoável
>0,6 e ≤0,7	Fraco
< 0,6	Inaceitável

Tabela 1 Classificação para o valor do coeficiente de Alfa de Cronbach.Escala de medida

A aplicação de métodos multivalorados necessita adotar uma escala para mensurar cada item no estudo. A escolha da escala depende do Universo a ser estudado e fundamenta as técnicas estatísticas a serem usadas.

Como o questionário possui respostas fechadas, ou seja, o respondente poderá selecionar apenas as respostas previamente estabelecidas pelo criador do questionário, faz-se necessário a elaboração de alternativas que satisfaçam o desejo do respondente para com o item.

Assim, as alternativas das respostas que os respondentes estarão limitados a fornecer, devido ao caráter fechado dos itens, buscam receber uma avaliação sobre um determinado item. Sobre a quantidade das alternativas de respostas, Hill, M. e Hill, A. (2005) indicam que o número ótimo irá depender do objetivo do item, a forma da pergunta e das características dos respondentes. Eles também sugerem que os respondentes requerem uma resposta mais detalhada do que duas opções e não mais que sete opções. Para público em geral eles indicam que o uso de cinco alternativas de resposta é satisfatório.

Seguindo essa recomendação, de usar cinco alternativas de respostas para cada item, os respondentes terão que escolher, para cada item, respostas que variam entre discordo fortemente, discordo, neutro, concordo e concordo fortemente. Hill e

Hill (2005) indicam que é muito importante a utilização de um conjunto equilibrado de respostas (como o escolhido), pois evita dúvidas no preenchimento do questionário e divergências de interpretação das respostas tanto pelo respondente e quanto pelo pesquisador.

Além disto, estas alternativas de respostas são consagradas na literatura e representam a Escala de Likert, onde os respondentes especificam o nível de concordância com uma dada afirmação. A Escala Likert, apresentada em 1932, é uma escala psicométrica onde os itens são avaliados pelo respondente baseado em algum nível de concordância com a afirmação exposta

Para caracterizar o respondente, na parte do questionário referente à *descrição do respondente*, as alternativas de respostas devem contemplar também as respostas abertas, sendo algumas alternativas opcionais para respostas que podem ser sensíveis (informações sensíveis são aquelas que podem prejudicar ou constranger de alguma forma o respondente, no julgamento dele), e respostas múltiplas, pois, são necessárias na caracterização satisfatória dos respondentes.

Uma vez selecionada as alternativas de respostas a preocupação é voltada para a definição dos valores para ela. Em cada resposta, quando se atribuem valores discretos numa determinada ordem, tem-se uma escala ordinal. Assim, têm-se os valores para cada alternativa de resposta: 1, 2, 3, 4 ou 5, como mostrado na Tabela 2.

Discordo fortemente	Discordo	Neutro	Concordo	Concordo fortemente
1	2	3	4	5

Tabela 2 Valores atribuídos a avaliação de um item numa escala ordinal.

Além das respostas alternativas na escala ordinal, pode-se fazer com que um item tenha codificação reversa. Na codificação reversa o item tem significado semântico contrário aos demais itens. Por exemplo, se um respondente atribui “concordo fortemente” para um item, então para manter a coerência, ele deve assinalar uma

resposta de discordância para os itens que são de codificação reversa, por exemplo, “discordo fortemente”.

A importância da codificação reversa para alguns itens reside no fato do respondente não saber que os itens buscam ter o mesmo significado, ou tem um relacionamento forte com o fator, e assim, com a codificação reversa, torna-se difícil eles marcarem apenas uma alternativa de resposta em sequência.

Desta maneira, itens com codificação reversa, onde a afirmação do item tem conotação inversa aos demais itens de um fator, os valores das respostas são invertidos, como mostra a Tabela 3. Estes valores não são mostrados aos usuários que respondem ao questionário, mas os itens com codificação reversa são marcados para serem computados na fase de análise dos dados.

Discordo fortemente	Discordo	Neutro	Concordo	Concordo fortemente
5	4	3	2	1

Tabela 3 Itens com codificação reversa terá valores invertidos na escala ordinal.

3.2 Análise fatorial

A análise fatorial envolve um conjunto de métodos direcionados para identificar ordem e estrutura sobre os dados. Todos os métodos têm o mesmo objetivo, nomeadamente, encontrar combinações de variáveis (fatores ou dimensões) que expliquem as correlações paramétricas (do tipo Pearson) entre um conjunto de variáveis (TUCKER e MACCALLUM, 1997).

Para se entender correlações, é válido lembrar o que é variância. Variância é um valor (mais precisamente o quadrado do desvio padrão) que representa a quantia total de dispersão de valores para uma única variável em torno de sua média. Uma variável é correlacionada com outra quando a variância de ambas ocorre de forma direta ou de forma inversa. A análise fatorial busca identificar grupos de variáveis correlacionadas. Estes grupos são chamados de fatores.

A teoria e os métodos aplicados na análise fatorial buscam identificar uma ordem e estrutura aos dados em um estudo, promovendo parcimônia e significado para a correlação entre as variáveis componentes. E isto remete ao postulado que na análise fatorial existem variáveis latentes, características não observáveis nos dados.

Em um estudo quantitativo, as características dos casos são medidas através de itens (ou variáveis). Na aplicação de um questionário, as variáveis componentes serão representadas pelas afirmações dos itens e as respostas atribuídas, serão utilizadas para medir cada variável componente.

No presente trabalho, a dificuldade de se medir a variável latente, percepção da segurança da informação, faz com ela seja mais bem mensurada através da utilização das várias variáveis componentes (fatores selecionados para a pesquisa, vide 2.4 Fatores a serem pesquisados) que descrevam, ou caracterizem, a variável latente.

Por fim, a análise fatorial pode atingir os objetivos do pesquisador ou em uma perspectiva exploratória, ou em uma perspectiva confirmatória. Na exploratória, busca-se uma estrutura em um conjunto de variáveis ou como um método de redução de dados, não estabelecendo restrições *a priori* sobre a estimação de componentes nem sobre o número de componentes a serem extraídos (HAIR, Jr. et al., 2009). Na perspectiva confirmatória, o pesquisador tem idéias preconcebidas da estrutura dos dados (através de uma teoria ou de pesquisas anteriores), e deseja testar hipóteses envolvendo questões sobre quais variáveis deveriam ser agrupadas em um fator, ou o número exato de fatores (HAIR, Jr. et al., 2009).

Não será utilizado no presente trabalho o caráter confirmatório da análise fatorial[9] (ou seja, análise fatorial confirmatória), mas sim, a análise fatorial exploratória, tendo em vista identificar uma estrutura nos dados que possa auxiliar na explica-

---

[9] O leitor interessado na análise fatorial confirmatória poderá consultar o Capítulo 11 do livro de Hair, Jr. e*t al* (2009) para uma abordagem mais aprofundada sobre o assunto.

ção da percepção da segurança da informação pelos usuários de uma universidade pública.

Para tornar mais evidente as diferenças entre análise fatorial exploratória e análise fatorial confirmatória. Em uma investigação empírica pouco se sabe sobre a estrutura dos dados, o pouco de informações que se tem ou são suposições baseadas na experiência ou estudos similares, mas que possuem outras características (por exemplo, público alvo diferente). Assim, as expectativas e hipóteses iniciais podem ser confirmadas ou não após a coleta de dados. Não existe uma obrigatoriedade de que os dados sigam aquilo que a experiência indica e então, a aplicação da análise fatorial em caráter exploratório se torna adequada para este tipo de investigação.

Entretanto, isto não acontece na análise fatorial confirmatória, onde os dados precisam se "encaixar" em uma teoria existente, a fim de confirmá-la. De uma maneira mais precisa, a análise fatorial confirmatória é utilizada para avaliar "o grau em que os dados satisfazem a estrutura esperada" (HAIR, Jr. et al, 2009) dos dados.

Para aplicação da análise fatorial deve-se verificar a adequação dos dados coletados para aplicação da análise fatorial, determinar o número de fatores a extrair, rotação dos fatores e a interpretação e rótulo dos novos fatores agrupados.

3.2.1 Adequação do uso da análise fatorial

Após a coleta de dados, o investigador deve aplicar vários métodos que o auxilie na correta aplicação da análise fatorial. Um método utilizado para avaliar se a quantidade de dados é adequada à realização da redução de dados, através da análise fatorial, é cálculo do Kaiser-Meyer-Olkin, ou KMO. A interpretação do valor do KMO pode ser encontrada na Tabela 4. Valores iguais ou inferiores a 0,5 do KMO inviabilizam a realização da AF.

Valor do KMO	Recomendação relativa à AFE
]0,9-1,0]	Excelente
]0,8-0,9]	Boa
]0,7-0,8]	Média
]0,6-0,7]	Razoável
]0,5-0,6]	Má
≤ 0,5	Inaceitável

Tabela 4Valores do KMO e a recomendação relativa à realização da AF..

Outro método que determina a adequação da amostra para a realização da AF é o teste de Bartlett. Ele é um teste estatístico que indica a presença de correlações entre as variáveis em estudo (Hair Jr. et al.,2009). Levanta a hipótese de que a matriz das correlações pode ser a matriz identidade (determinante igual a 1). Caso ocorra, a AF não é exequível. Um teste de esfericidade de Bartlett estatisticamente significante (sign. < 0,05) indica que correlações suficientes existem entre as variáveis para se continuar a análise.

A adequação da AF, para cada item, pode ser verificada com a análise da matriz anti-imagem. Ela é uma forma de obter informações sobre a necessidade de eliminação de uma variável (FÁVERO et al., 2009) da AF. Na matriz anti-imagem, há valores sobre a Medida de Adequação da Amostra, ou *Measure of Sampling Adequacy* (MSA). Tais valores estão localizados na diagonal da matriz anti-imagem e quantificam o grau de intercorrelações entre as variáveis, assumindo um valor entre 0 e 1, alcançando o valor 1 quando a variável é perfeitamente prevista sem erro pelas outras variáveis do modelo (HAIR Jr., 2009).

Valores do MSA abaixo de 0,5 não são aceitáveis para AF. Outros valores da MSA podem ser encontrados na Tabela 5.

Valor da MSA	Recomendação para a variável
≥ 0,8 e ≤1,0	Admirável
≥ 0,7 e <0,8	Média
≥ 0,6 e <0,7	Medíocre
≥ 0,5 e <0,6	Ruim
≤0,5	Inaceitável

Tabela 5 Valores para o índice da Medida de Adequação da Amostra, ou MSA.

3.2.2 Método de extração e número de fatores a extrair

Há vários métodos de extração para a realização da análise fatorial. A escolha do método depende do objetivo do pesquisador. Os mais populares são análise dos componentes principais, análise dos fatores comuns, máxima verossimilhança, mínimos quadrados ordinários e generalizados e alpha (FÁVERO et al., 2009) [10].

Assim, pelo objetivo da pesquisa se destinar a explicar a estrutura latente da matriz de correlações, então, será utilizado o método máxima verossimilhança que se destina a este fim. Além disso, ele é um método de extração indicado para uma amostra de indivíduos retirados de uma população normal (FÁVERO et al., 2009). Por fim, este método é indicado por Costello e Osborne (2005) como o verdadeiro método de extração para análise fatorial.

Além do método de extração, o pesquisador deve buscar critérios para decidir quantos fatores deve reter. Fávero et al. (2009) indica alguns critérios que auxiliam o pesquisador nessa tarefa: critério da raiz latente (critério de Kaiser); critério de percentagem de variância; critério do gráfico de Scree.

[10] O leitor interessado em outros métodos de extração podem consultar o Capítulo 7 de Fávero et al (2009) e o Capítulo 3 de Hair et al (2009).

O critério da raiz latente é uma técnica comumente utilizada, pois busca explicar a variância de pelo menos uma variável se a mesma há de ser mantida para interpretação. Assim, este critério indica que apenas fatores têm raízes latentes, ou autovalores (representa a quantia de variância explicada por um fator), maiores que 1 são considerados significantes. Todos os fatores com autovalores menores que 1 não são significantes e assim, descartáveis (HAIR, Jr. et al.,2009).

O critério da porcentagem de variância indica que o pesquisador deve utilizar, um valor mínimo para que o percentual de variância explicada alcance o nível satisfatório. Assim, esta porcentagem deverá indicar a quantidade de fatores a serem retidos. Hair Jr. et al. (2009) indicam que um percentual de 60% ou mais da variância é suficiente.

Já o critério do gráfico Scree consiste em definir um ponto de corte para a extração dos fatores através da observação do gráfico *Scree*. Este gráfico auxilia na seleção do número de fatores a serem extraídos por meio da plotagem dos valores da raiz latente, autovalores, no eixo vertical e o número de fatores no eixo horizontal (FÁVERO et al., 2009).

3.2.3 Método de rotação

Após a extração dos fatores, é importante que o pesquisador busque um método de rotação, pois isto torna a matriz estrutura (solução final da AFE).mais fácil de ser interpretada.

Pode-se escolher entre dois tipos de rotações: ortogonais e oblíqua. As rotações ortogonais produzem fatores que não estão correlacionados entre si e são interpretados a partir das cargas fatoriais. Já a rotação oblíqua produz fatores correlacionados e é mais realista do ponto de vista dos dados. Isto porque as dimensões inerentes que são teoricamente importantes, não são supostas sem correlações entre si (HAIR, Jr. et al., 2009).

Em um estudo comparativo entre os dois tipos de rotação, Costello e Osborne, (2005) indicam o uso da rotação obliqua *Direct Oblimin*. Conforme Fávero et al.

(2009), essa rotação preserva as comunalidades, mas, os fatores gerados apresentam-se de forma mais fortemente correlacionada.

3.2.4 Interpretação e rótulo dos fatores agrupados

Uma forma para verificar o quão bem uma variável é após a aplicação da AFE é através dos valores das comunalidades. Elas são a quantia de variância em uma variável que é explicada pelos fatores. Quanto maior a comunalidade, maior será o poder de explicação de uma variável para um dado fator (MORAES e ABIKO, 2006).

Costello e Osborne (2005) apud Velicer and Fava(1998) indicam um valor alto para comunalidade, como sendo maior que 0,8. Entretanto, nem sempre acontece em dados reais. Costello e Osborne (2005) afirmam que, em estudos sociais, valores moderados, entre 0,4 e 0,7, é o que geralmente ocorre, e assim, são aceitáveis.

Já valores inferiores a 0,4, não devem ser interpretados ou o fator não está relacionado aos outros itens ou há indícios para se explorar um fator adicional (COSTELLO e OSBORNE, 2005). Hair Jr et al. (2009) sugerem que comunalidades menores que 0,4 não sejam levadas em consideração durante a interpretação dos fatores.

Por fim, é necessário realizar a interpretação e nomeação dos fatores agrupados. Isto é feito examinando as cargas fatoriais, que são correlações entre as variáveis originais e os fatores (HAIR, Jr. et al., 2009).

Como indicado por Fávero et al. (2009), o pesquisador é quem decide quais cargas fatoriais serão consideradas na pesquisa. Entretanto, geralmente se consideram cargas fatoriais com o valor maior ou igual a 0,3 como o nível mínimo, maiores ou iguais 0,4 são consideradas importantes e maiores ou iguais a 0,5 são estatisticamente significativas (HAIR, Jr. et al., 2009).

Hair, Jr. et al. (2009) indicam, através da Tabela 6, as orientações para escolha do limiar para o valor de cargas fatoriais significantes, ao nível de 5% de significância,

com base no tamanho da amostra. Quanto maior é a carga fatorial de uma variável, maior é a contribuição da variável no agrupamento que ela pertence.

Carga fatorial	Tamanho da amostra
0,30	350
0,35	250
0,40	200
0,45	150
0,50	120
0,55	100
0,60	85
0,65	70
0,70	60
0,75	50

Tabela 6 Relação entre cargas fatoriais e tamanho da amostra, segundo (HAIR, Jr. et al., 2009).

3.3 Considerações finais

Este capítulo apresentou os principais conceitos e parâmetros estatísticos para a realização da investigação empírica com o uso do questionário e a aplicação da AF[11], na perspectiva exploratória.

[11] Leitores mais interessados nas nuanças matemáticas da AF podem consultar o capítulo 10 de Moroco (2003), o capítulo 3 de Hair Jr. (2009) e o apêndice II da tese de Camargo (1996).

Capítulo

4

Desenho do estudo

"Se o problema tem solução, não esquente a cabeça, porque tem solução. Se o problema não tem solução, não esquente a cabeça, porque não tem solução."

Provérbio Chinês

Para não ser obscuro, é bom tornar evidente que os usuários executam ações nos recursos computacionais e de redes sem que as ações estejam em concordância com a política de segurança da organização que pode ser explícita (formalmente escrita) ou implícita (não havendo o formalismo, mas subentendida na cultura da organização de forma habitual).

Ademais, este trabalho não irá procurar motivos para as ações dos usuários e nem para justificá-las. Tampouco buscará justificativas para os comportamentos dos usuários[12]. O que se quer é avaliar se os usuários do ambiente universitário conseguem perceber quais dos fatores encontrados na literatura são aqueles com carga de

[12] O leitor interessado poderá consultar Gonzalez e Sawicka (2002) sobre o entendimento dos fatores humanos na segurança da informação.

importância maior para explicar a efetividade da segurança da informação num ambiente acadêmico.

Então, foram extraídos da revisão da literatura oito fatores que descrevem a percepção dos usuários num ambiente acadêmico. A escolha dos fatores foi justificada através de estudos qualitativos e trabalhos relacionados. Assim, serão abordados os seguintes fatores:

- Apoio da administração;
- Atribuição de responsabilidade;
- Ambiente de liberdade acadêmica;
- Cultura da segurança;
- Prioridade da segurança
- Participação na segurança;
- Programas de conscientização;
- Comunicação.

Após a identificação e caracterização dos fatores, foi realizada a elaboração dos itens. Estes devem descrever aquilo que se quer avaliar nos fatores. Para cada fator há cinco perguntas que buscam ter o mesmo significado ou tem um relacionamento forte com o fator. As perguntas buscaram testar as hipóteses do trabalho (hipótese geral e as hipóteses operacionais, vide seção, 4.3 Hipóteses do trabalho). Também elas foram elaboradas visando à aplicação da análise fatorial, pois como indicado por Hill, M. e Hill, A. (2005, p. 33), "Quando o investigador está a planear (sic) o trabalho empírico, é essencial pensar na Hipótese Operacional nos métodos da investigação e nas análises de dados, em conjunto."

A validação do questionário ocorreu através da aplicação em uma pequena amostra representativa do Universo (usuários da UFRN). Na instituição UFRN há aproximadamente 40 mil usuários. Como a pesquisa sofre de restrições de tempo e

recursos financeiros, não é possível a consulta de todos os casos neste Universo. Assim, optou-se, portanto, por um Universo menor, sendo o Centro de Ensino Superior do Seridó - CERES/UFRN considerado um bom objeto de estudo. Pois nele, existem aproximadamente 2200 pessoas, entre técnicos administrativos, discentes e docentes, distribuídos em duas cidades no estado do Rio Grande do Norte, Caicó e Currais Novos. Este será o Universo a ser estudado.

Após a etapa de validação, os dados serão coletados através da aplicação do questionário *on-line*. Os convites para participação na pesquisa também foram divulgados em grupos eletrônicos de discussão e por *e-mail*.

Quando os dados coletados apresentaram significância estatística, eles foram computados e as hipóteses do trabalho testadas.

Este capítulo está organizado nas seguintes seções: 4.1 Aplicação do questionário piloto, expõe a preparação e testes do questionário; 4.2 Coleta de dados, descreve como foi realizada a coleta de dados do questionário; 4.3 Hipóteses do trabalho, indicam a hipótese geral e operacional do trabalho; 4.4 Questionário da pesquisa, descreve a estrutura das questões do questionário; 4.5 Análise dos dados quantitativos, indica como será realizado a análise dos dados após aplicação do questionário; 4.6 Considerações finais, compila e descreve as considerações finais do capítulo.

4.1 Aplicação do questionário piloto

Com o objetivo de identificar possíveis erros durante a coleta de dados, um questionário piloto foi realizado. Hill, M. e Hill, A. (2005) indicam a necessidade deste piloto para verificar a adequação dos itens e a escala de respostas utilizada no questionário.

Então, a uma pequena amostra de alunos, técnicos administrativos e professores ao questionário foi aplicado. Alguns itens utilizados no questionário de Machado (2008) precisaram ser modificados para se adequar ao vocabulário dos respondentes.

Outros itens, também de Machado (2008), foram refeitos visando acomodar a compreensão dos itens aos respondentes.

Os fatores não contemplados no estudo de Machado (2008) passaram pelo refinamento do estudo piloto, até que os respondentes não tivessem mais dúvidas sobre os itens do questionário.

Também houve uma preocupação com o tempo necessário para responder ao questionário (apesar do estudo poder ter mais fatores, limitou-se aos oito fatores por causa do tempo), itens que poderiam constranger os respondentes, ambigüidade dos itens, simplicidade nas afirmações dos itens (devido à população ter um nível intelectual bastante heterogêneo), entre outros cuidados.

O estudo piloto foi aplicado mais de uma vez até que todos os itens fossem considerados bons para a coleta de dados.

Durante a aplicação do questionário, percebeu-se a necessidade de colocar uma questão aberta visando ter uma resposta dos respondentes sobre o questionário. Então, foi incrementado mais uma pergunta ao questionário, de caráter opcional, solicitando algum comentário que se desejasse fazer sobre a pesquisa. Na Figura 3 está o item comentário no questionário *on-line*. O item comentário era o último do questionário.

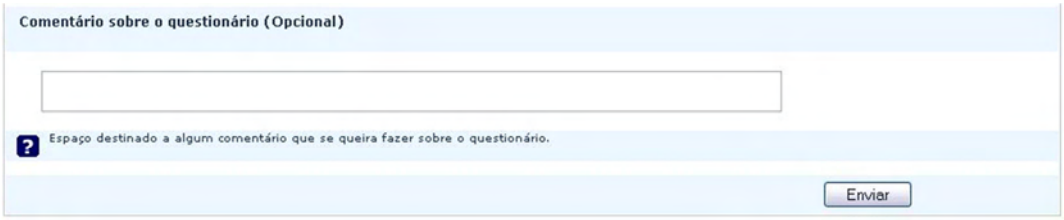

Figura 3 Pergunta aberta onde o respondente podia tecer algum comentário sobre o questionário.

4.2 Coleta de dados

O questionário foi implantado em um servidor *web*, através do Apache2[13]. Este servidor está hospedado no domínio da instituição a ser pesquisada e fornece um site contendo as informações sobre a pesquisa, onde o público alvo é convidado a participar.

Para a coleta de dados, a ferramenta LimeSurvey (2010), que proporciona a construção de pesquisas on-line, escrita em linguagem PHP, de código livre e aberto que fornece a camada de *software* entre o respondente e o banco de dados MySQL[14].

Cada grupo de itens de um fator possui uma apresentação aleatória da sequência de itens, e assim, cada respondente recebe uma ordem diferente dos itens do fator. Isto objetiva evitar o enviesamento de respostas por causa da sequência dos itens.

As ferramentas foram escolhidas por serem soluções de código aberto, livres e de aquisição sem custo para o uso, o que possibilita a instalação e a modificação das ferramentas para se adequarem as necessidades da pesquisa.

4.3 Hipóteses do trabalho

Após fazer a seleção dos fatores que descrevem a percepção da segurança da informação dos usuários no ambiente acadêmico, a segurança da informação será mensurada através de questões quantitativas. Assim, ela será medida com base na percepção (de segurança) dos usuários.

---

[13] Apache2 é um *software* de servidor web com código aberto e livre, estando disponível para *download* no site <http://httpd.apache.org/download.cgi>.

[14] MySQL é um sistema de gerenciamento de banco de dados. Este *software* possui código aberto e livre. Está disponível para *download* através do site: <http://dev.mysql.com/downloads/mysql/>

Hill, M. e Hill, A. (2005, p.25) destacam a importância da revisão da literatura, “A revisão da literatura tem por objetivo encontrar uma (ou mais) Hipóteses Gerais [abstração do que se quer alcançar na pesquisa] para a investigação empírica”. Também eles indicam que “[...] é essencial pensar na Hipótese Operacional [indica a natureza das operações estatísticas], nos métodos da investigação e nas análises de dados, em conjunto.” (HILL, M.; HILL, A., 2005, p. 33). Então, com a revisão da literatura, é possível realizar as hipóteses a serem investigadas. Sendo assim, temos:

Hipótese Geral:

HG: Dos fatores a serem investigados, há fatores que são mais determinantes para descrever a percepção do usuário sobre a segurança da informação no âmbito de uma universidade pública. Buscar-se-á identificar tais fatores através do grau de relacionamentos entre eles.

Hipótese Operacional:

HO: Dentre os fatores que mais contribuem para explicar a percepção da segurança da informação dos usuários está à participação nas atividades de segurança e o apoio da administração.

Assim, após a aplicação da análise fatorial exploratória será encontrada uma estrutura entre os oito fatores estudados. Nessa estrutura irá indicar fatores mais importantes para explicar a percepção de segurança dos usuários. Não se conhece o grau em que os dados satisfazem a estrutura esperada, por isto o caráter exploratório da pesquisa.

A hipótese operacional - HO é uma suposição do que a literatura forneceu sobre a percepção dos usuários e também a experiência pessoal acumulada na área de segurança da informação. O sucesso do estudo não é confirmar ou refutar a HO (todo estudo científico deve levantar hipóteses a serem investigadas), mas sim, investigar a segurança da informação dos usuários no âmbito acadêmico.

Assim, o **apoio da administração** tem destaque na literatura como sendo indício de fator mais determinante nos diversos tipos de organizações (MACHADO, 2008; CHANG; HO, 2006; KANKANHALLI et al., 2003). Entretanto, poucos trabalhos encontrados na literatura expõem como foco principal o estudo dos usuários, e nenhum aborda os três tipos de usuários do ambiente acadêmico, docentes, discentes e técnicos-administrativos de forma conjunta. Logo, acredita-se que o apoio da administração tenha influência grande na percepção do usuário sobre a segurança da informação no âmbito acadêmico.

Também se observa na prática da profissão de gerentes de redes que somente os usuários ativos para as questões de segurança conseguem, de fato, conduzir a instituição à efetividade da segurança, e isso somente pode ser alcançado através da **participação nas atividades de segurança** por parte dos usuários da universidade.

4.4 Questionário da pesquisa

A pesquisa foi autorizada no mês de outubro de 2010 pela direção do CERES – UFRN (vide Apêndice E). Logo após o questionário on-line foi disponibilizado no endereço eletrônico: http://www.cerescaico.ufrn.br/pesquisa/. Ele está dividido em três partes: convite, descrição do respondente e fatores da segurança da informação.

4.4.1 Convite para participação do questionário *on-line*

O convite contém as informações sobre a pesquisa, o motivo do convite, o público alvo e o contato com o pesquisador. A Figura 4 mostra o texto utilizado no convite do questionário *on-line*.

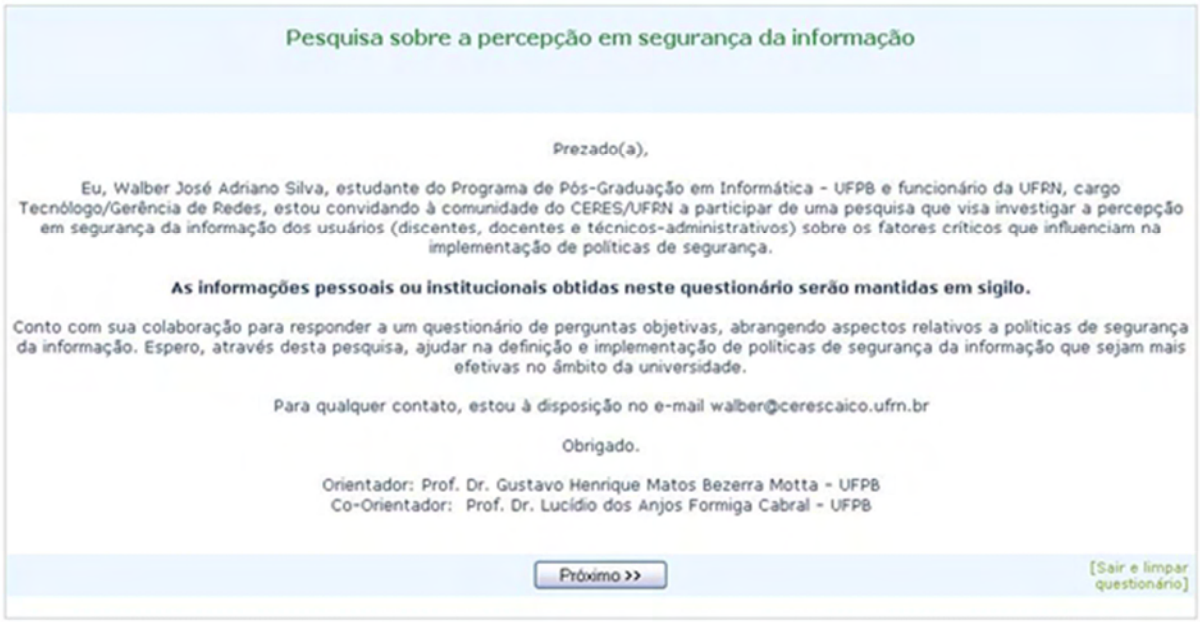

Figura 4 Convite para participação da pesquisa sobre a percepção em segurança da informação.

4.4.2 Perguntas sobre a descrição do respondente

Na parte do questionário referente à descrição dos respondentes (casos), são solicitados que eles forneçam informações sobre:

- **Instituição**
    - Opções de respostas: UFRN – CERES/Caicó, UFRN – CERES/Currais Novos, outra.
- **Há quanto tempo está vinculado à instituição (aproximadamente)**
    - Opções de respostas: Resposta aberta (com a inserção de apenas dois caracteres numéricos).
- **E-mail (Opcional)**
    - Opções de respostas: Resposta aberta (limite de 250 caracteres alfanuméricos).

- **Você possui quantos anos de idade**
    - Opções de respostas: Resposta aberta (com a inserção de apenas dois caracteres numéricos).
- **Categoria**
    - Opções de respostas: Aluno(a) – discente, Professor(a) - docente, Servidor(a) – técnico administrativo;
- **Titulação**
    - Opções de respostas: Pós-doutorado, Doutorado, Mestrado, Especialização, Graduação, Ensino Médio, Ensino Fundamental, outra.
    - Esta opção está condicionada a seleção do tipo de resposta da categoria. Caso o respondente seja docente ou técnico administrativo, o item titulação irá surgir, pois para o caso de discente já está subentendido que ele está na graduação.
- **Você possui vínculo com qual(is) curso(s)**
    - Opções de respostas: Administração, Ciências Contábeis, Direito, Geografia, História, Letras, Matemática, Pedagogia, Sistemas de Informação, Turismo, outro curso.
    - Esta opção está condicionada a seleção do tipo de resposta da categoria. Caso o respondente seja discente ou docente, o item de vínculo com o curso de graduação irá surgir. Os técnicos administrativos não respondem este item porque não é interesse da pesquisa ter ciência se eles têm ou não vínculo com um ou mais cursos e quais, pois há técnicos administrativos que nem vínculo têm com nenhum curso de graduação.
- **Sexo**
    - Opções de respostas: Feminino, Masculino.

A Figura 5 mostra a parte do questionário *on-line* referente à *descrição do respondente*.

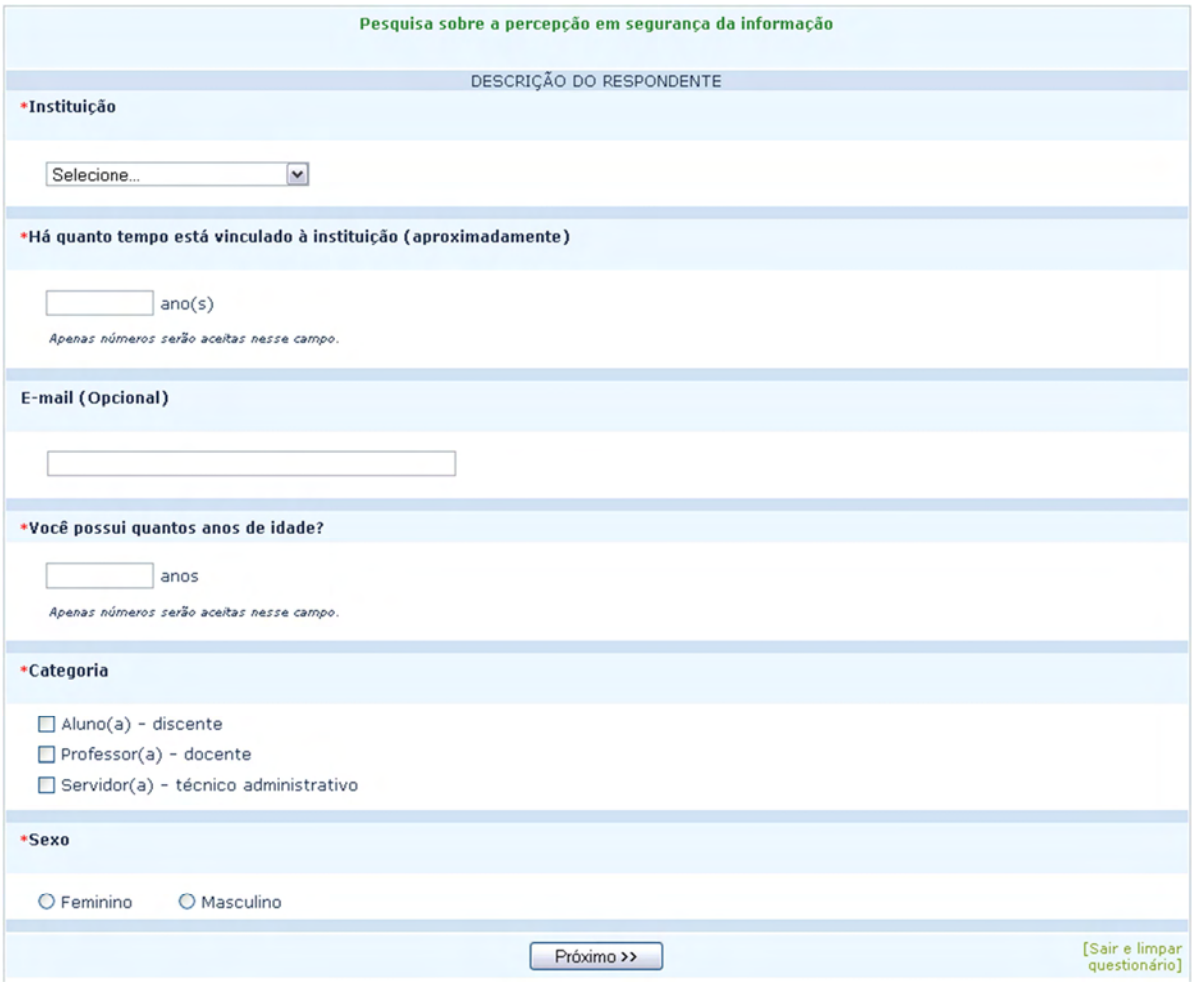

Figura 5 Parte do questionário sobre a descrição do respondente. As perguntas sobre vínculo com o curso e titulação não estão nessa figura por causa deles serem condicionados ao item sobre a categoria do respondente.

4.4.3 Itens sobre fatores da segurança da informação

Para cada fator (variáveis componentes) estudado foram elaboradas cinco afirmações. Cada afirmação será denominada, de **item** no questionário, e será usado para medir as variáveis componentes. Hill, M. e Hill, A. (2005, p. 112) destacam a importância de "[...] haver pelo menos um item e, de preferência, de 4 a 6 itens para medir cada uma das variáveis componentes". Isto é necessário para que se evite que um item mal formulado prejudique a análise de dados do fator.

Com relação aos itens, eles não são de caráter interrogativo, mas sim, afirmações que visam ser imparciais e não enviesadas para com as respostas.

As respostas terão uma escala ordinal de cinco pontos (escala de Likert) onde as respostas variam de discordo fortemente, discordo, neutro, concordo, até concordo fortemente. Como indicado por Hill, M. e Hill, A. (2005, p. 112) a escala ordinal é útil "Para analisar as respostas dadas [...] usam-se normalmente métodos paramétricos (por exemplo, [...] análises multivariadas – análise factorial)".

Antes dos usuários responderem aos fatores da pesquisa, eles são apresentados a um pequeno texto introdutório sobre o assunto: *"Segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada de informações."*.

Após este trecho é solicitado, aos usuários, o julgamento sobre as afirmações sobre cada um dos oitos fatores.

4.4.3.1 Ambiente de liberdade acadêmica

Apesar de Machado (2008) ter estudado esse fator e elaborado itens que foram validados sobre o ambiente de liberdade acadêmica, julgou-se que alguns deles não são adequados para o público alvo da presente pesquisa. Sendo assim, foi necessário elaborar e alterar alguns itens para que sejam inteligíveis aos usuários.

Além disto, visando facilitar o entendimento dos itens sobre este fator, um pequeno texto introdutório foi colocado antes de cada grupo do item. Esse texto continha: "*Liberdade acadêmica, no ambiente acadêmico, significa a averiguação e discussão de assuntos sensíveis e polêmicos, sendo o acesso à informação uma questão chave para tal. Neste sentido, mecanismos de segurança, tais como detector de intrusão e firewalls, podem ser considerados censura.*"

Logo após, os itens a serem avaliados seguiam:

- *O ambiente de liberdade acadêmica prejudica a segurança da informação da instituição.*

- *A liberdade requerida pelos usuários da instituição proporciona o mau uso dos computadores.*

- *A realização de atividades de ensino, pesquisa ou extensão devem respeitar as normas de segurança.*

- *Geralmente, medidas restritivas de segurança da informação, por exemplo, uso de senhas fortes, não são bem aceitas pela comunidade universitária.*

- *A liberdade conquistada pela comunidade universitária para realização de atividades acadêmicas é algo inquestionável e intocável. [codificação reversa]*[15]

4.4.3.2 Apoio da Administração

Por considerar que Machado (2008) elaborou e validou um questionário com o interesse em medir esta variável (conseguindo ao final do trabalho significação estatística), os itens dele serão utilizados. Entretanto, o público alvo desta pesquisa é diferente do dele. Ele teve como o público alvo da pesquisa, os responsáveis diretamente pela segurança da informação. Aqui serão estudados todos os usuários de TI no âmbito da universidade.

Por causa disto, foram feitas as devidas precauções, alterações nos itens, para que os respondentes do questionário não fiquem em dúvida no momento do preenchimento do questionário, o que implicaria o descarte do item durante a fase de análise dos dados.

---

[15] Um item com codificação reversa tem significado semântico contrário aos demais itens. Por exemplo, se um respondente atribui "concordo fortemente" para um item com codificação reversa, então para ele manter a coerência, é preciso discordar, por exemplo, assinalando "discordo fortemente" nos demais itens que não foram de codificação reversa.

Com o objetivo de definir as pessoas com função de administração na instituição, um texto introdutório foi introduzido contendo os dizeres: "*Dirigentes são professores que possuem função de chefia na instituição, por exemplo, reitor, pró-reitores, diretores de centro, chefes de departamento e outros*".

Assim, têm-se os itens:

- *Os dirigentes da universidade apóiam a elaboração das medidas de segurança nas máquinas, rede e sistemas da organização;*
- *Os dirigentes universitários consideram a segurança da informação uma importante prioridade;*
- *Os dirigentes se interessam pelos problemas relacionados à segurança da informação*[16]*;*
- *Os dirigentes se envolvem regularmente na tomada de decisão sobre questões importantes de segurança da informação;*
- *Os dirigentes levam em conta questões de segurança quando realizam o planejamento da organização*[17]*;*

Como uma última observação, neste último item foi suprimido o termo "estratégico" por considerar que esta palavra não pertence ao jargão de todos os usuários envolvidos na pesquisa.

4.4.3.3 Comunicação

Antes do grupo de itens sobre o fator comunicação, o respondente podia ler um texto que facilitasse o entendimento sobre o que se pede sobre esse fator de estu-

---

[16] Item validado no questionário da dissertação de mestrado (MACHADO, 2008).

[17] Item validado no questionário da dissertação de mestrado (MACHADO, 2008).

do. O texto diz que: "*Comunicação são as interações entre usuários da instituição: alunos, professores e funcionários*". Após este texto seguia os itens abaixo.

- *Os usuários são comunicados de maneira efetiva sobre as atuais ameaças da Internet, como por exemplo, novos vírus de computadores;*
- *Na universidade, os usuários são avisados sobre as ameaças, regras de uso, políticas e conjunto de boas práticas de segurança da informação;*
- *Não existe comunicação entre os responsáveis diretos pela segurança da informação da instituição e os usuários [codificação reversa];*
- *Os usuários são suficientemente informados sobre os problemas de segurança da informação;*
- *A instituição considera importante a divulgação de eventos que prejudiquem a segurança da informação, quando pertinente.*

4.4.3.4Cultura da segurança

Esses itens são adaptados do questionário quantitativo de Machado (2008). As mudanças feitas nos itens buscam refletir a adequação ao público alvo. E para facilitar o entendimento sobre do que se trata a cultura da segurança da informação, um texto introdutório foi introduzido antes do grupo de itens sobre este fator. O texto tinha as seguintes palavras: "*A cultura da segurança pode ser caracterizada como as atitudes e comportamentos que direta ou indiretamente afetam o ambiente da segurança da informação na organização*".

Após o texto, seguiam os itens abaixo.

- *Os usuários valorizam a importância da segurança da informação;*
- *Os usuários se queixam frequentemente das regras de segurança nos computadores da instituição. [codificação reversa]*
- *Percebe-se que existe uma cultura, na instituição, que promova as boas práticas de segurança.*

- *Os usuários têm compromisso com a segurança da informação.*
- *Os usuários são conscientes da necessidade de proteger as informações e os recursos computacionais da instituição.*

4.4.3.5 Prioridade da segurança

Um texto introdutório fornecia informações sobre o fator prioridade da segurança. O texto tinha: "*Os usuários do ambiente acadêmico desenvolvem diversas atividades que, em algum momento, demandam atividades de segurança da informação, por exemplo, localizar vírus em pendrivers".*

Após o texto, os itens sobre o fator seguiam.

- *Para os usuários, a segurança da informação é uma prioridade quando se utiliza os recursos disponíveis na universidade;*
- *Os usuários percebem a importância de proteger as máquinas da instituição contra perda de dados;*
- *Executar programas de computadores de procedência duvidosa como, por exemplo, softwares piratas, são ações que não preocupam os usuários [codificação reversa];*
- *As regras de segurança presente na universidade dificultam as atividades diárias de alunos, funcionários e professores [codificação reversa].*
- *Os usuários não veem a segurança da informação como algo importante [codificação reversa].*

4.4.3.6 Participação nas atividades de segurança

Para este conjunto de itens um texto introdutório fornecia informações sobre o fator participação nas atividades de segurança. Assim, o texto informava: "*A participação na segurança da informação descreve o envolvimento da comunidade de usuários para com a segurança da informação*". Após o texto, os itens sobre o fator seguiam.

- *Geralmente, os usuários participam na solução dos problemas de segurança, emitindo opiniões e participando de reuniões com os envolvidos diretamente com a segurança da informação;*

- *Os usuários regulam o acesso à Internet indicando o que deve ser liberado ou não, por exemplo, sites de relacionamentos ou mensageiros, como MSN.*

- *Os usuários cobram da instituição o uso seguro da rede e das máquinas que lhes estão disponíveis.*

- *A comunidade de usuários é consultada quando surge uma questão crítica de segurança.*

- *Percebe-se que os usuários participam na proteção de informações, sistemas e na rede da instituição.*

4.4.3.7 Programas de conscientização

Para facilitar o entendimento dos respondentes sobre do que se tratam os programas de conscientização, um texto introdutório foi introduzido antes do grupo de itens sobre este fator. O texto continha as seguintes palavras: "*Programas de conscientização se referem aos treinamentos apropriados em conscientização, e atualizações regulares, sobre as atividades desempenhadas pelos usuários na instituição.*" Após o texto os itens sobre o fator seguiam.

- *Os usuários recebem o devido treinamento antes de usar os sistemas da instituição.*

- *As campanhas, palestras, eventos, cartazes, entre outras ações de conscientização dos usuários são suficientes para o uso correto e seguro das máquinas e sistemas na instituição.*

- *Os usuários são orientados a lerem os avisos afixados nos laboratórios, corredores, quadros de aviso, enviados por e-mails, em folhetos e em demais locais que contenham instruções de segurança.*

- *No geral, os usuários da universidade não sabem se proteger contra os perigos da Internet [codificação reversa].*

- *Os usuários realizam as atividades acadêmicas nos sistemas da universidade sem saber muito bem com usá-los [codificação reversa].*

4.4.3.8Atribuição de Responsabilidade

Um texto introdutório fornecia informações sobre este conjunto de itens. O texto informava aos respondentes: "*Atribuição de responsabilidade se refere à obrigação da proteção de ativos, visando à prevenção de erros, uso não autorizado da informação e perda de dados.*" Após este texto os itens sobre o fator seguiam.

- *Os usuários têm responsabilidades com a segurança da informação, mesmo que a instituição possua funcionários específicos com a obrigação de proteger as máquinas da instituição.*

- *Os professores, alunos e funcionários não são responsáveis pela segurança da informação na universidade[codificação reversa].*

- *A falta de atribuição de responsabilidades explícita para os usuários é um fator problemático à segurança da informação.*

- *Atribuir responsabilidades a cada usuário contribui para que eles não comprometam a segurança da informação*

- *Cada usuário está ciente da responsabilidade no uso da rede, dos sistemas e das máquinas da universidade.*

4.5 Análise dos dados quantitativos

Os dados coletados foram analisados utilizando o *software* estatístico *Statistical Package for the Social Sciences* – SPSS, na versão de avaliação 17.0, para a plataforma do sistema operacional Microsoft Windows XP-SP3.

As hipóteses operacionais do trabalho foram testadas utilizando técnicas paramétricas (uso de parâmetros). Essas técnicas são utilizadas com o pressuposto que

os valores das variáveis possuem distribuição normal na medida de escala. Como a escala ordinal (de cinco pontos) adotada é a de Likert, Hill, M. e Hill, A. (2005) indicam a possibilidade de poder tratar os valores numéricos ligados às respostas dos itens, dessa escala, como sendo uma escala métrica, e assim, se justifica a utilização de técnicas paramétricas para análise.

Na análise, a hipótese operacional será confirmada ou refutada, através da aplicação da técnica de análise fatorial exploratória, que é uma técnica paramétrica. Ela visa explicar os fatores, variáveis componentes, através da análise das correlações entre as variáveis. Na análise fatorial, os pressupostos são distribuições relativamente normais e relações lineares entre as variáveis.

4.6 Considerações finais

Foi apresentada a metodologia utilizada para realizar a investigação sobre a percepção da segurança da informação a fim de alcançar os objetivos do trabalho. Tendo em vista a revisão da literatura e a experiência profissional em TI do pesquisador em universidades públicas, foram identificados os fatores (vide 2.4 Fatores a serem pesquisados) que influenciam a segurança da informação neste tipo de ambiente.

Assim, selecionado oito fatores (variáveis componentes) que descrevem aspectos da “Percepção da segurança da informação” (variável latente) foi criado à hipótese geral e hipótese operacional da pesquisa.

Por fim, o questionário *on-line* foi instrumento para coletar informações que validassem ou refutassem a hipótese operacional (HO) através do uso da AFE.

Capítulo

5

Resultados

> The scientist does no study nature because it is useful; he studies it because he delights in it, and he delights in it because it is beautiful. If nature were not beautiful, it would not be worth knowing, and if nature were not worth knowing, life would not be worth living.
>
> *Henri Poincaré*

O questionário foi disponibilizado para coleta de dados on-line no dia 19 de outubro de 2010 e ficou disponível até o final do mês de dezembro de 2010.

Diversos convites foram afixados nos murais do CERES, tanto na cidade de Caicó quanto na cidade de Currais Novos, solicitando a participação dos usuários na pesquisa. Um exemplo do convite divulgado está disponível no Apêndice D.

A pesquisa também foi divulgada nas salas, corredores e setores do CERES, tanto na cidade de Caicó-RN quanto em Currais Novos-RN, convidando alunos, professores e técnicos administrativos a participarem. Além disso, foram enviados *e-mails*, para listas de discussão de professores e funcionários. Na lista de discussão dos professores, solicitou que eles repassassem o convite aos alunos.

Após a coleta de dados, a pesquisa obteve um total de 122 casos válidos. Assim, estes casos disponibilizaram os valores finais da coleta de dados utilizados na pesquisa.

O restante do capítulo está organizado em: 5.1 Exclusão de registros na amostra, elucidar a motivação da retirada de alguns registros na computação da AFE; 5.2 Limitações da ferramenta para coleta de dados, expõe as falhas e limitações da ferramenta durante a coleta de dados; 5.3 Estatísticas descritivas dos casos, descreve as características dos casos; 5.4 Estatísticas indutivas, aplicação da técnica estatística multivariada da AFE, objetivando testar a hipótese operacional da pesquisa; 5.5 Comentários dos respondentes, expõe os comentários sobre o questionário baseado no item comentário; o capítulo é encerrado com a seção 5.6 Considerações finais.

5.1 Exclusão de registros na amostra

Na coleta de dados, obteve-se o total de 186 registros, dentre os quais, 123 registros são completos (ou seja, o respondente preencheu a pesquisa até o fim) e 63 incompletos (houve o interesse em começar o questionário, mas o respondente não chegou a concluí-lo). Os registros incompletos foram possíveis por causa da ferramenta de coleta de dados que gravava no banco de dados as informações das respostas à medida que o respondente ia preenchendo o questionário.

Embora fosse possível utilizar os registros incompletos para aumentar a quantidade de respostas na amostra, optou-se por excluí-los. Isto porque o questionário era anônimo e muitos dos respondentes achavam mais cômodo retornar ao questionário, para finalizá-lo, num momento oportuno.

Também é digno de nota o fato de não ser exequível disponibilizar o questionário aos usuários somente após eles passarem por algum mecanismo de autenticação, por exemplo, login e senha. Pois, isto poderia constranger os respondentes e fazer com que eles não respondessem as respostas por livre arbítrio. Assim, o questionário era anônimo (única maneira de estar disponível para milhares de pessoas) e,

retirando o item sobre *e-mail*, não havia informações dadas pelo respondente que fosse possível identificá-lo, somente com análise dos dados.

Além disso, o tempo médio de aproximadamente treze minutos para responder a todo o questionário, foi o fator limitador que desencorajava o respondente a preencher o questionário mais de uma vez.

Após a coleta dos dados, o registro de identificador (ID) 134 não foi considerado porque o respondente claramente desrespeitou a pesquisa. Isto ficou explícito na resposta aberta do item Comentário[18], onde o respondente escreveu "Só para acanalhar um pouco sua pesquisa, nem da ufrn sou". Além disso, as respostas do ID 134 foram incoerentes, pois não é possível um usuário possuir vínculo com todos os cursos do CERES-UFRN[19].

Apesar de haverem outros casos, poucos, onde é possível identificar má fé nas respostas, todos os demais casos foram introduzidos nos cálculos do estudo. Isto introduz ruídos nos valores das técnicas estatísticas utilizadas, mas garante a fidelidade na coleta dos dados e o não enviesamento da pesquisa.

Portanto, no total foram considerados úteis 122 registros completos para os fins de computação das técnicas estatísticas.

5.2 Limitações da ferramenta para coleta de dados

Como é passível de ocorrer com *softwares*, à ferramenta Limesurvey (2010) apresentou falhas durante a coleta de dados. Uma dessas falhas ocorreu na gravação dos registros no banco de dados. Para um item obrigatório, a ferramenta permitia a

---

[18] Todos os comentários introduzidos na pesquisa, através do item Comentário, estão disponíveis no Apêndice C.

[19] As normas da instituição impedem que um aluno, o id 134 respondeu que era aluno, tenha vínculo com mais de um curso.

gravação do registro do item mesmo sem ter uma resposta (ou seja, gravava uma resposta em branco). Entretanto, isto apenas aconteceu na parte do questionário referente à descrição do respondente. Nesta situação, apenas o registro de ID igual a 18 foi considerado completo, mesmo não tendo registros na parte da descrição do respondente. Os registros com falhas na parte dos fatores da segurança da informação (itens mais importantes para o objetivo final da pesquisa) foram considerados incompletos, e, portanto, descartados.

Ademais, para tornar os valores dos itens corretos para início da computação das estatísticas, foi preciso realizar uma inversão nos valores da escala para os itens de codificação reversa. Isto foi necessário devido à limitação da ferramenta que não possibilita atribuir valores diferentes da escala utilizada na matriz de respostas do questionário, ou seja, todos os itens eram codificados da mesma maneira.

Então, os itens de codificação reversa precisaram ser pré-processados de modo que refletissem os reais valores do item, antes de aplicar as técnicas estatísticas. Então, um item de codificação reversa que receberá o valor x de um respondente deverá ter valor 6 – x, assim[20]:

$$Valor\_do\_item = 6 - Valor\_do\_item$$

Equação 1 Pré-processamento dos valores recebidos pelos itens de codificação reversa

Desta maneira, os valores dos itens de codificação reversa terão os valores finais da Tabela 7, para fins de computação dos dados.

[20] O valor seis se refere à soma do intervalo utilizado na escala, ou seja, o valor inicial, que é um, e o valor final, que é cinco.

Valor da resposta de um item, com codificação reversa.	Pré-processamento dos itens de codificação reversa	Valor final do item de codificação reversa.
1	6 – 1	5
2	6 – 2	4
3	6 – 3	3
4	6 – 4	2
5	6 – 5	1

Tabela 7 Representação do pré-processamento para os itens de codificação reversa com uso da Equação 1.

Os itens do questionário que tiveram pré-processamento, devido à codificação reversa, são representados pelas variáveis (vide Apêndice A, onde se encontra o relacionamento entre as variáveis e os itens): AMBI5, COMU3, CULT2, PRIO3, PRIO4, CONS4, CONS5 e RESP2. A Tabela 22 do Apêndice B ilustra o pré-processamento dos itens através da Equação 1. E as saídas dos comandos de execução do pré-processamento no *software* SPSS, sobre os itens de codificação reversa, podem ser encontradas na Tabela 23, também do Apêndice B.

5.3 Estatísticas descritivas dos casos

No total, foram 122 registros completos válidos obtidos no período em que o questionário esteve disponível ao acesso. As próximas seções mostram as estatísticas básicas dos casos relativas à parte do questionário sobre a descrição do respondente.

5.3.1 Participação na instituição

A maior parte dos respondentes se consideram associados à cidade de Caicó-RN, com cerca de 88% dos respondentes, e correspondem ao total de 108 casos. Esta alta parcela foi causada pela divulgação, do questionário *on-line*, ter sido mais intensa no CERES da cidade de Caicó-RN. Na cidade de Currais Novos-RN, obteve-se 9 casos, ou 7,38% dos respondentes da pesquisa.

Apenas 2 casos responderam que eram da UFRN em Natal. Outros 3 casos marcaram outros, entretanto, dois deles não preencheram o campo com uma resposta (ficando a resposta vazia) e o outro é o ID 18, que teve o registro da parte da descrição do respondente não preenchida no banco de dados (falha no *software* de coleta de dados). As porcentagens e os números de casos sobre o local da instituição na qual os respondentes se denominam associados pode ser analisado no Gráfico 1.

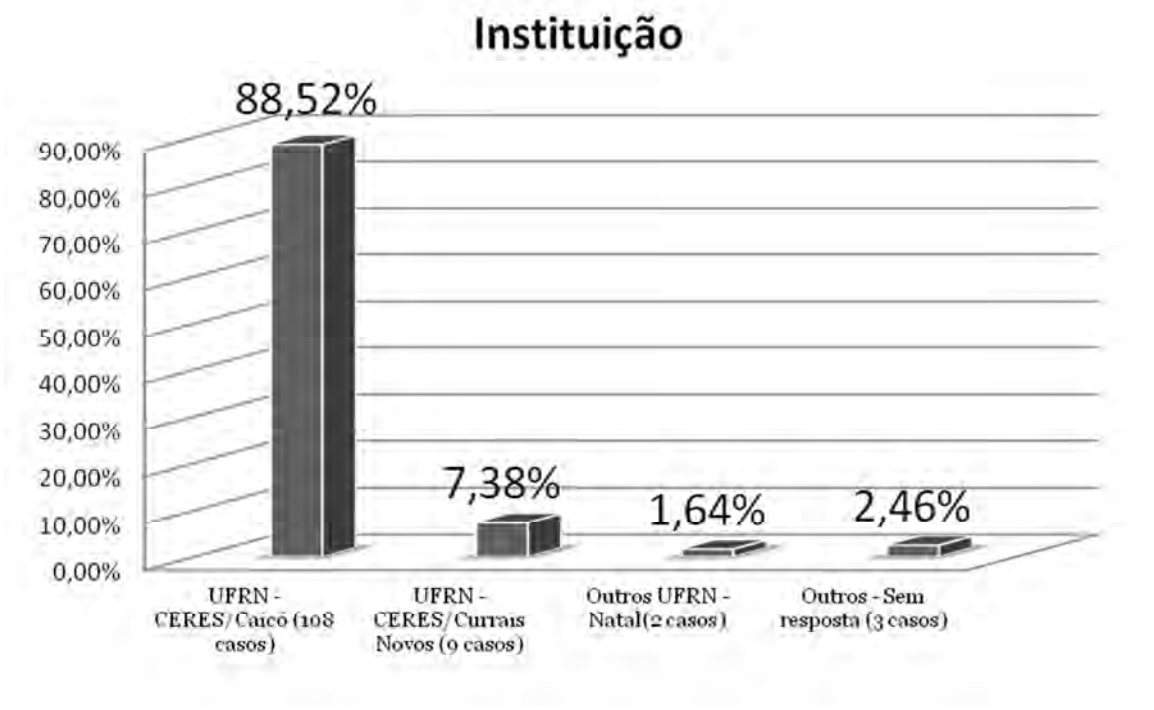

Gráfico 1 Porcentagens das cidades da UFRN que responderam ao questionário.

5.3.2 Tempo de vínculo com a instituição

O Gráfico 2 mostra a distribuição do tempo de vínculo dos respondentes para com o CERES-UFRN. Como é possível observar, a maior parte dos respondentes possui 5 anos ou menos de tempo vinculado à instituição.

Gráfico 2 Distribuição do tempo de vínculos dos respondentes com a instituição.

5.3.3 E-mail

A situação ideal seria utilizar apenas os casos nos quais o respondente introduziu o *e-mail* (este item era opcional devido ao fato do questionário ser anônimo) no campo do item *e-mail*. Pois, parte-se do princípio de que as pessoas que confiaram na salvaguarda dos dados da pesquisa, empenharam-se em fazer uma reflexão mais séria sobre os itens.

Entretanto, não é exequível uma análise fatorial com 66 casos (vide o número de casos com resposta no Gráfico 3), por causa do tamanho pequeno da amostra. Sendo assim, é importante a junção dos casos com e sem respostas, para o item e-mail, na realização da análise fatorial. Para este item 66 casos, ou 54,10%, responderam ao campo e-mail enquanto 56 casos, ou 45,90%, optaram por deixá-lo em branco.

Gráfico 3 Quantidade e porcentagem dos casos completos que responderam o item e-mail.

5.3.4 Idade

Como indica o Gráfico 4, a maior parte dos respondentes tem menos de 30 anos. Este fato decorre da maioria dos respondentes serem discentes. A distribuição das idades dos respondentes pode ser encontrada no Gráfico 4.

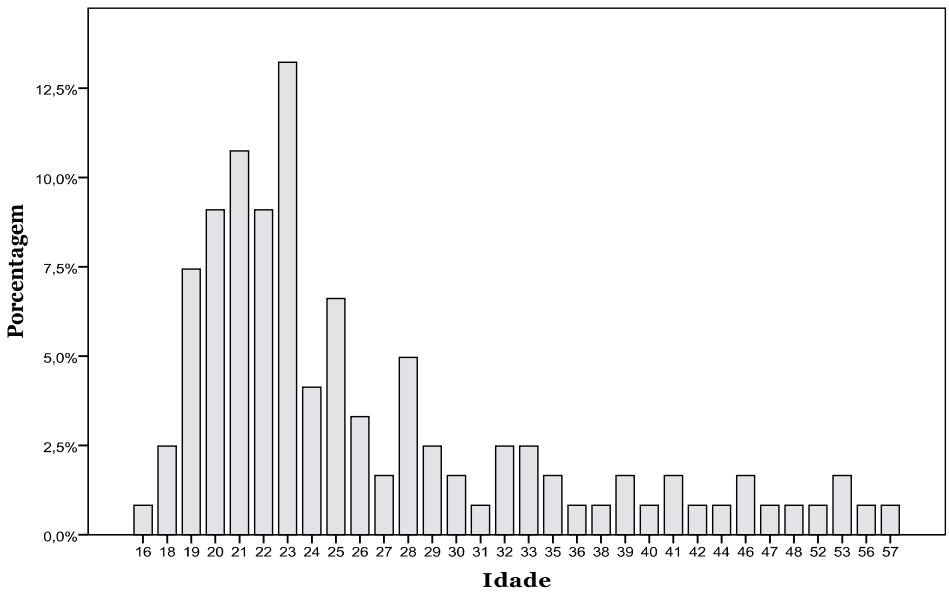

Gráfico 4 Distribuição de idades dos casos.

5.3.5 Categoria

Apesar dos respondentes terem a opção de escolha de um das três categorias discentes, docentes e técnicos administrativos, uma ou mais das categorias poderiam ser selecionadas (já era previsto). Sendo assim, o Gráfico 5 mostra a porcentagem e número dos casos da categoria dos respondentes.

Foram 9 casos, ou 7%, dos casos compostos por técnicos administrativos, 23 casos, ou 19%, são docentes e 89 casos, 73% dos respondentes, são do corpo discente. Apenas 1 caso, é aluno e técnico-administrativo, totalizando aproximadamente 1% dos respondentes.

Gráfico 5 Categorias dos casos.

5.3.6 Titulação

Pela lógica de apresentação atribuída aos itens no questionário *on-line* na ferramenta de coleta de dados, a titulação apenas era mostrada para as categorias de docentes e técnico administrativos.

O Gráfico 6 apresenta 0,82% dos respondentes possui o titulo de Pós-doutorado, com 1 caso. Ademais, são 6 casos com titulação de Doutorado, 4,92% dos casos, 14 casos declarados com titulação de mestre, correspondendo a 11,48% dos casos. Aqueles com nível titulação mais alta sendo a especialização são 6 casos, ou 4,92% dos casos, que possuem graduação 3 casos, ou 2,46% e 3 casos tem a titulação máxima o ensino médio. Não houve respondentes que possuíam apenas ensino fundamental, ou seja, 0,0% de casos.

Gráfico 6 Distribuição da titulação nos casos. Observação: os 89 casos “Não mostrados” indicados no gráfico significam os alunos que estão na graduação (titulação graduando), pois as regras de apresentação, na coleta de dados, somente apresentavam este item para aqueles respondentes que não eram discentes.

Por fim, no Gráfico 6, os 89 casos nos quais este item não foi apresentado aos respondentes, correspondem às respostas da categoria de discentes, e, portanto, graduandos.

5.3.7 Associações entre os casos e os cursos

As associações buscaram coletar informações de quais cursos o respondente possui algum vínculo. Como um usuário pode possuir vínculos com mais de um curso, por exemplo, um professor do curso de Sistemas de Informação que também leciona nas turmas de Matemática, o número de associações excede o número de respondentes.

Assim, o Gráfico 7 indica que no total foram 130 associações entre os respondentes e os cursos. Os cursos com maior vínculo entre os respondentes foram o curso de Sistemas de Informação (29 associações), o de Geografia (23 associações), o de História (19 associações) e o de Matemática (19 associações). Os demais números podem ser consultados no Gráfico 7. Só para constar, não houve respondentes com vínculo no curso de Turismo e os outros cursos foram Engenharia Civil e Ciências e Tecnologia da UFRN da cidade de Natal-RN.

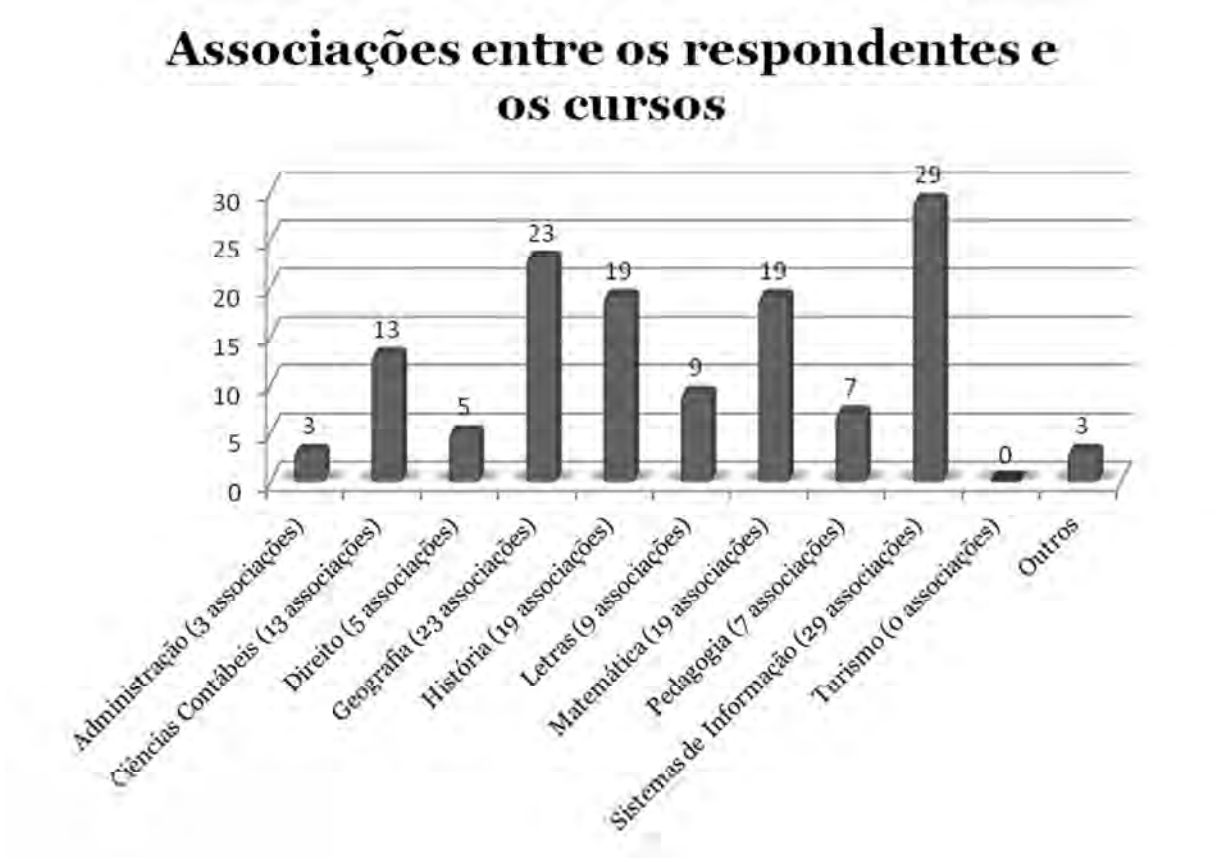

Gráfico 7 Associações entre os respondentes e os cursos. Observação: o número de associações é maior do que o número de casos, pois um respondente pode possuir mais de um vínculo com os cursos da instituição.

5.3.8 Sexo

No item sexo, 61% dos casos responderam ser do sexo masculino, o que representa 75 casos. Respondentes do sexo feminino foram 46 casos, 38 % dos casos. O caso de id 18 entrou na computação dos dados, mesmo não tendo informações na parte do questionário sobre a descrição do respondente. Por isso, ele é o 1% restante dos casos, e não tem resposta para este item. O Gráfico 8 ilustra esses dados.

Gráfico 8 Porcentagem dos casos do sexo feminino e masculino. O caso "Sem resposta", no gráfico, ocorreu devido a uma falha, excepcional, no software de coleta de dados.

5.4 Estatísticas indutivas

Nesta seção serão apresentadas as estatísticas indutivas utilizando a análise fatorial, na perspectiva exploratória.

5.4.1 Confiabilidade interna

O alfa de Cronbach é um mecanismo utilizado para testar a confiabilidade interna dos itens. Ele tem as seguintes premissas: os itens descrevem um mesmo aspecto; os itens devem ser respondidos por uma amostra heterogênea (se as respostas forem muito parecidas o alfa será próximo de zero); a escala utilizada já deve estar validada.

No Apêndice G encontram-se as computações do alfa de Cronbach para todos os quarenta itens do questionário *on-line*. Por causa de alguns dos itens não terem atingidos confiabilidade interna acima de 0,6, optou-se por utilizar apenas duas variáveis para cada conjunto de cinco variáveis pesquisadas. Elas, as variáveis, são selecionadas de forma a maximizar o alfa de Cronbach e possuírem maior correlação.

Assim, a Tabela 8 resume os itens que tornam o conjunto de variáveis com confiabilidade interna e estão mais correlacionadas[21].

Variáveis indicadoras selecionadas	Alfa de Cronbach	Correlação
AMBI1 e AMBI2	0,638	0,598
ADMI3 e ADMI4	0,859	0,638
COMU1 e COMU4	0,711	0,672
CULT4 e CULT5	0,648	0,699
PRIO1 e PRIO2	0,655	0,695
PART1 e PART4	0,769	0,612
CONS4 e CONS5	0,738	0,587
RESP3 e RESP4	0,661	0,485

Tabela 8 Variáveis que maximizam o valor do alfa de Cronbach e que estão mais correlacionadas.

Após o cálculo do alfa de Cronbach, ficaram 16 variáveis, com confiabilidade interna para 122 casos. Portanto, tem-se uma taxa de 7,6 casos para cada variável indicadora (item).

5.4.2 Adequação do uso da análise fatorial

Para analisar a viabilidade da AF, foram realizados os cálculos do KMO e o teste de Bartlett. Os resultados são apresentados na Tabela 9. O KMO foi 0,667, e pela recomendação relativa à realização da AF, (recomendação para realização da AF com relação ao KMO, no capítulo de fundamentação teórica), indica que a continuidade da AF no estudo é razoável e portanto, aceitável de ser realizada.

[21] O leitor pode consultar o Apêndice G para ter ciência de como se chegou a tal resultado.

Já o teste de Bartlett (Sig = 0,000, último valor da segunda coluna da Tabela 9), é menor do que 0,05, e também indica a presença de correlações entre as variáveis em estudo, pois rejeita a hipótese da matriz de correlações ser a matriz identidade. Portanto, a AF é passível de ser executada sobre os dados coletados.

Kaiser-Meyer-Olkin Medida de adequação da amostra		0,667
Teste de Bartlett	Aprox. Chi-Square	734,936
	DF	120
	Sig.	0,000

Tabela 9 Valores do KMO e teste de Bartlett.

A Tabela 10 representa a matriz anti-imagem para as correlações. Ela contém os valores das medidas de adequação da amostra, ou MSA, na diagonal principal.

	ADMI3	ADMI4	AMBI1	AMBI2	PRIO1	PRIO2	CULT4	CULT5	PART4	PART1	CONS5	CONS4	RESP3	RESP4	COMU1	COMU4
ADMI3	,662	-,611	-,015	,147	,009	-,202	-,048	,031	-,187	,123	,090	-,141	,037	,059	-,355	,120
ADMI4	-,611	,574	,014	-,038	,079	,035	-,010	,020	,130	-,213	-,117	,082	-,100	-,071	,202	-,170
AMBI1	-,015	,014	,546	-,576	-,202	,101	,245	-,028	-,275	,030	-,082	-,079	-,104	-,094	-,030	,015
AMBI2	,147	-,038	-,576	,568	,104	,026	-,175	,095	,117	-,007	-,063	,208	-,087	,096	-,139	-,036
PRIO1	,009	,079	-,202	,104	,752	-,544	-,173	-,115	-,020	-,075	,100	-,042	,068	-,074	-,039	,106
PRIO2	-,202	,035	,101	,026	-,544	,761	-,110	-,133	,077	-,014	-,180	,070	-,139	,028	,168	-,201
CULT4	-,048	-,010	,245	-,175	-,173	-,110	,787	-,492	,005	-,104	-,065	-,035	,113	-,172	-,081	,018
CULT5	,031	,020	-,028	,095	-,115	-,133	-,492	,835	,010	,043	-,033	-,063	-,008	-,014	-,003	-,099
PART4	-,187	,130	-,275	,117	-,020	,077	,005	,010	,603	-,555	,005	,085	-,006	-,086	,099	-,203
PART1	,123	-,213	,030	-,007	-,075	-,014	-,104	,043	-,555	,686	,050	-,067	,121	,089	-,136	,007
CONS5	,090	-,117	-,082	-,063	,100	-,180	-,065	-,033	,005	,050	,589	-,553	,208	,090	-,170	,205
CONS4	-,141	,082	-,079	,208	-,042	,070	-,035	-,063	,085	-,067	-,553	,623	-,147	,100	,156	-,201
RESP3	,037	-,100	-,104	-,087	,068	-,139	,113	-,008	-,006	,121	,208	-,147	,559	-,435	-,089	,104
RESP4	,059	-,071	-,094	,096	-,074	,028	-,172	-,014	-,086	,089	,090	,100	-,435	,557	-,074	,121
COMU1	-,355	,202	-,030	-,139	-,039	,168	-,081	-,003	,099	-,136	-,170	,156	-,089	-,074	,602	-,614
COMU4	,120	-,170	,015	-,036	,106	-,201	,018	-,099	-,203	,007	,205	-,201	,104	,121	-,614	,657

Tabela 10 Matriz anti-imagem contendo as correlações para os 16 itens. A diagonal principal da matriz indica os valores do MSA.

O MSA quantifica o grau de correlações entre as variáveis e assume um valor entre 0 e 1, alcançando o valor 1 quando a variável é perfeitamente prevista sem erro pelas outras variáveis do modelo (HAIR Jr. et al., 2009).

Valores do MSA abaixo de 0,5 não são aceitáveis para AF (como indica a Tabela 5, índice da MSA no capítulo de fundamentação teórica). Todas as 16 variáveis possuem valores de MSA maiores que 0,5, e logo, são todas adequadas para AF.

5.4.3 Número de fatores a extrair

A aplicação do método de extração da máxima verossimilhança, para extração dos fatores, requer que os valores coletados para cada item sigam uma distribuição normal. Os gráficos dessa distribuição, para cada um dos 16 itens, estão no Apêndice F.

Na Tabela 11, estão os valores dos autovalores para cada fator, assim como os percentuais de variância compartilhada.

Fator	Autovalor	% da variância	Acumulado %
1	**4,062**	**25,388**	**25,388**
2	**2,375**	**14,843**	**40,231**
3	**1,786**	**11,164**	**51,395**
4	**1,367**	**8,542**	**59,937**
5	**1,255**	**7,842**	**67,779**
6	**1,030**	**6,437**	**74,217**
7	0,807	5,041	79,258
8	0,638	3,986	83,243
9	0,495	3,091	86,334
10	0,446	2,788	89,122
11	0,389	2,429	91,551
12	0,362	2,261	93,813
13	0,321	2,004	95,817
14	0,262	1,637	97,453
15	0,231	1,446	98,899
16	0,176	1,101	100,000

Tabela 11 Autovalores e percentual de variância explicada pelos fatores.

Utilizando o critério da raiz latente na identificação de fatores que tem autovalores maiores que 1, o critério indica a extração de 6 fatores (coluna **Autovalores-**

Total da Tabela 11). O critério de percentagem de variância confirma a retenção de seis fatores. A retirada de seis fatores explicam 74,217% da variância nos dados originais (coluna Acumulado % da Tabela 11).

Além da variância compartilhada indicar o número de fatores a serem extraídos na amostra, ela é um indicativo do quão expressivo cada fator é. Assim, na Tabela 11, a coluna **% de variância** indica que o primeiro fator compartilha aproximadamente 25% da variância nos dados, bem mais do que o segundo fator, com quase 15% de variância. E este decaimento da quantidade de porcentagem de variância continua até a extração dos seis fatores.

Para ratificar a retenção de seis fatores, o Gráfico 9 corrobora com a Tabela 11, onde há seis fatores com autovalores maiores do que 1.

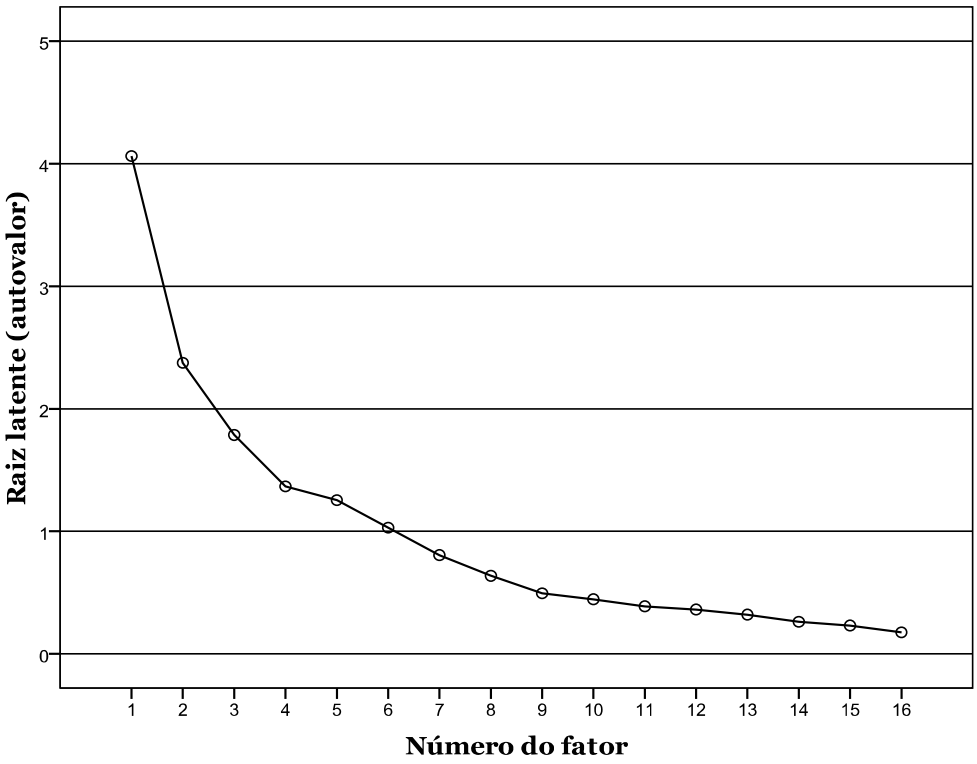

Gráfico 9 Gráfico de Scree do autovalor para o critério da raiz latente, extraindo 6 fatores (autovalores maiores que 1).

5.4.4 Interpretação e rótulo dos fatores agrupados

As comunalidades são a quantia de variância em que uma variável é explicada pelos fatores. Quanto maior a comunalidade, maior será o poder de explicação de uma variável para o fator. Assim, na Tabela 12 há os valores das comunalidades antes e depois no método de extração máxima verossimilhança.

	Inicial	**Após a extração**
ADMI3	,583	,999
ADMI4	,470	,424
AMBI1	,507	,999
AMBI2	,475	,427
PRIO1	,570	,648
PRIO2	,617	,668
CULT4	,603	,595
CULT5	,554	,568
PART4	,489	,588
PART1	,474	,700
CONS5	,446	,667
CONS4	,449	,500
RESP3	,346	,206
RESP4	,330	,211
COMU1	,572	,998
COMU4	,570	,519

Tabela 12 Comunalidades dos itens. O método de extração utilizado foi Maximum Likelihood.

O nível aceitável para a comunalidade utilizado foi >0,4 (vide Capítulo 2 – Fundamentação Teórica). Apenas duas variáveis RESP3 e RESP4 não atingiram este nível e assim, não tem explicação suficiente para um fator. Elas não serão interpretadas na solução final da análise fatorial exploratória. Todas as demais variáveis possuem forte relação com os fatores retidos, pois têm elevadas comunalidades, como mostra a coluna **Após a extração** da Tabela 12. Após o método de extração de fatores máxima verossimilhança, foram retidos seis fatores dos dados. Para facilitar a interpretação dos fatores, o método de rotação oblíqua *Direct Oblimin* foi aplicado. O resultado compõe a matriz estrutura, solução da pesquisa, na Tabela 13. Nela estão os 6

fatores e suas cargas fatoriais que explicam a percepção da segurança da informação para cada fator.

Matriz estrutura - Solução da pesquisa

Variáveis	Fatores					
	1	2	3	4	5	6
ADMI3	,993	-,087	,379	,330	,222	-,144
ADMI4	,644	-,069	,194	,148	,220	-,114
AMBI1	-,026	,980	,120	-,120	,152	,162
AMBI2	-,168	,612	,158	-,203	,004	,190
COMU1	,320	,175	,994	,184	,263	-,049
COMU4	,300	,043	,687	,251	,383	-,132
PRIO2	,344	-,160	,153	,804	,069	-,178
PRIO1	,224	-,002	,145	,796	,128	-,054
CULT4	,266	-,212	,275	,739	,144	-,206
CULT5	,218	-,154	,223	,737	,086	-,214
PART1	,256	-,024	,365	,187	,822	-,151
PART4	,264	,188	,303	,090	,728	,015
CONS5	,140	-,083	,135	,247	,023	-,782
CONS4	,226	-,142	,098	,285	,075	-,667
RESP3	-,018	,288	-,038	-,016	-,203	,371
RESP4	,001	,195	-,008	,161	-,118	,385

Tabela 13 Matriz estrutura, solução final da AFE, com as cargas fatoriais após a aplicação da análise fatorial sobre os 16 itens. As variáveis estão agrupadas nos seis fatores. As variáveis RESP3 e RESP4 não serão interpretadas. O método de extração e o método de rotação foram máxima verossimilhança e *Direct Oblimin*, respectivamente.

O primeiro fator, apoio da administração, é explicado pelas variáveis ADMI3 e ADMI4, contribuem com cargas fatoriais 0,993 e 0,644, respectivamente (Tabela 13). Essas variáveis estão associadas à percepção da segurança da informação. Como ambas variáveis são do fator apoio da administração, este agrupamento terá o mesmo nome.

O segundo fator, ambiente de liberdade acadêmica, é explicado pelas duas variáveis AMBI1 e AMBI2. A primeira possui maior carga fatorial, com 0,980 e tem maior contribuição para explicar o fator. A segunda, tem 0,612 de carga fatorial. Ambas estão associadas com a percepção da segurança da informação na instituição em

estudo (Tabela 13). Como ambas variáveis são do fator ambiente de liberdade acadêmica, este agrupamento esse nome.

O terceiro fator, comunicação, tem maior contribuição da variável COMU1, que possui 0,994 de carga fatorial. Seguido pela variável COMU4 com 0,687 de carga fatorial. Ambas as variáveis estão associadas com a percepção da segurança da informação (Tabela 13). Como ambas variáveis são do fator comunicação, este agrupamento terá esse nome.

O quarto fator, prioridade e cultura da segurança, é explicado por quatro variáveis PRIO2, PRIO1, CULT4 e CUT5. Elas possuem, nesta ordem, cargas fatoriais de 0,804, 0,796, 0,739 e 0,737. Todas as quatro variáveis estão associadas com a percepção da segurança da informação (Tabela 13). Como as variáveis são do fator prioridade da segurança e cultura da segurança, um novo rótulo definindo este fator é criado baseado nas cargas fatoriais. Então, este agrupamento terá o nome de prioridade e cultura da segurança.

O quinto fator, participação na segurança, recebe as contribuições de duas variáveis para explicar o fator. A primeira variável PART1 tem carga fatorial 0,822 e a segunda, PART4, possui carga fatorial 0,728. E ambas, estão associadas com a percepção da segurança da informação (Tabela 13). Como ambas variáveis são do fator participação na segurança, este agrupamento terá o mesmo nome.

O último e sexto fator, indicado pela análise fatorial é rotulado por programas de conscientização e responsabilidade da segurança. A variável que mais explicar o fator é a CONS5 e CONS4, com cargas fatoriais -0,782 e -0,667, respectivamente. As variáveis RESP3 e RESP4 estão associadas a este fator, entretanto, como recomendação da relação entre cargas fatoriais e tamanho da amostra (vide Tabela 6, capítulo 3) o tamanho da amostra é aproximadamente 120 casos o que implica numa carga fatorial no mínimo maior ou igual a 0,5. Portanto, as cargas fatoriais de RESP3 e RESP4, 0,371 e 0,385, respectivamente não são significantes para explicar o fator. Como as variáveis são do fator programas de conscientização para a segurança, este agrupamento terá o mesmo nome.

Então, de acordo com os resultados da análise fatorial exploratória, a hipótese geral HG foi alcançada, ou seja, realmente há fatores que são mais determinantes para descrever a percepção do usuário sobre a segurança da informação no âmbito de uma universidade pública. Também a hipótese operacional da pesquisa HO foi atendida, e assim, o fator que mais contribuem para explicar da percepção da segurança da informação é o apoio da administração. O fator participação nas atividades de segurança também contribui para explicar essa percepção.

5.5 Comentários dos respondentes

Após a apresentação do resultado final da pesquisa, é interessante saber quais foram os comentários emitidos pelos respondentes durante a aplicação do questionário. Isto foi feito através do item comentário.

Este item, opcional, era uma forma dos respondentes expressarem algum comentário sobre o questionário *on-line*. O conteúdo dos comentários foram indagações, elogios, importância do trabalho e reflexões sobre o assunto segurança da informação.

Abaixo alguns comentários ratificam a necessidade e reflexão da segurança da informação na instituição:

- ***"[...] mas friso aqui a devida importâcia (sic) do mesmo [questionário on-line] para procedimentos de segurança futuros para instituições de ensino."***
- ***"Acho que a parte que indaga sobre a concientização (sic) dos usuários deveria vir em primeiro lugar, visto que esta é o maior desafio de nosso tempo. No mais, ficou muito bom, precisamos de mais dessas![omitido]"***
- ***"De todas as questões abordadas, uma das principais é da educação dos usuarios (sic), torná-los conscientes do que pode vir a acontecer com os dados delas."***

- ***"O assunto Segurança da Informação deveria ser mais debatido dentro da universidade. E tendo como foco um dos principais elos da segurança que são as pessoas. Não adianta sistemas robustos na parte de segurança, se os usuários não fazem o uso devido do mesmo."***

- ***"Toda e qualquer barreira ao conhecimento é burra! E por muitas vezes os usuários não tem acesso de complementos para o ensino e para a pesquisa."***

- ***"Há alguns sites que são bloqueados, mais isso não deveria ocorrer, pois são através destes que muitos alunos baixam conteúdos acadêmicos, como também se comunicam com outras pessoas, ato que é de fundamental importância no mundo globalizado no qual atualmente estamos inseridos."***

- ***"Muito bom para o ceres [CERES] pensar em mecanismos e uma política de para que deixe a comunidade acadêmica ciente de suas responsabilidades, sobretudo fazer esse trabalho no inicio do período letivo, que são quando os calouros entram na istituição (sic). [omitido]"***

- ***"A propria (sic) universidade usa software piratas, quem somos nós para para (sic) usa apenas softwares verdadeiros?[...]"***

Outras sobre como foi elaborado, a metodologia, sugestões, reclamações e elogios do questionário *on-line*:

- ***"De fato senti com relação a algumas questões dificuldades, mas o questionário foi bem elaborado."***

- ***"O questionário poderia abrir espaço para questões discursivas."***

- ***"Penso que, em várias afirmativas, a percepção do elaborador sobre os temas estaria transparecendo de forma bastante evidente para influenciar a opção do entrevistado. Em certos casos, nos quais eu não sou neutro, também não era contra nem a favor do problema posto nos***

termos da afirmativa: nesses casos,parece-me que faltou objetividade na formulação da afirmativa."

- ***"O quesitonário (sic) é constituído apenas por um tipo de questão. Isso o torna estafante! Além disso, por vezes, as questões confundem o raciocínio do respondente."***
- ***"NÃO GOSTEI DO QUESTIONÁRIO, PODERIA SER ALGO MAIS SIMPLES,DIRETO E OBJETIVO."***
- ***"Algumas questões senti dificuldade de responder por não entender muito do asunto (sic) de segurança da informação. para mim está ligado só a vírus, portanto no decorrer do questionário observei que muito amplo esta questão. Espero ter contibuido (sic)."***
- ***"O questionário em alguns momentos ficou confuso. As perguntas eram feitas para "os usuários" e não para "o usuário" que responde as questões, o que deixa um problema para a objetividade da resposta. Respostas que demandam de quem responde o conhecimento ou opinião sobre o que todo o conjunto de usuários pode achar genericamnete (sic) ou respostas que seriam a opinião do usuário-individuo (sic) que responde o questionários, respondendo por ele mesmo."***
- ***"Os questionamentos feitos requerem respostas que generalizem o público alvo (os usuários do sistema acadêmico como um todo), quando na verdade em parte das indagações só conseguiria responder por mim, por isso muitas vezes minha resposta foi neutra."***
- ***"[omitido] parabéns por sua pesquisa. Que ela contribua para o aumento da segurança da informação em toda a comunidade acadêmica."***

O restante dos comentários, do item comentário, pode ser encontrado no Apêndice C.

5.6 Considerações finais

Neste capítulo foram apresentadas as principais dificuldades enfrentadas durante a pesquisa. A exclusão de registros na amostra e as limitações da ferramenta de coleta de dados. No total, 122 casos foram utilizados na pesquisa, onde se apresentou as estatísticas básicas dos casos.

Na realização da análise estatística indutiva se usou a análise fatorial numa perspectiva exploratória, através do método de máxima verossimilhança e rotação oblíqua. Esse método traz o grau de importância de cada fator, na explicação do problema proposto, proporcionado pelos autovalores associados a cada fator e pelos percentuais da variação total explicada por cada fator.

Assim, tem-se o primeiro fator “Apoio da administração”, segundo fator “Ambiente de liberdade acadêmica”, terceiro fator “Comunicação”, quarto fator “Prioridade e cultura da segurança”, quinto fator “Participação na segurança”, sexto fator “Programas de conscientização e responsabilidade da segurança”.

Também foi confirmada a hipótese operacional HO, com os achados do apoio da administração e participação na segurança como fatores mais importantes para explicar a percepção da efetividade da segurança da informação.

Por fim, foram apresentados os comentários dos respondentes sobre o questionário *on-line* sobre percepção da segurança da informação.

Capítulo

6

Discussão

> "O homem que não sabe expressar seus pensamentos está no mesmo nível daquele que não sabe pensar."
>
> *Benjamin Franklin*

Este estudo representa uma continuidade das pesquisas em segurança da informação, em especial no ambiente universitário. Entretanto, essa investigação se tornou genuína por ser um estudo voltado para todos os usuários de TI de uma universidade pública do país sobre a percepção da efetividade da segurança da informação.

Neste capítulo, será realizada uma reflexão sobre os resultados obtidos na investigação empírica. Na seção 6.1 Otimização na obtenção de casos, há o relato de como o questionário *on-line* foi reestruturado para obter mais casos; 6.2 Discussão sobre a amostra, caracteriza o perfil dos respondentes para os resultados obtidos; 6.3 Interpretação dos fatores, discussão sobre os fatores mais importantes para explicar a percepção da segurança da informação, de acordo com o resultado da análise fatorial exploratória; 6.4 Os resultados da AFE e as normas internacionais de segurança, confronta os seis fatores encontrados no estudo com as normas de segurança; 6.5 Limita-

ções do estudo, indica as limitações da pesquisa; O capítulo termina com a seção 6.6 Considerações finais.

6.1 Otimização na obtenção de casos

A ferramenta LimeSurvey (2010) permite a visualização dos dados assim que são coletados. Isto permitiu verificar o quão bem estava sendo a coleta dos dados. Entretanto, nos primeiros dias verificou-se a quantidade de usuários que acessavam o questionário, mas não concluía, era maior do que os que preenchiam todo o questionário. Assim, optou-se por reestruturar a apresentação do questionário *on-line*, mas deixando-o com o mesmo conteúdo.

O questionário inicialmente era composto por três partes: o convite para pesquisa, a caracterização do respondente, e a investigação dos fatores. Nesta última parte do questionário contém 40 itens a serem avaliados (8 fatores, com 5 itens cada). Percebeu-se que as respostas, mais da metade dos usuários chegavam até a investigação dos fatores, mas não continuava, ou seja, não concluíam a pesquisa.

Com este problema, optou-se por destrinchar a última parte do questionário em oito, e assim, contemplar cada fator separadamente, reestruturando o questionário. Então, ele ficou com 10 partes: o convite, a descrição do respondente, e 8 partes uma para cada conjunto de 5 itens que aborda um fator específico da pesquisa. Esta modificação otimizou a quantidade de casos completos, o que possibilitou atingir o número de casos necessários para a pesquisa.

Na fase de aplicação do piloto o objetivo principal era verificar dificuldades no conteúdo do questionário, e essa característica, a apresentação do questionário, emergiu durante a coleta de dados.

Portanto, o resultado da pesquisa contém respostas de dois tipos de questionários, com o mesmo valor semântico, porém organizado de maneira diferente.

6.2 Discussão sobre a amostra

A receptividade com o questionário foi satisfatória. Entretanto, a quantidade de itens a serem respondidos acabou limitando o número de respondentes. Esta dificuldade pode ser comprovada pela resposta do respondente de id 038 “Um pouco grande, mas se é pelo bem da informação ... tá legal” e do respondente de id 066 “muito grande rsrsrs” (vide Apêndice C, item comentário do questionário *on-line*)

Estando o CERES localizado em duas cidades do interior do Rio Grande do Norte, Caicó e Currais Novos, separadas por uma distância de aproximadamente 100 Km, a divulgação do questionário de maneira presencial na cidade de Currais Novos não foi tão eficiente. Isto se refletiu na quantidade de casos na amostra, apenas nove casos referentes à cidade de Currais Novos-RN. Com 108 casos associados à cidade de Caicó, pode-se concluir que a amostra contém majoritariamente respondentes desta localidade.

Além disso, a maior parte deles possui pouco tempo de vínculo com a instituição, cinco anos ou menos (Gráfico 2). Ademais, a faixa etária dominante na amostra é até os trinta anos de idade (Gráfico 4), e a categoria, quase um quarto dos casos, são declarados como discentes (Gráfico 5). Por causa disto, a titulação mais presente na amostra é a graduando. E os cursos em que os respondentes indicaram estar associados têm um perfil tecnológico, como os cursos de Sistemas de Informação, Geografia e Matemática. Por fim, mais de 60% dos casos são de respondentes do sexo masculino.

É válido lembrar que a pesquisa foi divulgada como um convite (Apêndice D), não obrigando nenhum usuário a fazê-la. Aqueles que alocaram seu tempo para participar da pesquisa fizeram porque, de alguma maneira, assim quiseram.

6.3 Interpretação dos fatores

Nesta seção, será discutido sobre os fatores mais relevantes para explicar a percepção da segurança da informação, de acordo com a análise fatorial realizada.

6.3.1 Fator 1 – Apoio da Administração

A pesquisa empírica realizada no âmbito do CERES revela que o apoio da administração, indicado pela análise fatorial, tem maior influência para explicar a percepção da segurança da informação. As pesquisas encontradas na literatura também apresentam o apoio da administração como fator de grande influência na percepção da segurança da informação, como Machado (2008) no ambiente acadêmico e Chang e Ho (2006) e Knapp et al. (2005) voltados para o ambiente empresarial.

O item que mais explica o fator apoio da administração é a variável ADMI3[22] (vide Tabela 13), com a seguinte afirmação (Gráfico 10):

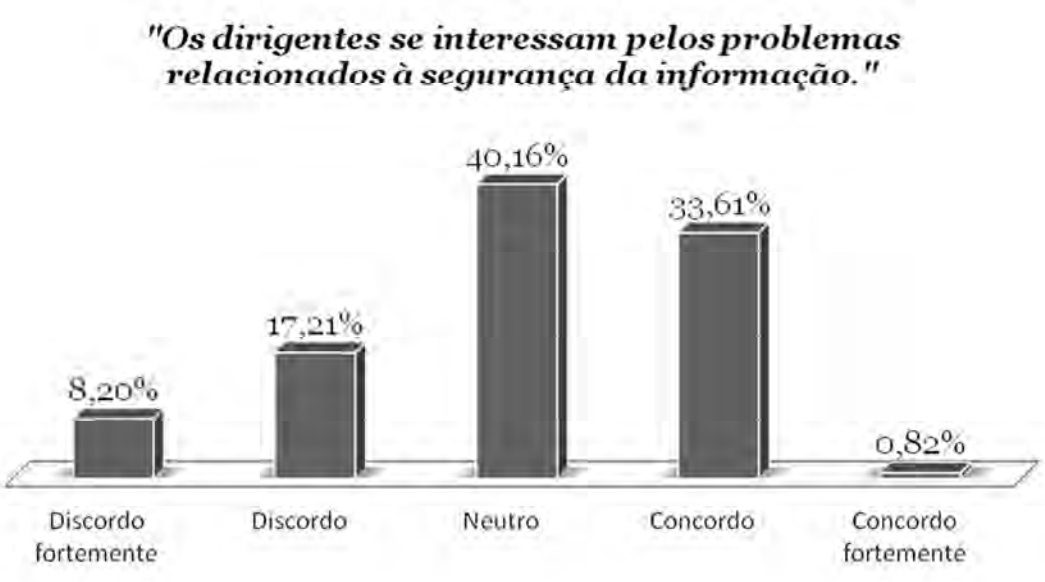

Gráfico 10 Representação gráfica da variável ADMI3 (apoio da administração).

Onde, 8,20% dos respondentes discordam fortemente, 17,21% discordam, 40,16% ficaram neutros, 33,61% concordam e 0,82% concordaram (num total de

[22] O Apêndice A fornece a codificação das variáveis utilizados no SPSS e os itens do questionário.

34,43% de concordância) fortemente com a afirmação. Então, a maioria dos respondentes preferiu ser neutros com relação a esta afirmação.

A outra variável ADMI4, na Tabela 13, que compõe a variável apoio da administração, possui a seguinte afirmação (Gráfico 11):

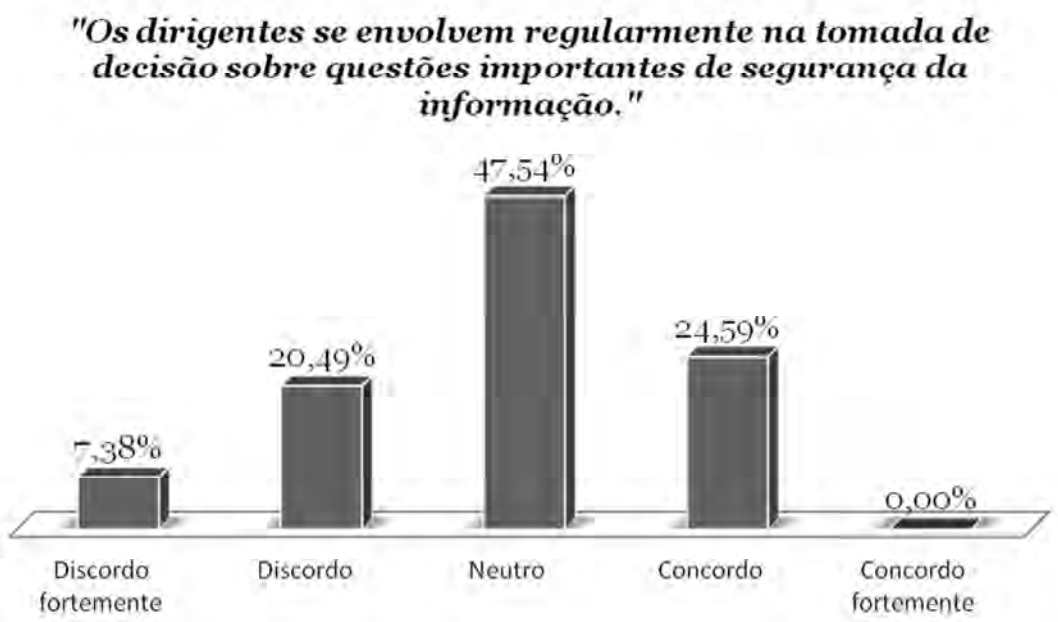

Gráfico 11 Representação gráfica do item ADMI4 (apoio da administração).

Dos respondentes, 7,38% discordam fortemente, 20,49% discordam (um total de 27,87% de discordância), 47,54% ficaram neutros e 24,59% concordam com a afirmação. Assim, a maioria dos respondentes optou por serem neutros com relação à afirmação.

6.3.2 Fator 2 – Ambiente de liberdade acadêmica

Este é o segundo fator que, segundo a análise fatorial, explica a percepção da segurança da informação. Machado (2008) estava na direção correta quando indicou o apoio da administração e o ambiente liberal (ambiente de liberdade acadêmica) na universidade como fatores mais marcantes para explicar a percepção de segurança

dos usuários. Entretanto, ele não conseguiu confirmar ou rejeitar essa hipótese devido à falta de significância estatística.

No item comentário, do questionário *on-line*, este fator foi referenciado pelo ID 082:

"Toda e qualquer barreira ao conhecimento é burra! E por muitas vezes os usuários não tem acesso de complementos para o ensino e para a pesquisa." – ID 082.

Outro comentário a este fator foi exposto pelo respondente de ID 087. Ele também indica o controle de acesso a *sites* como uma barreira para liberdade acadêmica:

"Há alguns sites que são bloqueados, mais (sic) isso não deveria ocorrer, pois são através destes que muitos alunos baixam conteúdos acadêmicos, como também se comunicam com outras pessoas, ato que é de fundamental importância no mundo globalizado no qual atualmente estamos inseridos." – ID 087.

Apesar dos usuários do ambiente acadêmico necessitarem da liberdade para realizar suas atividades, neste tipo de organização, algum controle deve ser implementando. Isto é preciso para proteger a infraestrutura de computadores e rede da instituição, além de prevenir a organização contra processos judiciais.

Assim, a variável AMBI1, na Tabela 13, é um dos itens selecionados para medir a variável componente ambiente de liberdade acadêmica através da seguinte afirmação (Gráfico 12):

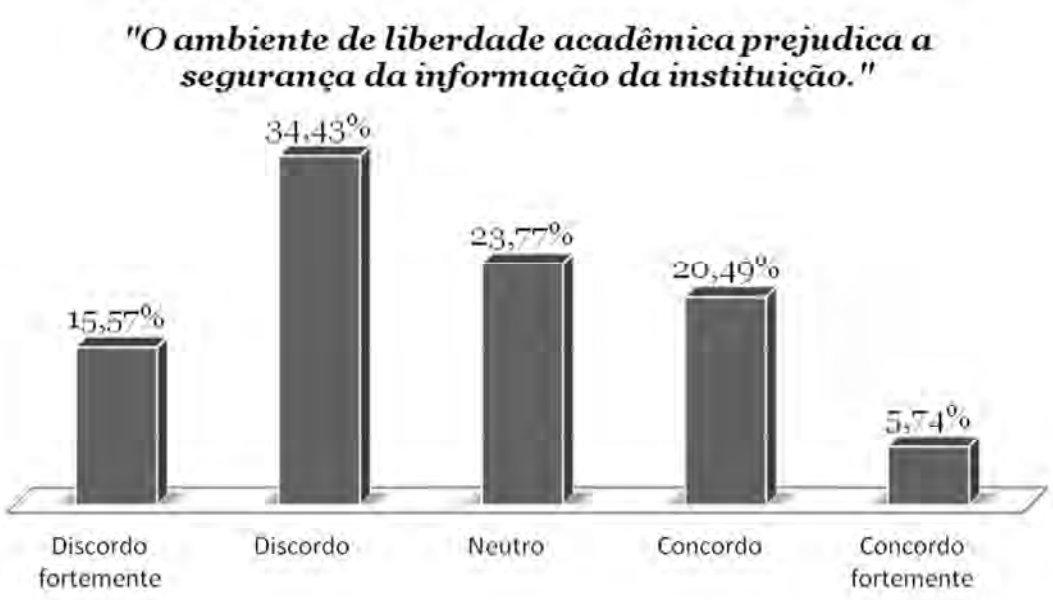

Gráfico 12 Representação gráfica do item AMBI1 (Ambiente de liberdade acadêmica).

Onde, 15,57% discordam fortemente, 34,43% discordam (um total de 50% de discordância), 23,77% são neutros, 20,49% concordam e 5,74% concordam fortemente com a afirmação. Ou seja, a maioria dos respondentes discorda que o ambiente de liberdade acadêmica prejudica a segurança da informação.

Outra variável AMBI2, na Tabela 13, é um dos itens selecionados para medir a variável componente ambiente de liberdade acadêmica através da seguinte afirmação (Gráfico 13):

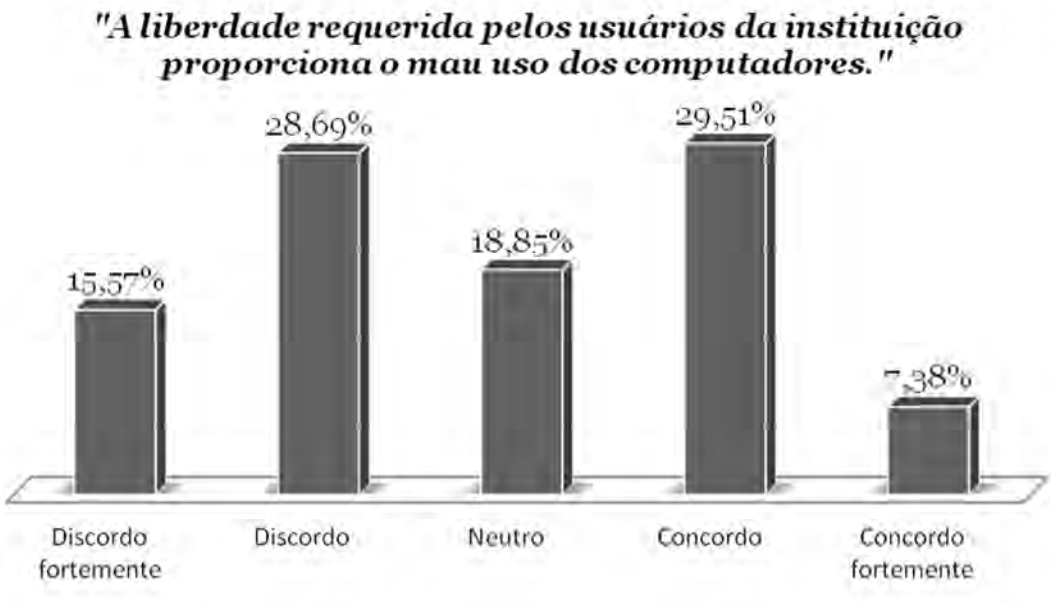

Gráfico 13 Representação gráfica do item AMBI2.

Onde, 15,57% discordam fortemente, 28,69% discordam (um total de 44,26% de discordância), 18,85% são neutros, 29,51% concordam e 7,38% concordam fortemente com a afirmação. Assim, pelo ponto de vista dos respondentes, a maioria discorda que a liberdade requerida pelos usuários da instituição proporciona o mau uso dos computadores.

6.3.3 Fator 3 – Comunicação

Kraemer e Carayon (2007) definem comunicação como sendo as interações entre os membros da instituição. Eles apontam que a comunicação é um dos fatores organizacionais que, quando falha, causa vulnerabilidades de segurança. Assim, ela, a comunicação, é o terceiro fator que, segundo a análise fatorial, explica a percepção da segurança da informação.

A variável COMU1 na Tabela 13 é um dos itens selecionados para medir a variável componente comunicação com a seguinte afirmação (Gráfico 14):

Gráfico 14 Representação gráfica do item COMU1.

Onde, 21,31% discordam fortemente, 37,70% discordam (um total de 59,01% de discordância), 22,13% são neutros, 15,57% concordam e 3,28% concordam fortemente com a afirmação. Dessa forma, os usuários não consideram serem comunicados sobre as atuais ameaças advindas do acesso externo, no caso a Internet.

Outra variável COMU4 na Tabela 13 é um dos itens selecionados para medir a variável componente comunicação com a seguinte afirmação (Gráfico 15):

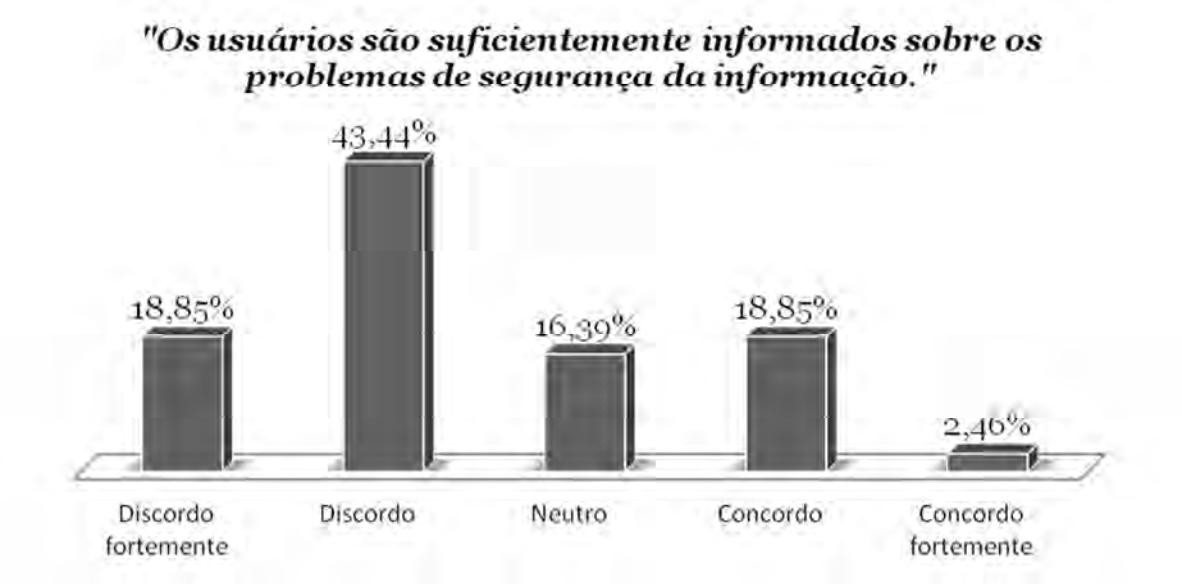

Gráfico 15 Representação gráfica do item COMU4.

Onde, 18,85% discordam fortemente, 43,44% discordam (um total de 62,29% de discordância), 16,39% são neutros, 18,85% concordam e 2,46% concordam fortemente com a afirmação. Portanto, os usuários discordam que estão sendo suficientemente informados sobre os problemas de segurança da informação. Albrechtsen (2006) indica que a baixa habilidade dos usuários em lidar com a segurança da informação é explicado pela falta de comunicação dos profissionais em segurança em fornecer informações sobre o correto comportamento dos usuários. Assim, é possível que isto também esteja acontecendo com os usuários da instituição estudada.

6.3.4 Fator 4 – Prioridade e cultura da segurança

No quarto fator, prioridade e cultura da segurança, as variáveis que se destacaram foram sobre a prioridade da segurança da informação, seguidas pela cultura da segurança, todos associados com a percepção da efetividade da segurança da informação.

Desta maneira, existe uma relação entre a prioridade da segurança e a cultura da segurança. Uma interpretação para isto é se os usuários não percebam a priorida-

de da segurança no ambiente acadêmico eles não irão, através de atitudes e comportamentos, propagar uma cultura para com a segurança da informação na organização.

Um comentário do respondente de identificador –ID 133, corrobora com este achado, e indica a percepção que o respondente tem sobre a prioridade da segurança na instituição e questiona como a cultura da segurança está sendo afetada:

"A propria (sic) universidade usa software piratas, quem somos nós para para (sic) usa apenas softwares verdadeiros?[...]" – ID 133.

Além disso, a variável PRIO2 na Tabela 13 é um dos itens selecionados para medir a variável componente prioridade da segurança com a seguinte afirmação (Gráfico 16):

Gráfico 16 Representação gráfica do item PRIO2.

Onde, 9,84% discordam fortemente, 28,69% discordam (um total de 38,53% de discordância), 22,13% são neutros, 32,79% concordam e 6,56% concordam fortemente (um total de 39,35% de concordância) com a afirmação. Apesar da análise fatorial, em caráter exploratório, indicar este item como mais importante para explicar este fator, os graus de discordância e concordância estão muito próximos, não sendo

possível indicar se os usuários percebem a importância de proteger as máquinas da instituição contra perda de dados.

Outra variável PRIO1 na Tabela 13 é um dos itens selecionados para medir a variável componente prioridade da segurança com a seguinte afirmação (Gráfico 17):

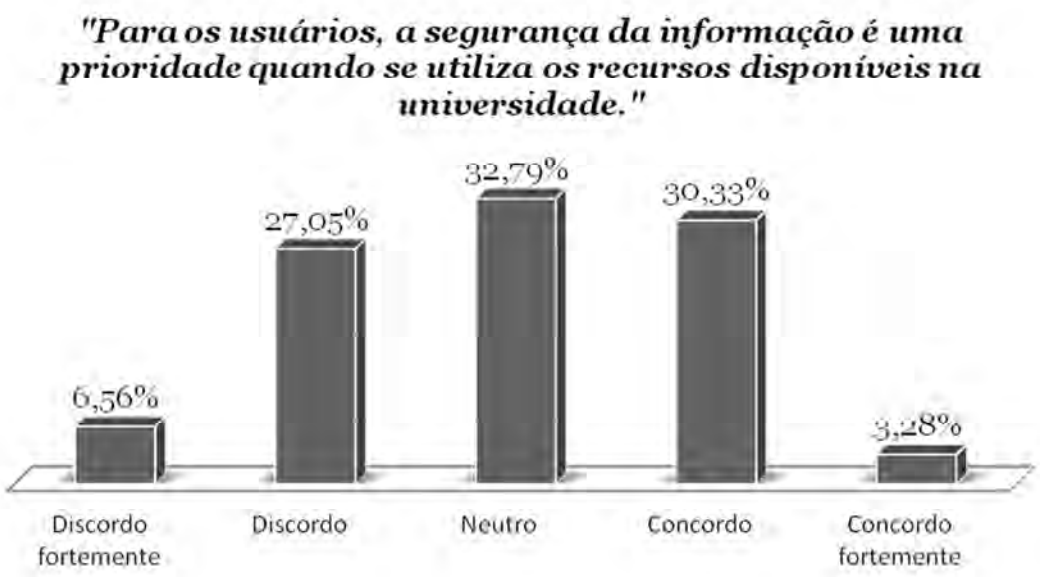

Gráfico 17 Representação gráfica do item PRIO1.

Onde, 6,56% discordam fortemente, 27,05% discordam (um total de 33,61% de discordância), 32,79% são neutros, 30,33% concordam e 3,28% concordam fortemente (um total de 33,61% de concordância) com a afirmação. Também através desta variável não é possível indicar se os usuários percebem que a segurança da informação é uma prioridade quando se utiliza os recursos disponíveis na universidade, pois os graus de concordância e discordância são iguais, ou seja, exatamente 33,61%. Além disto, a alternativa de resposta **neutro** obteve o maior número de respondentes.

A variável CULT4 na Tabela 13 é um dos itens selecionados para medir a variável componente cultura da segurança com a seguinte afirmação (Gráfico 18):

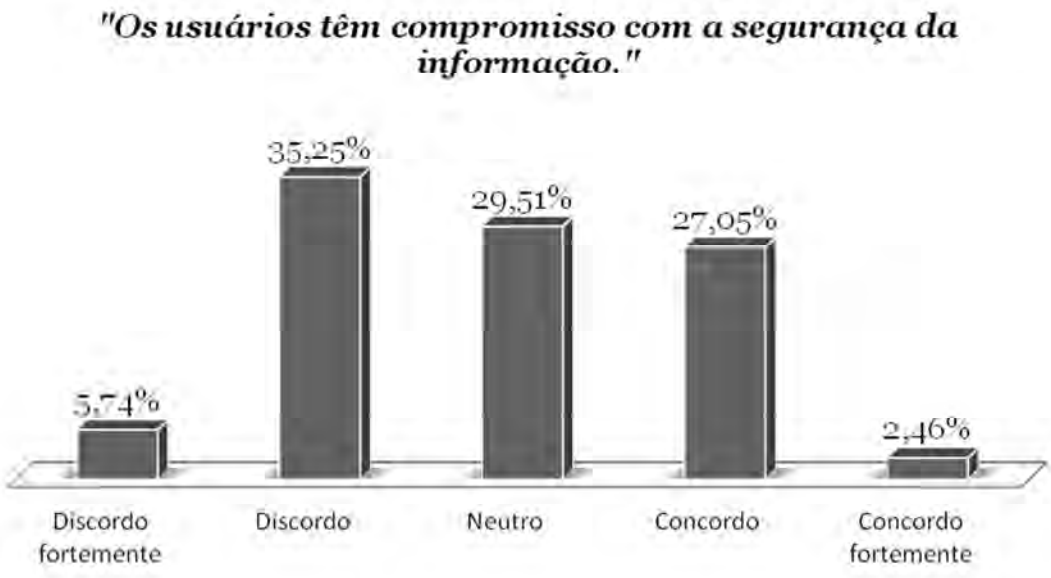

Gráfico 18 Representação gráfica do item CULT4.

Onde, 5,74% discordam fortemente, 35,25% discordam (um total de 40,99% de discordância), 29,51% são neutros, 27,05% concordam e 2,46% concordam fortemente com a afirmação. Através desta variável, é possível indicar que a maioria dos usuários discorda que os usuários têm compromisso com a segurança da informação.

Outra variável CULT5 na Tabela 13 é um dos itens selecionados para medir a variável componente cultura da segurança com a seguinte afirmação (Gráfico 19):

Gráfico 19 Representação gráfica do item CULT5.

Onde, 7,38% discordam fortemente, 28,69% discordam, 22,95% são neutros, 35,25% concordam e 5,74% concordam fortemente (um total de 40,99% de concordância) com a afirmação. Apesar da grande parte dos usuários indicarem que os demais usuários são conscientes da necessidade de proteger as informações e os recursos computacionais da instituição, com 40,99% de concordância, também há uma grande parte que discorda com a afirmação, 36,07%. E, portanto, não é possível inferir a concordância ou discordância dos usuários sobre esta variável.

6.3.5 Fator 5 – Participação na segurança

Como indicado no estudo de Albrechtsen (2006), os usuários possuem um papel importante na realização da segurança da informação. E geralmente, uma abordagem que os envolva, tornando-os mais conscientes com relação à importância da segurança da informação, é um meio para alcançar a efetividade da segurança da informação.

Um comentário referente a este fator, feito por um dos respondentes do questionário, identificado com ID 039, corrobora com a literatura:

“O assunto Segurança da Informação deveria ser mais debatido dentro da universidade. E tendo como foco um dos principais elos da segurança que são as pessoas. Não adianta sistemas robustos na parte de segurança, se os usuários não fazem o uso devido do mesmo.” – ID 039.

Ademais, a variável PART1 na Tabela 13 é um dos itens selecionados para medir a variável componente participação na segurança com a seguinte afirmação (Gráfico 20):

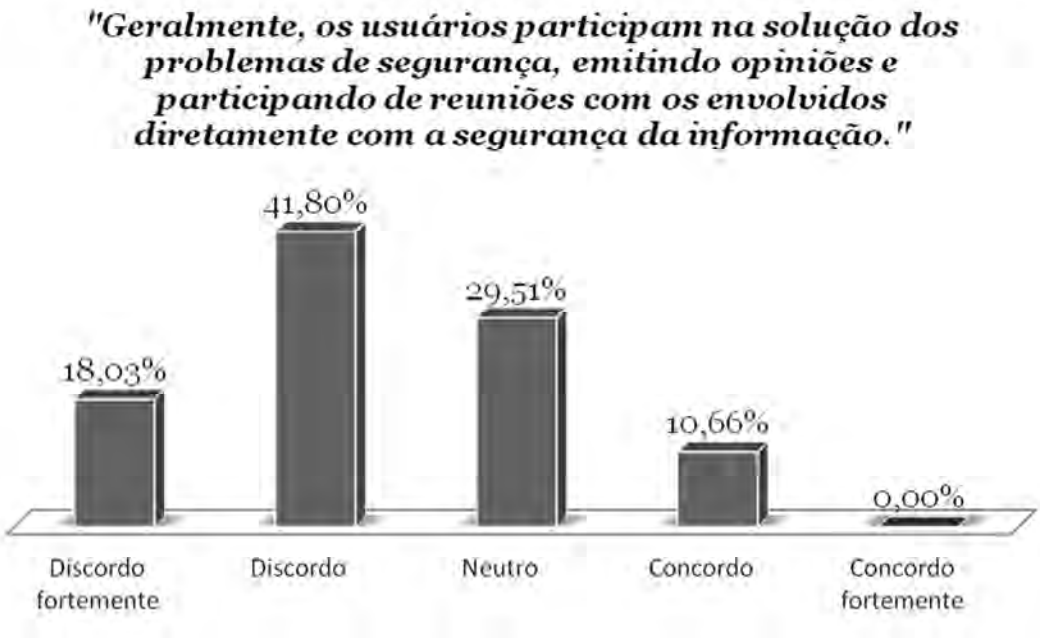

Gráfico 20 Representação gráfica do item PART1.

Onde, 18,03% discordam fortemente, 41,80% discordam (um total de 59,83% de discordância), 29,51% são neutros, 10,66% concordam com a afirmação. Assim, com uma grande maioria que discorda com a afirmação, torna-se enfático a necessidade de envolver os usuários da instituição a participarem na solução dos problemas de segurança.

Outra variável PART4, na Tabela 13, é, também, um dos itens selecionados para medir a variável componente participação na segurança com a seguinte afirmação (Gráfico 21):

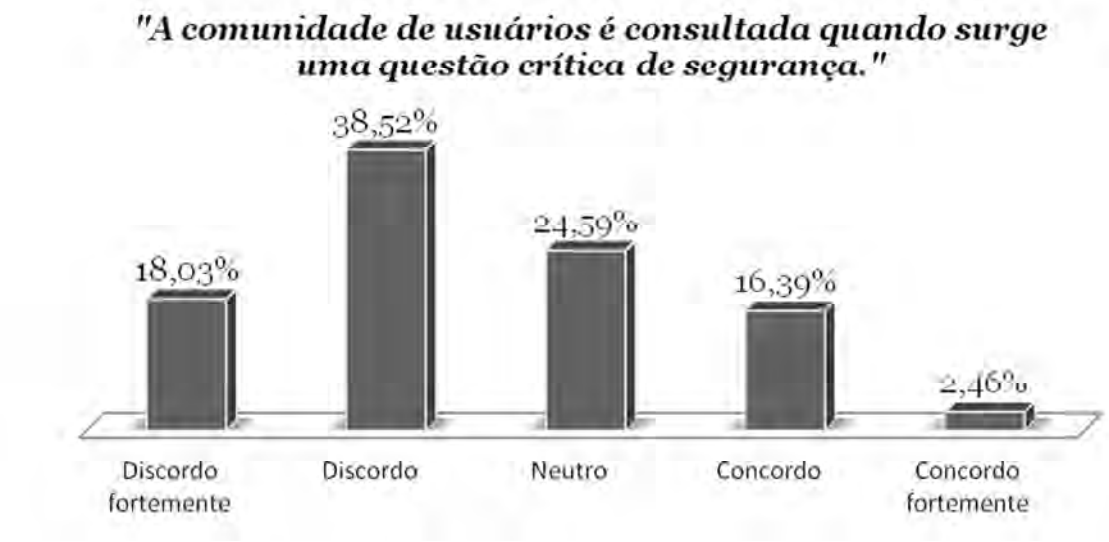

Gráfico 21 Representação gráfica do item PART4.

Onde, 18,03% discordam fortemente, 38,52% discordam (um total de 56,55% de discordância), 24,59% são neutros, 16,39% concordam e 2,46% concordam fortemente com a afirmação. Novamente, a maioria dos usuários da instituição discorda que eles são consultados quando questões críticas de segurança surgem.

6.3.6 Fator 6 – Programas de conscientização para a segurança.

A segurança da informação enfrenta desafios práticos dentro das organizações como indicado por Werlinger, Hawkey e Beznosov (2009). Um esforço internacional para confrontar tais desafios, reside nas normas internacionais de segurança da informação. Entretanto, elas são abrangentes e dificilmente uma organização irá cobrir todas as lacunas de segurança existentes. Uma dessas lacunas são os programas de conscientização para a segurança da informação e a responsabilidade de segurança da informação dos usuários.

Alguns comentários dos usuários, que corroboram com este fator:

“Muito bom para o ceres pensar em mecanismos e uma política de para que deixe a comunidade acadêmica ciente de suas responsabilida-

des, sobretudo fazer esse trabalho no inicio do período letivo, que são quando os calouros entram na istituição (sic). [omitido]" – ID 094;

"Algumas questões senti dificuldade de responder por não entender muito do asunto (sic) de segurança da informação. para mim está ligado só a vírus, portanto no decorrer do questionário observei que muito amplo esta questão. [...]" – ID 129;

"De todas as questões abordadas, uma das principais é da educação dos usuarios (sic), torná-los conscientes do que pode vir a acontecer com os dados delas." – ID 013;

"Acho que a parte que indaga sobre a concientização (sic) dos usuários deveria vir em primeiro lugar, visto que esta é o maior desafio de nosso tempo. No mais, ficou muito bom, precisamos de mais dessas![omitido]" – ID 018;

Este fator foi o que mais recebeu comentários dos usuários. Isto indica a necessidade da instituição em questionar a efetividade dos programas de conscientização e a responsabilidade da segurança da informação para seus usuários.

Ademais, a variável CONS5, na Tabela 13, é um dos itens selecionados para medir a variável componente programas de conscientização com a seguinte afirmação (Gráfico 22):

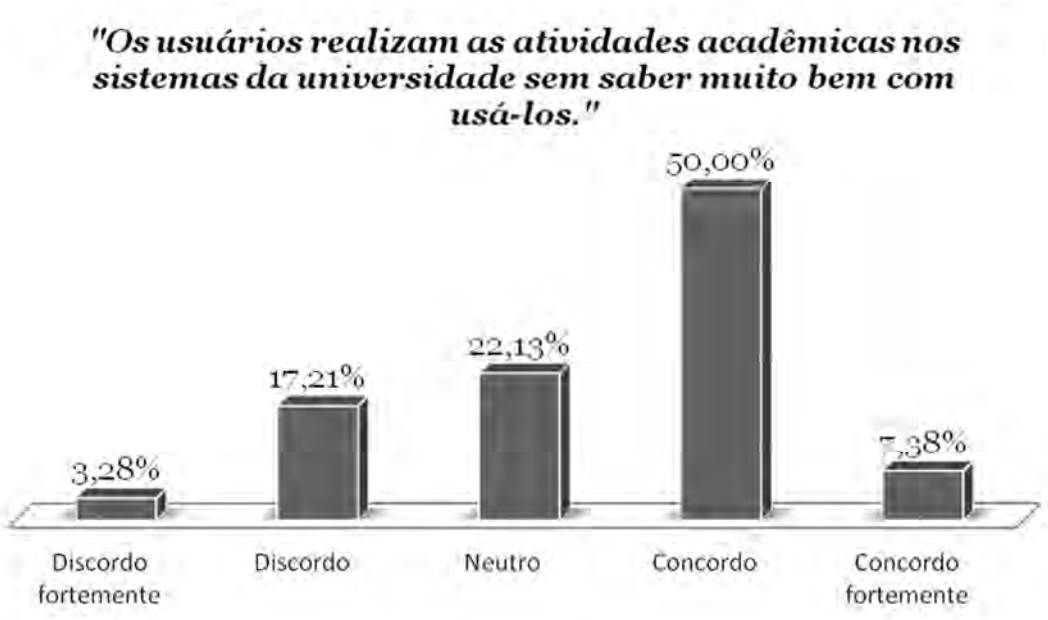

Gráfico 22 Representação gráfica do item CONS5.

Onde, 3,28% discordam fortemente, 17,21% discordam, 22,13% são neutros, 50,00% concordam e 7,38% concordam fortemente (um total de 57,38% de concordância) com a afirmação. Esta variável revela que os usuários percebem que eles não estão sendo devidamente instruídos para realizarem as atividades acadêmicas nos sistemas da universidade. E isto é problemático no sentido deles não terem ciência do que proteger, e nem quais são os perigos e riscos que eles estão envolvidos.

Outra variável CONS4, na Tabela 13, é um dos itens selecionados para medir a variável componente programas de conscientização com a seguinte afirmação (Gráfico 23):

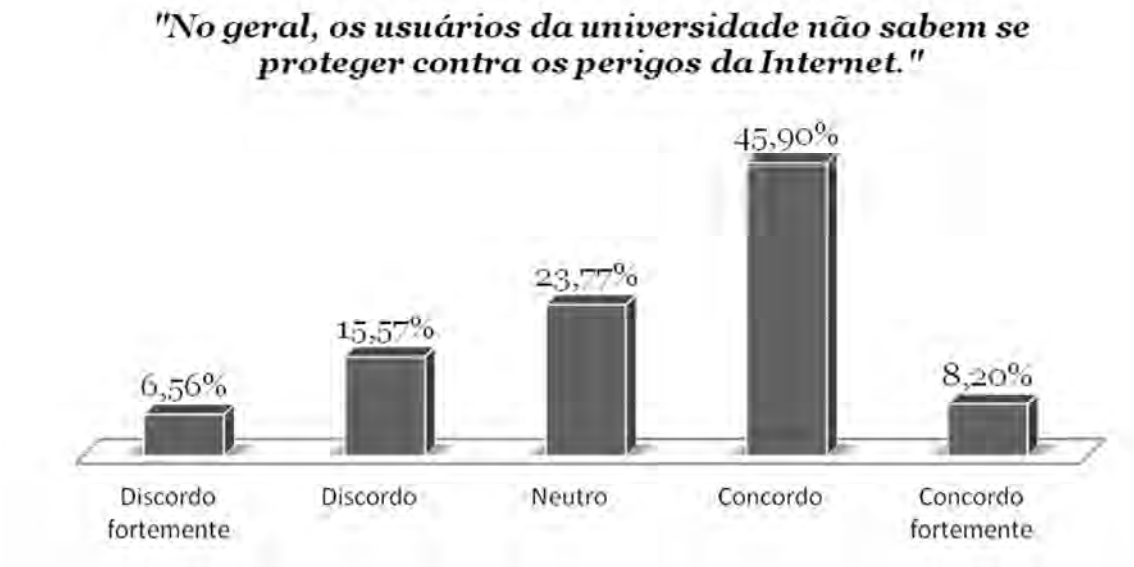

Gráfico 23 Representação gráfica do item CONS4.

Onde, 6,56% discordam fortemente, 15,57% discordam, 23,77% são neutros, 45,90% concordam e 8,20% concordam fortemente (um total de 54,10% de concordância) com a afirmação. Então, fica claro que, assim como os sistemas utilizados na instituição, os usuários também não estão devidamente cientes dos problemas advindos de acessos externos, especificamente a Internet.

Os itens RESP3 e RESP4 possuem comunalidades baixas e assim, não são significativos para explicar o fator (vide Tabela 12, na página **Erro! Indicador não definido.**). Entretanto, pode-se fazer uma reflexão sobre as respostas.

A variável RESP3 na Tabela 13 é um dos itens selecionados para medir a variável componente atribuição de responsabilidade com a seguinte afirmação (Gráfico 24):

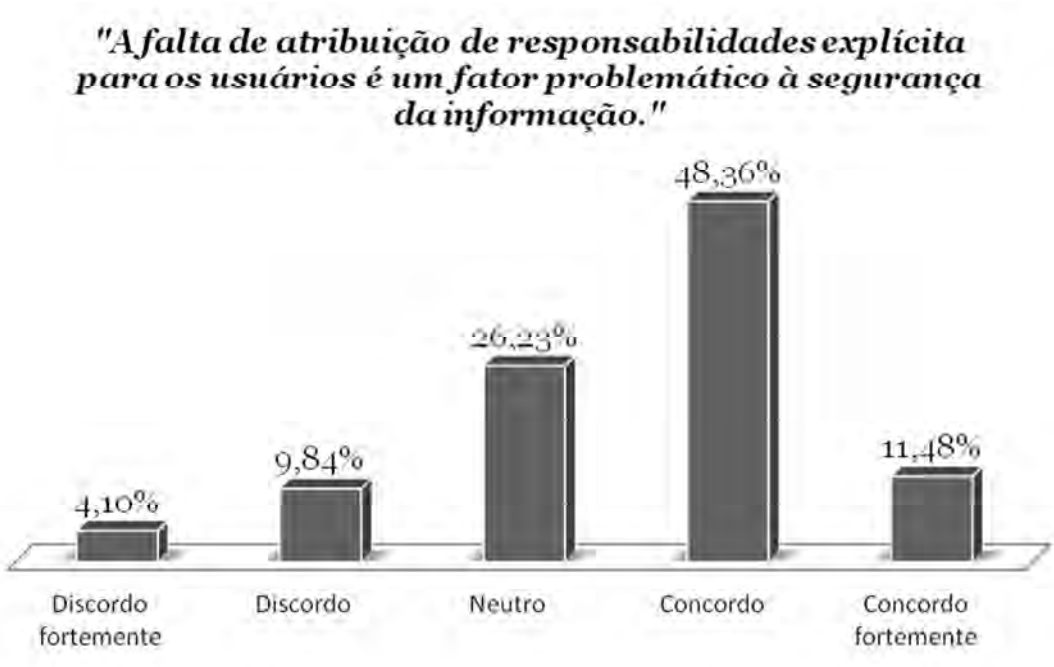

Gráfico 24 Representação gráfica do item RESP3.

Onde, 4,10% discordam fortemente, 9,84% discordam, 26,23% são neutros, 48,36% concordam e 11,48% concordam fortemente (um total de 59,84 % de concordância) com a afirmação.

Outra variável RESP4 na Tabela 13 é um dos itens selecionados para medir a variável componente atribuição de responsabilidade com a seguinte afirmação (Gráfico 25):

Gráfico 25 Representação gráfica do item RESP4.

Onde, 4,10% discordam fortemente, 8,20% discordam, 19,67% são neutros, 54,92% concordam e 13,11% concordam fortemente (um total de 68,03% de concordância) com a afirmação.

6.4 Os resultados da AFE e as normas internacionais de segurança

Como o ambiente acadêmico possui características específicas que o difere dos demais tipos de organizações, é importante que a política de segurança, para este tipo de ambiente, atente aos seis fatores estudados. Pois tais fatores fornecem informações do que precisa ser considerado na escrita da política de segurança.

A importância da política de segurança consiste em indicar o que deve ser protegido e quais as restrições e descrições que os controles devam obedecer para implementar a política (BARMAN, 2001). Uma política de segurança no ambiente acadêmico, como indicado pelos fatores estudados, deverá ter o apoio efetivo da administração. Além disto, é necessário que o ambiente de liberdade acadêmica seja levado em consideração, respeitando as particularidades e interesses das três categorias discentes, docentes e técnicos administrativos.

Com uma política de segurança que contemple tais requisitos, os mecanismos de segurança da instituição, como, por exemplo, *firewalls*, sistemas detectores de intrusão, sistemas acessados por *login* e senha, deverão ser configurados voltados ao cumprimento do que está escrito na política de segurança. Caso seja necessário, e é recomendável, a política de segurança da instituição pode ser composta por várias políticas de segurança (BARMAN, 2001). Assim, se escreve uma política de segurança para o serviço de *e-mail*, para senhas, para acesso à Internet, para acesso a sistemas acadêmicos, para criptografia, etc.

Para se ter um guia do que é preciso ser feito, ou o que se falta contemplar, as normas internacionais de segurança deverão ser consultadas[23]. As normas auxiliam no reconhecimento dos riscos de segurança (por exemplo, cópias de segurança, ou *backups*) nas quais a instituição possa está exposta, além de fornecer informações para um tratamento adequado, através da indicação de diversos controles que busquem minimizar os riscos até um nível aceitável.

6.5 Limitações do estudo

O número de registros válidos da pesquisa não permitiu realizar outros tipos de investigação sobre a percepção da segurança da informação no âmbito acadêmico, como, por exemplo, a análise das três categorias de usuários. Devido à limitação do número de casos, não foi possível realizar computações para as três categorias em separados. Não foram encontrados registros na literatura que os diferenciem com relação à percepção da segurança, entretanto, seria fundamental investigar a existência dessa diferença. Além de outras características como idade, tempo de vínculo, curso,

[23] Atualmente, 2011, no Brasil duas importantes normas são a ABNT NBR ISO/IEC 27001:2006, que trata do Sistema de gestão de segurança da informação e a ABNT NBR ISO/IEC 27001:2005, que fornece o Código de prática para a gestão da segurança da informação.

sexo e titulação, Portanto, fica, mais uma vez, registrado aqui, o caráter exploratório da pesquisa, abrindo, assim, novas vertentes a serem exploradas.

Por fim, alguns usuários indicaram, através das respostas do item comentário do questionário, que sentiram dificuldades em entender o modo como os itens estavam dirigidos. Por exemplo, o seguinte comentário corrobora com esta dificuldade de interpretação:

"O questionário em alguns momentos ficou confuso. As perguntas eram feitas para "os usuários" e não para "o usuário" que responde as questões, o que deixa um problema para a objetividade da resposta. Respostas que demandam de quem responde o conhecimento ou opinião sobre o que todo o conjunto de usuários pode achar genericamnete (sic) ou respostas que seriam a opinião do usuário-individuo (sic) que responde o questionários, respondendo por ele mesmo." – ID 147.

A ideia por trás dos itens, era que o usuário respondesse por si. Com a coleta de dados, as respostas de todos os usuários iriam compor a percepção dos usuários. Os itens não foram elaborados invocando diretamente o usuário para não causar intimidação, ou constrangimento, durante o preenchimento do questionário. Apesar do trabalho ter atingido níveis satisfatórios de significância estatística, o que, possivelmente, indica que poucos tiveram este problema, é importante notar que este ruído (possível falha na interpretação dos itens), pode ter limitado a investigação a atingir resultados mais expressivos.

Este ruído pode ter sido a causa dos respondentes terem assinalados a resposta "Neutro" em alguns itens. Um comentário de um respondente corrobora com esta interpretação:

"Os questionamentos feitos requerem respostas que generalizem o público alvo (os usuários do sistema acadêmico como um todo), quando na verdade em parte das indagações só conseguiria responder por mim, por isso muitas vezes minha resposta foi neutra." – ID 157.

6.6 Considerações finais

O capítulo mostrou que a reestruturação da apresentação do questionário *on-line* culminou no maior número final de casos. Além disso, foi caracterizado o perfil dos respondentes que compõe a amostra.

Com as respostas fornecidas, foi possível indicar seis fatores, através da análise fatorial exploratória, nos quais foram discutidos e analisados com o referencial teórico. Logo após, estes fatores e as normas de segurança foram considerados como meio para elaborar políticas de segurança mais efetivas no ambiente universitário.

Algumas limitações do trabalho foram expostas. O número de respondentes impediu a elaboração de mais computações que visassem diferenciar as percepções de segurança entre os diferentes usuários do ambiente acadêmico. Além disso, uma falha de interpretação do questionário pode ter introduzido um ruído que limitou a investigação a ter resultados mais expressivos.

Capítulo

7

Considerações finais

FTW - For the win

Expressão da Internet que expressa entusiasmo.

A partir dos resultados obtidos, conclui-se que o apoio da administração é o fator mais determinante para explicar a percepção em segurança da informação na instituição pesquisada, segundo a análise fatorial em caráter exploratório. Entretanto, também se indica que o ambiente de liberdade acadêmica deve ser guia para a elaboração de políticas de segurança neste tipo de organização, já que este é o segundo fator mais importante para explicar a segurança da informação.

O trabalho estendeu outros trabalhos apresentados na literatura, tais como Chang e Ho (2006), Werling, Hawkey e Beznosov (2009), Knapp et al. (2005), em especial o estudo de Machado (2008).

O objetivo geral do trabalho, estudar a percepção da segurança da informação num ambiente acadêmico, foi alcançado. Objetivos secundários, também foram atingidos, como a confirmação da hipótese geral e operacional do trabalho. Isto foi possível devido à revisão da literatura, com especial atenção a estudos qualitativos na área. Através da aplicação do questionário *on-line*, sobre os fatores encontrados na litera-

tura, foram coletados dados de 122 usuários da instituição pesquisada. Nos dados, foram aplicados às técnicas estatísticas apropriadas e os resultados apresentados e discutidos.

Portanto, conclui-se que após a análise fatorial, em caráter exploratório, o apoio da administração é o fator mais determinante para explicar a percepção da segurança da informação em um ambiente acadêmico, seguido pelo ambiente de liberdade acadêmica. Conclusões e contribuições

A realização desta investigação indica a necessidade do apoio efetivo da administração (por exemplo, reitores, pró-reitores, chefes de departamentos, diretores, e outros) como sendo relevante para a segurança da informação em universidades públicas. Sendo assim, é importante sensibilizar os administradores das universidades para as questões de segurança da informação, pois são eles os responsáveis por ela, seja diretamente, por exemplo, através do provimento dos meios para a implementação de uma política de segurança da informação na instituição, ou indiretamente, por exemplo, quando do vazamento de provas de vestibular.

Além do fator apoio da administração, o fator ambiente de liberdade acadêmica deve ser considerado na elaboração de uma política de segurança direcionada para o ambiente acadêmico. Os demais fatores devem ser considerados também, porém com menor prioridade. Além do mais, as normas de segurança deverão ser consultadas para a identificação de riscos e a implementação de controles que reflitam a política de segurança.

Mais uma contribuição, foi sobre os itens do questionário referentes ao fator apoio da administração que foram mais uma vez validados, ou seja, tanto este trabalho quanto o de Machado (2008) reforçam a validade dos itens para serem utilizados em futuros questionários sobre apoio da administração na percepção da segurança.

Ademais, a perspectiva da segurança da informação dos usuários de uma universidade pública brasileira coincide com a perspectiva daqueles que tem atribuições e funções de TI nas universidades brasileira.

Logo, os resultados deste estudo podem ser utilizados pelas equipes de tecnologia da informação e comunicação - TIC para sensibilizar os dirigentes universitários da necessidade deles apoiarem as medidas de segurança, geralmente expressas em políticas de segurança. Sem este apoio, o sucesso da efetividade da segurança estará limitado.

7.1 Trabalhos futuros

Pode-se pensar como trabalhos futuros, a necessidade de aplicar este questionário em outras universidades públicas brasileiras. Ou aplicar novamente o questionário na instituição buscando aumentar o número de respondentes e, também, para investigar se existe a influência do tempo na percepção da segurança da informação dos usuários.

Como não foram encontrados registros na literatura que diferenciem as três categorias de usuários estudados (discentes, docentes e técnicos-administrativos) com relação à percepção da segurança, seria fundamental investigar a existência dessa diferença.

Também, pode-se investigar como os controles de segurança deverão ser implementados para garantir o ambiente de liberdade acadêmica com as novas tecnologias, por exemplo, as redes sociais e dos dispositivos móveis.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: **2005**; Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. ISBN 978-85-07-00648-0. Rio de Janeiro, 2005.

ADAMS, A.; SASSE, M. A. Users are not the enemy; Communications of the ACM; Vol. 42. No 12, Dec 1999.

ALBRECHTSEN, E. A qualitative study of users' view on information security. Trondheim, Norway. Computer & Security, nº 26, páginas 276-289, 2007.

BAKER, W. H.; WALLACE, L. Is Information Security Under Control? Investigating Quality in Information Security Management; Publicado por: THE IEEE COMPUTER SOCIETY; IEEE SECURITY & PRIVACY; Jan./Fev. 2007.

BARMAN, S. Writing Information Security Policies. New Riders. Primeira Edição, Nov. 2001.

BRASIL. Ministério da Educação. Reestruturação e Expansão das Universidades Federais. Disponível em: <http://reuni.mec.gov.br>. Acesso em: 4 jul. 2010.

CHANG, S. E.; HO, C. B. Organizational factors to the effectiveness of implementing information security management; Jornal: Industrial Management & Data Systems; Volume: 106; Número: 3; ISSN: 0263-5577; p. 345-361, 2006

COSTELLO, A. B.; OSBORNE, J. W. Best Practices in exploratory factor analysis: Four Recommendations for getting the most from your analysis. Practical Assessment, Research & Evaluation; Volume 10, Número: 7; ISSN: 1531-7714; p.1-9, Jun. 2005.

CAMARGO, Celso De Brasil. Gerenciamento pelo lado da demanda metodologia para identificação do potencial de conservação de energia elétrica de consumidores residenciais. 1996. 0 f. Tese (Doutorado) - Curso de Engenharia de Produção, Universidade Federal de Santa Catarina. Florianópolis, 1996. Disponível em: <http://www.eps.ufsc.br/teses96/camargo/>. Acesso em: 12 dez. 2010.

DOURISH, P.; GRINTER, R. E.; FLOR, J. D. de la; JOSEPH, M. Security in the wild: user strategies for managing security as an everyday, practical problem; Spring-Verlag London Limited, 2004;

FÁVERO, L. P.; BELFIORE, P.; SILVA, F. L.; CHAN, B. L. Análise de dados - modelagem multivariada para tomada de decisões. Elsevier. ISBN 978-85-352-3046-8. Rio de Janeiro, 2009.

GONZALEZ, J. J.; SAWICKA, A. A framework for Human Factors in Information Security; WSEAS International Conference on Information Security (ICIS'02). Brasil, Rio de Janeiro, 2002.

HAIR Jr., J. F.; BLACK, W. C.; BABIN, B. J.; ANDERSON, R. E.; TATHAM, R. L. Análise multivariada de dados. ISBN 978-85-7780-402-3. 6. ed. - Porto Alegre: Bookman, 2009.

HILL, M. M.; HILL, A. Investigação por questionário. Edições Sílabo, 2. ed. Lisboa, 2005.

HORA, H. R. M.; MONTEIRO, G. T. R.; ARICA, J.; Confiabilidade em questionários para qualidade: um estudo com o coeficiente alfa de cronbach.Produto & Produção. Volume: 11; Número: 2; p. 85-103, Jun. 2010.

HÖNE, K.; ELOFF, J.H.P. Information security policy – what do international information security standards says; Elsevier - Computers & Security, 2002.

KANKANHALLI, A.; TEO, H.; TAN, B. C.Y.; WEI, K. An integrative study of information systems security effectiveness; International Jornal of Information Management, nº23, p. 139-154, 2003.

KNAPP, K. J.; MARSHALL, T. E.; RAINER, R. K.; FORD, F. N. Managerial dimensions in information security: a theoretical model of organizational effectiveness. Palm Harbor, Florida and Auburn University, Auburn, Alabama. Oct. 25, 2005.

KRAEMER, S.; CARAYON, P. Human erros and violations in computer and information security – the viewpoint of network administrators and security specialists. Applied Ergonomics nº 38, p. 143-154. Elsevier, 2007.

LAUDON, K. C.; LAUDON, J. P. Sistemas de informação gerenciais: administrando a empresa digital / Kenneth C. Laudon, Jane P. Laudon; tradução Arlete Simille Marques; revisão técnica Erico Veras Marques, Belmiro João. São Paulo, Prentice Hall, 2004.

LIMESURVEY. The survey software - free and open source; Disponível em: <http://www.limesurvey.org/>. Acesso em: 23 jun. 2010.

MACHADO, C. A. N. Um estudo empírico sobre a influência de fatores organizacionais na percepção da efetividade da segurança da informação em universidades pú-

blicas. 2008. 95 p. Dissertação (Mestrado em Informática) - Programa de Pós-graduação em Informática, Universidade Federal da Paraíba, João Pessoa, 2008.

MITNICK, K. D.; SIMON, W. L. The Art of Deception: Controlling the Human Element of Securit; John Wiley & Sons, Inc. New York, NY, USA; Ano da publicação: 2003.

MORAES, O. B. de; ABIKO, A. K. Utilização da análise fatorial para a identificação de estruturas de interdependência de variáveis em estudos de avaliação pós-ocupação. XI Encontro Nacional de Tecnologia no Ambiente Construído. Florianópolis, 2006.

MOROCO, J. Análise estatística com utilização do SPSS. Edições Silabo. Lisboa, 2003.

MUNLEY, M. Moving from Consciousness to culture: Creating an environment of security awareness; GSEC Practical Assignment, 10 Apr. 2004.

OBLINGER, D. Computer and Network Security and Higher Education's Core Values EDUCAUSE, Center for applied research. Research Bulletin. Volume 2003, Issue 6. 18 Mar. 2003.

REDE NACIONAL DE ENSINO E PESQUISA. Incidentes reportados ao CAIS. Disponível em: <http://www.rnp.br/cais/estatisticas/index.php>. Acesso em: 18 jan. 2010.

SASSE, M. A.; BROSTOFF, S.; WEIRICH, D. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security; BT Technol J Vol 19 No 3, July 2001.

SILVA, D. R. P. da; STEIN, L. M. Segurança da Informação: uma reflexão sobre o comportamento humano; Ciência & Cognição; Vol 10, p 46-53, 2007.

SIPONEN, M. T. Five dimensions of information security awareness; Computer and Society, p. 24-29, June 2001.

SOLMS, B. V. Information Security - a multidimensional discipline. Computer & Security, nº 20, p. 504-508, 2001.

TUCKER, L. R.; MACCALLUM, R. C. Exploratory Factor Analysis, Capítulo 1. General concepts and objectives of factor analysis, 1997.

WERLINGER, R.; HAWKEY, K.; BEZNOSOV, K. An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security. Emerald Group Publishing Limited, Volume 17, Nº 1, 2009.

WHITMAN, M. E.; Enemy at the gate: threats to information security; Communications of the ACM; Vol. 46, No. 8, Aug. 2003.

Apêndice A

O Apêndice A reúne a codificação dos itens, usado no programa SPSS, com as afirmações utilizadas no questionário para investigação dos fatores que definem a percepção da segurança da informação dos usuários de uma universidade pública. Também há a informação se um item é de codificação reversa ou não.

Assim, a Tabela 14 se refere os itens do ambiente de liberdade acadêmica, a Tabela 15 sobre os itens apoio da administração, Tabela 16 itens comunicação, Tabela 17 cultura da segurança, Tabela 18 prioridade da segurança, Tabela 19 participação na segurança da informação, Tabela 20 programas de conscientização e Tabela 21 atribuição de responsabilidade.

Nome da variável no SPSS	Itens sobre o ambiente de liberdade acadêmica	Item de Codificação Reversa?
AMBI1	*O ambiente de liberdade acadêmica prejudica a segurança da informação da instituição.*	Não
AMBI2	*A liberdade requerida pelos usuários da instituição proporciona o mau uso dos computadores.*	Não
AMBI3	*A realização de atividades de ensino, pesquisa ou extensão devem respeitar as normas de segurança.*	Não
AMBI4	*Geralmente, medidas restritivas de segurança da informação, por exemplo, uso de senhas fortes, não são bem aceitas pela comunidade universitária.*	Não.
AMBI5	*A liberdade conquistada pela comunidade universitária para realização de atividades acadêmicas é algo inquestionável e intocável.*	Sim.

Tabela 14 Correspondência dos itens sobre ambiente de liberdade acadêmica com o nome da variável utilizada no SPSS.

Nome da variável no SPSS	Itens sobre o apoio da administração	Item de Codificação Reversa?
ADMI1	*Os dirigentes da universidade apóiam a elaboração das medidas de segurança nas máquinas, rede e sistemas da organização.*	Não
ADMI2	*Os dirigentes universitários consideram a segurança da informação uma importante prioridade.*	Não
ADMI3	*Os dirigentes se interessam pelos problemas relacionados à segurança da informação*	Não
ADMI4	*Os dirigentes se envolvem regularmente na tomada de decisão sobre questões importantes de segurança da informação*	Não
ADMI5	*Os dirigentes levam em conta questões de segurança quando realizam o planejamento da organização*	Não

Tabela 15 Correspondência dos itens sobre apoio da administração com o nome da variável utilizada no SPSS.

Nome da variável no SPSS	Itens sobre comunicação	Item de Codificação Reversa?
COMU1	*Os usuários são comunicados de maneira efetiva sobre as atuais ameaças da Internet, como por exemplo, novos vírus de computadores*	Não
COMU2	*Na universidade, os usuários são avisados sobre as ameaças, regras de uso, políticas e conjunto de boas práticas de segurança da informação*	Não
COMU3	*Não existe comunicação entre os responsáveis diretos pela segurança da informação da instituição e os usuários*	Sim
COMU4	*Os usuários são suficientemente informados sobre os problemas de segurança da informação*	Não
COMU5	*A instituição considera importante a divulgação de eventos que prejudiquem a segurança da informação, quando pertinente.*	Não

Tabela 16 Correspondência dos itens sobre comunicação com o nome da variável utilizada no SPSS.

Nome da variável no SPSS	Itens sobre a cultura da segurança	Item de Codificação Reversa?
CULT1	*Os usuários valorizam a importância da segurança da informação*	Não
CULT2	*Os usuários se queixam frequentemente das regras de segurança nos computadores da instituição.*	Sim
CULT3	*Percebe-se que existe uma cultura, na instituição, que promova as boas práticas de segurança.*	Não
CULT4	*Os usuários têm compromisso com a segurança da informação.*	Não
CULT5	*Os usuários são conscientes da necessidade de proteger as informações e os recursos computacionais da instituição.*	Não

Tabela 17 Correspondência dos itens sobre cultura da segurança com o nome da variável utilizada no SPSS.

Nome da variável no SPSS	Itens sobre a prioridade da segurança	Item de Codificação Reversa?
PRIO1	*Para os usuários, a segurança da informação é uma prioridade quando se utiliza os recursos disponíveis na universidade*	Não
PRIO2	*Os usuários percebem a importância de proteger as máquinas da instituição contra perda de dados*	Não
PRIO3	*Executar programas de computadores de procedência duvidosa como, por exemplo, softwares piratas, são ações que não preocupam os usuários*	Sim
PRIO4	*As regras de segurança presente na universidade dificultam as atividades diárias de alunos, funcionários e professores*	Sim
PRIO5	*Os usuários não veem a segurança da informação como algo importante*	Sim

Tabela 18 Correspondência dos itens sobre prioridade da segurança com o nome da variável utilizada no SPSS.

Nome da variável no SPSS	Itens sobre a participação nas atividades de segurança	Item de Codificação Reversa?
PART1	*Geralmente, os usuários participam na solução dos problemas de segurança, emitindo opiniões e participando de reuniões com os envolvidos diretamente com a segurança da informação*	Não
PART2	*Os usuários regulam o acesso à Internet indicando o que deve ser liberado ou não, por exemplo, sites de relacionamentos ou mensageiros, como MSN*	Não
PART3	*Os usuários cobram da instituição o uso seguro da rede e das máquinas que lhes estão disponíveis*	Não
PART4	*A comunidade de usuários é consultada quando surge uma questão crítica de segurança*	Não
PART5	*Percebe-se que os usuários participam na proteção de informações, sistemas e na rede da instituição*	Não

Tabela 19 Correspondência dos itens sobre a participação na segurança da informação com o nome da variável utilizada no SPSS.

Nome da variável no SPSS	Itens sobre programas de conscientização	Item de Codificação Reversa?
CONS1	*Os usuários recebem o devido treinamento antes de usar os sistemas da instituição*	Não
CONS2	*As campanhas, palestras, eventos, cartazes, entre outras ações de conscientização dos usuários são suficientes para o uso correto e seguro das máquinas e sistemas na instituição*	Não
CONS3	*Os usuários são orientados a lerem os avisos afixados nos laboratórios, corredores, quadros de aviso, enviados por e-mails, em folhetos e em demais locais que contenham instruções de segurança*	Não
CONS4	*No geral, os usuários da universidade não sabem se proteger contra os perigos da Internet*	Sim
CONS5	*Os usuários realizam as atividades acadêmicas nos sistemas da universidade sem saber muito bem com usá-los*	Sim

Tabela 20 Correspondência dos itens sobre programas de conscientização com o nome da variável utilizada no SPSS.

Nome da variável no SPSS	Itens sobre atribuição de responsabilidade	Item de Codificação Reversa?
RESP1	*Os usuários têm responsabilidades com a segurança da informação, mesmo que a instituição possua funcionários específicos com a obrigação de proteger as máquinas da instituição*	Não
RESP2	*Os professores, alunos e funcionários não são responsáveis pela segurança da informação na universidade*	Sim
RESP3	*A falta de atribuição de responsabilidades explícita para os usuários é um fator problemático à segurança da informação*	Não
RESP4	*Atribuir responsabilidades a cada usuário contribui para que eles não comprometam a segurança da informação*	Não
RESP5	*Cada usuário está ciente da responsabilidade no uso da rede, dos sistemas e das máquinas da universidade*	Não

Tabela 21 Correspondência dos itens sobre atribuição de responsabilidade com o nome da variável utilizada no SPSS.

Apêndice B

O Apêndice B reúne os itens que sofreram pré-processamento dos dados, visando à correção dos valores referentes aos itens de codificação reversa, por causa da limitação da ferramenta de coleta de dados. Desta maneira, a Tabela 22 se refere à aplicação da Equação 1 sobre os itens do questionário que foram codificados de forma reversa.

Variável do item de codificação reversa	Valor final da variável
AMBI5	6 - AMBI5
COMU3	6 - COMU3
CULT2	6 - CULT2
PRIO3	6 - PRIO3
PRIO4	6 - PRIO4
PRIO5	6 - PRIO5
CONS4	6 - CONS4
CONS5	6 - CONS5
RESP2	6 - RESP2

Tabela 22 Pré-processamento dos itens de codificação reversa através da aplicação da Equação 1.

Na Tabela 23 estão as saídas dos comandos no SPSS após a codificação reversas dos itens que sofreram pré-processamento.

Item	Saída dos comandos do SPSS para o pré-processamento
AMBI5	COMPUTE AMBI5=6 - AMBI5. EXECUTE.
COMU3	COMPUTE COMU3=6 - COMU3. EXECUTE.
CULT2	COMPUTE CULT2=6 - CULT2. EXECUTE.
PRIO3	COMPUTE PRIO3=6 - PRIO3. EXECUTE.
PRIO4	COMPUTE PRIO4=6 - PRIO4. EXECUTE.
PRIO5	COMPUTE PRIO5=6 - PRIO5. EXECUTE.
CONS4	COMPUTE CONS4=6 - CONS4. EXECUTE.
CONS5	COMPUTE CONS5=6 - CONS5. EXECUTE.
RESP2	COMPUTE RESP2=6 - RESP2. EXECUTE.

Tabela 23 Resultado da saída dos comandos do SPSS para o pré-processamento dos itens de codificação reversa.

.

Apêndice C

O Apêndice C reúne todos os comentários feitos pelos usuários para o item comentário do questionário *on-line* sobre a investigação empírica sobre a percepção da segurança da informação pelos usuários de uma universidade pública baseada na análise fatorial exploratória.

Na Tabela 24 Comentários dos respondentes sobre o questionário.Tabela 24 está o id do respondente juntamente com o comentário sobre o questionário.

Identificador do caso (id)	Comentário sobre o questionário
002	Frases afirmativas e negativas se misturam no decorrer do questionário, mas friso aqui a devida importâcia do mesmo para procedimentos de segurança futuros para instituições de ensino.
004	Sem comentários.
013	De todas as questões abordadas, uma das principais é da educação dos usuarios, torná-los conscientes do que pode vir a acontecer com os dados delas.
018	Acho que a parte que indaga sobre a concientização dos usuários deveria vir em primeiro lugar, visto que esta é o maior desafio de nosso tempo. No mais, ficou muito bom, precisamos de mais dessas![omitido]
019	De fato senti com relação a algumas questões dificuldades, mas o questionário foi bem elaborado.
026	Muito bom
032	O questionário poderia abrir espaço para questões discursivas.
037	Penso que, em várias afirmativas, a percepção do elaborador sobre os temas estaria transparecendo de forma bastante evidente para influenciar a opção do entrevistado. Em certos casos, nos quais eu não sou neutro, também não era contra nem a favor do problema posto nos termos da afirmativa: nesses casos,parece-me que faltou objetividade na formulação da afirmativa.
038	Um pouco grande , mas se é pelo bem da informação... tá legal.
039	O assunto Segurança da Informação deveria ser mais debatido dentro da universidade. E tendo como foco um dos principais elos da segurança que são as pessoas. Não adianta sistemas robustos na parte de segurança, se os usuários não fazem o uso devido do mesmo.

040	ao final deste questionario, cofesso que senti muita dificuldade em responder a algumas questos porque esta não é a minha area e o questionario é feito para respondermos com uma opinião generalizada enão individual, porem foi boa a experiencia de me questionar sobre a segurança na universidade.
052	Um Questionario muito tecnico e formal, denso de responder e que levam as mesmas respostas!
058	Gostaria de saber em quais fatores entrei em contradição.
059	ESPERO QUE ESTE QUESTIONÁRIO TRAGA BENEFÍCIOS PARA TODOS NÓS.
066	muito grande rsrsrs
072	Falta de compreensão nas questões
080	faltou perguntar sobre o serviço dos técnicos da área, muitas vezes sem capacidade de lidar com o público.
082	Toda e qualquer barreira ao conhecimento é burra! E por muitas vezes os usuários não tem acesso de complementos para o ensino e para a pesquisa.
087	Há alguns sites que são bloqueados, mais isso não deveria ocorrer, pois são através destes que muitos alunos baixam conteúdos acadêmicos, como também se comunicam com outras pessoas, ato que é de fundamental importância no mundo globalizado no qual atualmente estamos inseridos.
094	Muito bom para o ceres pensar em mecanismos e uma política de para que deixe a comunidade acadêmica ciente de suas responsabilidades, sobretudo fazer esse trabalho no inicio do período letivo, que são quando os calouros entram na istituição. [omitido]
118	O quesitonário é constituído apenas por um tipo de questão. Isso o torna estafante! Além disso, por vezes, as questões confundem o raciocínio do respondente.
126	Perca de tempo...Só pra quem não tem o que fazer...
127	NÃO GOSTEI DO QUESTIONÁRIO, PODERIA SER ALGO MAIS SIMPLES,DIRETO E OBJETIVO.
129	Algumas questões senti dificuldade de responder por não entender muito do asunto de segurança da informação. para mim está ligado só a vírus, portanto no decorrer do questionário observei que muito amplo esta questão. Espero ter contibuido.
133	A propria universidade usa software piratas, quem somos nós para para usa apenas softwares verdadeiros?fora isso o questionario é muito repetitivo, sugiro reelaborar buscando enfocar uma prioridade
134	Só para acanalhar um pouco sua pesquisa, nem da ufrn sou
147	O questionário em alguns momentos ficou confuso. As perguntas eram feitas para "os usuários" e não para "o usuário" que responde as questões, o que deixa um problema para a objetividade da resposta. Respostas que demandam de quem responde o conhecimento ou opinião sobre o que todo o conjunto de usuários pode achar genericamnete ou respostas que seriam a opinião do usuário-individuo que responde o questionários, respondendo por ele mesmo.
157	Os questionamentos feitos requerem respostas que generalizem o público alvo (os usuários do sistema acadêmico como um todo), quando na verdade em parte das indagações só conseguiria responder por mim, por isso

	muitas vezes minha resposta foi neutra.
199	Walber, parabéns por sua pesquisa. Que ela contribua para o aumento da segurança da informação em toda a comunidade acadêmica.

Tabela 24 Comentários dos respondentes sobre o questionário.

Apêndice

D

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE ENSINO SUPERIOR DO SERIDÓ

CONVITE

Prezado(a),

Eu, Walber José Adriano Silva, funcionário da UFRN e estudante do Programa de Pós-Graduação em Informática - UFPB, estou convidando a comunidade do CERES/UFRN a participar de uma pesquisa que visa investigar a percepção em segurança da informação dos usuários (discentes, docentes e técnicos administrativos) sobre os fatores críticos que influenciam na implementação de políticas de segurança na instituição. A pesquisa, questionário on-line, está disponível no site da instituição através do endereço:

http://www.cerescaico.ufrn.br/pesquisa/

Para qualquer contato, estou à disposição no e-mail walber@cerescaico.ufrn.br

Grato, desde já, pela participação.

Orientador: Prof. Dr. Gustavo Henrique Matos Bezerra Motta – UFPB

Co-Orientador: Prof. Dr. Lucídio dos Anjos Formiga Cabral - UFPB

Apêndice

E

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

CENTRO DE ENSINO SUPERIOR DO SERIDÓ

Caicó(RN), Outubro de 2010.

Eu, Walber José Adriano Silva, participante do Programa de Pós-Graduação em Informática – PPGI, e ocupante do cargo Tecnólogo/Gerência de Redes na Universidade Federal do Rio Grande do Norte, solicito autorização de uso dos recursos computacionais e de conectividade do Centro de Ensino Superior do Seridó - CERES localizado na cidade de Caicó-RN, para realizar instalação, configuração e manutenção de programas de computadores que objetiva coletar dados, para fins de pesquisa, através de um questionário quantitativo on-line. O questionário estará hospedado no endereço institucional *http://www.cerescaico.ufrn.br/pesquisa/* .A coleta de dados faz parte da minha dissertação de mestrado intitulada "*Investigação empírica sobre percepção da segurança da informação pelos usuários de uma universidade pública baseada na análise fatorial exploratória*", cujo objetivo é estudar a definição e implementação de políticas de segurança da informação que sejam mais efetivas no âmbito da universidade.

Autorizo,

Assinatura
DIRETOR

Apêndice F

O Apêndice F compila os gráficos da distribuição normal dos 16 itens utilizados na computação da análise fatorial exploratória. Cada gráfico tem a mesma escala tanto no eixo horizontal quanto vertical, facilitando assim, a visualização e comparação da distribuição das respostas para os itens.

Distribuição normal dos itens ADMI3 e ADM4

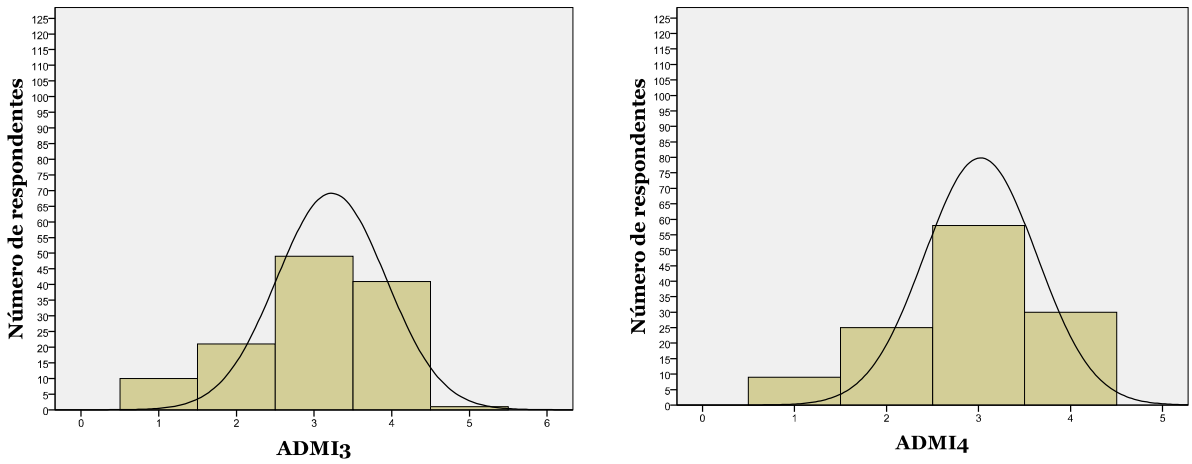

Tabela 25 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente ao apoio da administração.

Distribuição normal dos itens PRIO1 e PRIO2

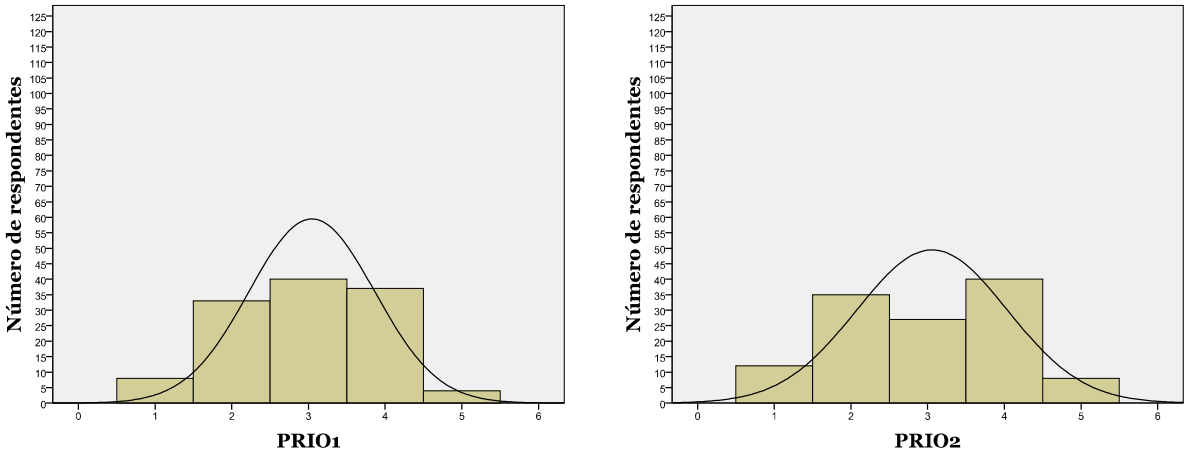

Tabela 26 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente à prioridade da segurança.

Distribuição normal dos itens CULT4 e CULT5

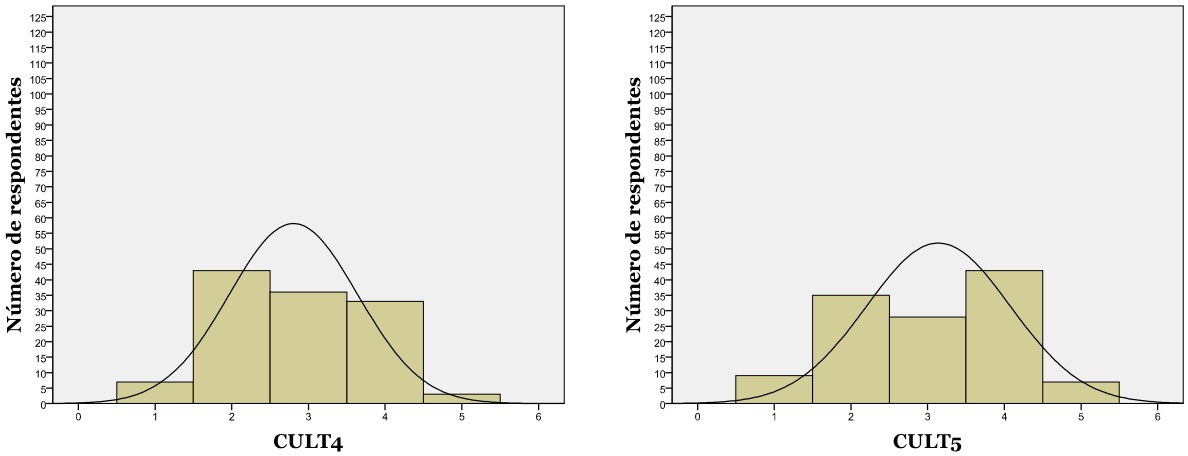

Tabela 27 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente à cultura da segurança.

Distribuição normal dos itens AMBI1 e AMBI2

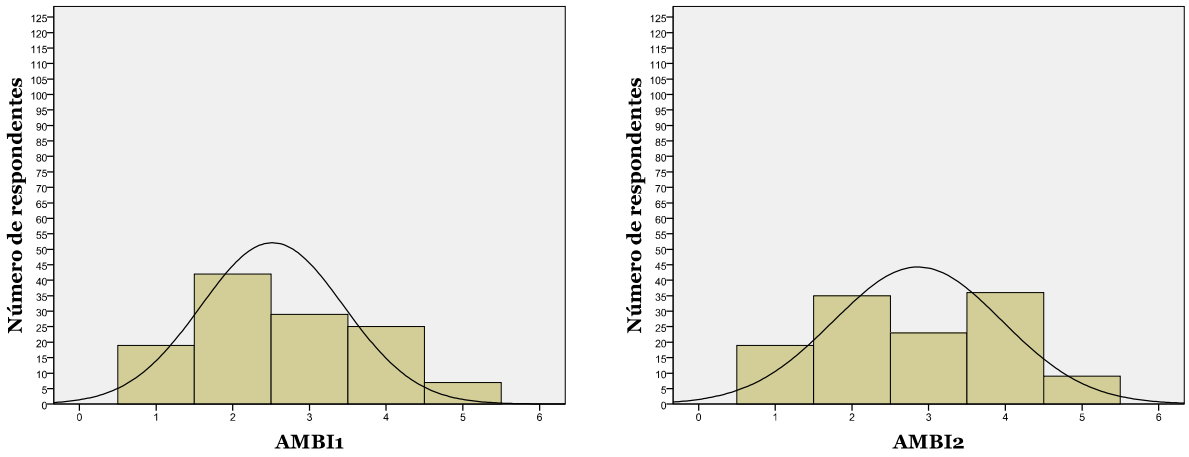

Tabela 28 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente à ambiente de liberdade acadêmica.

Distribuição normal dos itens PART1 e PART4

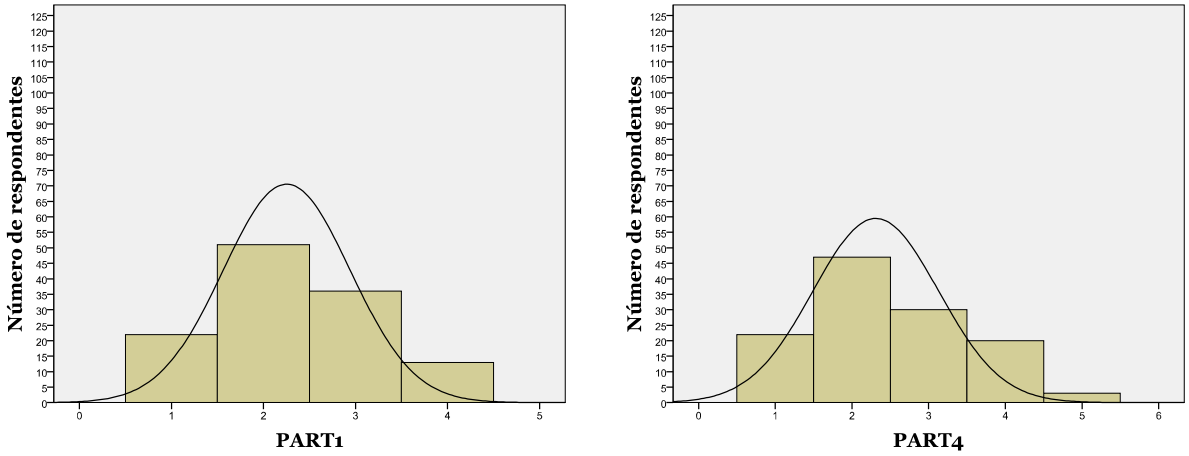

Tabela 29 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente à participação na segurança da informação.

Distribuição normal dos itens COMU1 e COMU4

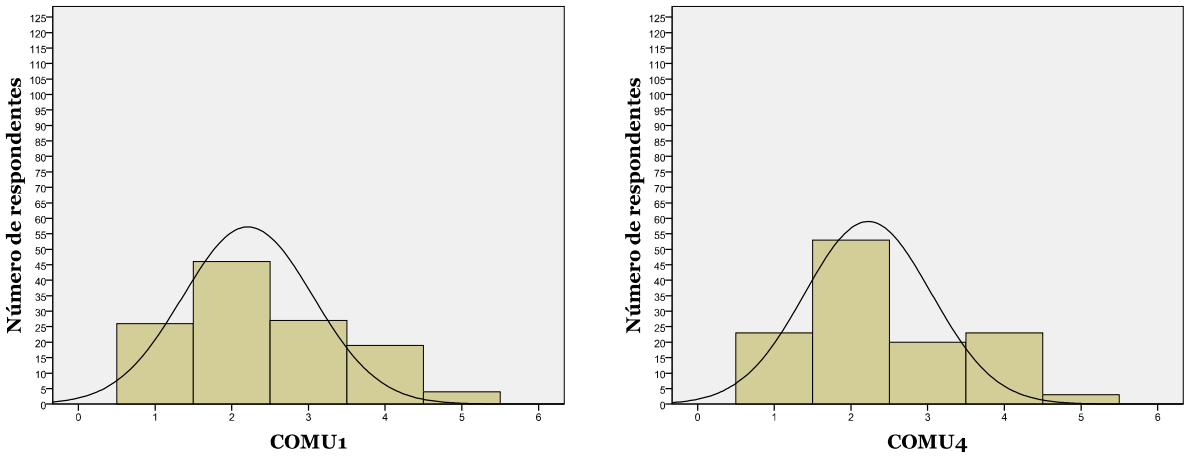

Tabela 30 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente à comunicação.

Distribuição normal dos itens RESP3 e RESP4

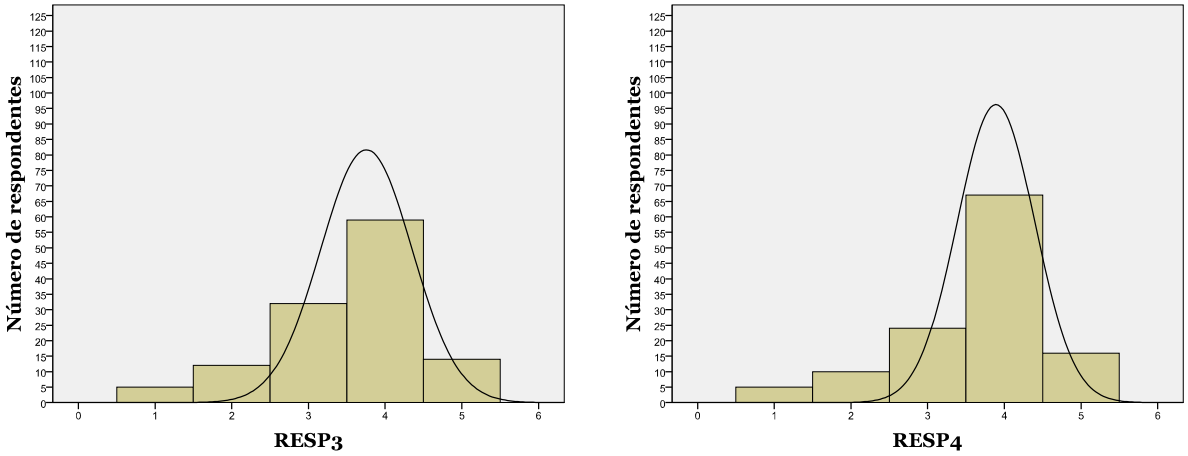

Tabela 31 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente à atribuição de responsabilidade.

Distribuição normal dos itens CONS4 e CONS5

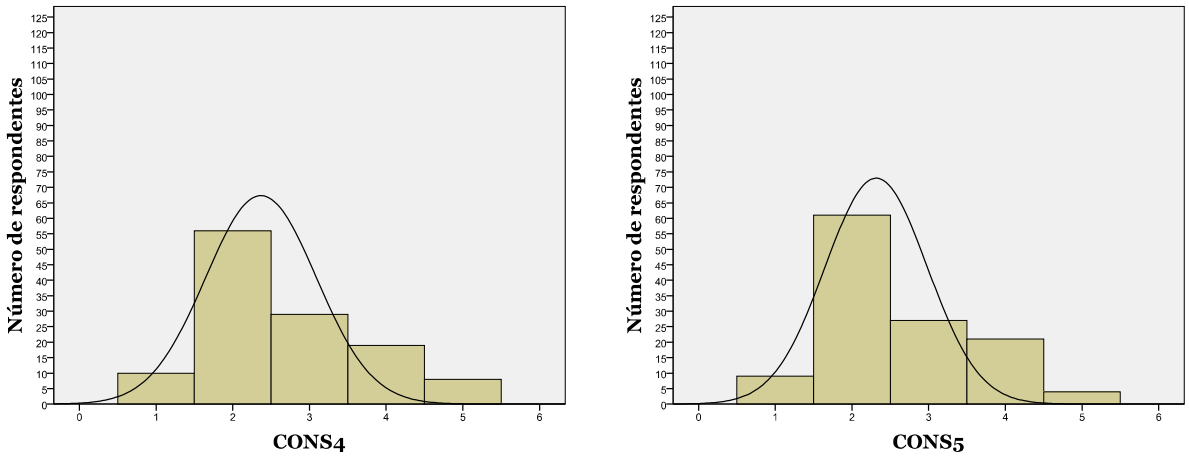

Tabela 32 Distribuição normal dos dois itens utilizados na análise fatorial exploratória referente ao programa de conscientização.

Apêndice G

O Apêndice G compila as tabelas resultantes dos cálculos realizados no SPSS para definição da confiabilidade interna do conjunto de itens do questionário. Para tal, foi calculado o coeficiente de alfa de Cronbach para os cinco itens e o mesmo coeficiente se cada item individual fosse excluído do cálculo.

O alfa de Cronbach é considerado satisfatório quando atinge um valor acima de 0,6. Nas situações em que isto não ocorre, aquele item que aumenta o coeficiente é excluído, ou seja, descartado da pesquisa (isto não prejudica a pesquisa porque os cinco itens buscam medir a mesma coisa) e o alfa é novamente calculado.

O objetivo é selecionar as variáveis que estejam mais correlacionadas e com o alfa mais próximo possível do valor 1. Assim, serão selecionadas apenas duas variáveis de cada conjunto de cinco itens que sigam essa característica (HILL, M.; HILL, A., 2005).

Ambiente de liberdade acadêmica

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,496 (vide Tabela 33) que é considerado um valor inaceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,496	5

Tabela 33 Alfa de Cronbach para os cinco itens referentes ao ambiente de liberdade acadêmica.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 34. Nela, pode-se perceber que o alfa irá para 0,638 em caso de exclusão da AMBI5.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
AMBI1	12,48	6,202	,519	,385	,257
AMBI2	12,30	5,901	,516	,403	,245
AMBI3	11,03	8,524	,217	,084	,472
AMBI4	12,26	7,833	,232	,138	,464
AMBI5	12,45	9,282	-,039	,039	,638

Tabela 34 Cálculo do alfa de Cronbach no SPSS com a opção de "*Scale if item deleted*" para as variáveis AMBI1, AMBI2, AMBI3, AMBI4 e AMBI5.

Então, como o alfa foi recalculado retirando à variável AMBI5, e assim, obteve-se o valor de 0,638 (Tabela 35), que é um valor fraco do alfa, mas aceitável. Então, as variáveis AMBI1, AMBI2, AMBI3, AMBI4 são consideradas como possuindo confiabilidade interna.

Alfa de Cronbach	Número de itens
0, 638	5

Tabela 35 Alfa de Cronbach para o fator ambiente de liberdade acadêmica, com a exclusão da variável AMBI5.

Por fim, a matriz de correlação é calculada, Tabela 36. Como as variáveis mais correlacionadas são AMBI1 e AMBI2, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

	AMBI1	AMBI2	AMBI3	AMBI4
AMBI1	1,000	,598	,203	,208
AMBI2	,598	1,000	,176	,303
AMBI3	,203	,176	1,000	,156
AMBI4	,208	,303	,156	1,000

Tabela 36 Matriz de correlação para as variáveis AMBI1, AMBI2, AMBI3 e AMBI4.

Apoio da Administração

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,859 (vide Tabela 37) que é considerado um valor aceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,859	5

Tabela 37 Alfa de Cronbach para os cinco itens referentes ao apoio da administração.

Assim, o próximo passo foi calcular a matriz de correlação, Tabela 38. Como as variáveis mais correlacionadas são ADMI3 e ADMI4, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

	ADMI1	ADMI2	ADMI3	ADMI4	ADMI5
ADMI1	1,000	,540	,459	,367	,552
ADMI2	,540	1,000	,616	,512	,596
ADMI3	,459	,616	1,000	,638	,572
ADMI4	,367	,512	,638	1,000	,414
ADMI5	,552	,596	,572	,414	1,000

Tabela 38 Matriz de correlação para as variáveis ADMI1, ADMI2, ADMI3, ADMI4 e ADMI5.

Comunicação

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,711 (videTabela 39) que é considerado um valor aceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,711	5

Tabela 39 Alfa de Cronbach para os cinco itens referentes à comunicação.

Assim, o próximo passo foi calcular a matriz de correlação, Tabela 40. Como as variáveis mais correlacionadas são COMU1 e COMU4, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

	COMU1	COMU2	COMU3	COMU4	COMU5
COMU1	1,000	,516	,176	,672	,371
COMU2	,516	1,000	,137	,584	,335
COMU3	,176	,137	1,000	,111	-,015
COMU4	,672	,584	,111	1,000	,487
COMU5	,371	,335	-,015	,487	1,000

Tabela 40 Matriz de correlação para as variáveis COMU1, COMU2, COMU3, COMU4 e COMU5.

Cultura da segurança

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,648 (vide Tabela 41) que é considerado um valor aceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,648	5

Tabela 41 Alfa de Cronbach para os cinco itens referentes à cultura da segurança.

Assim, o próximo passo foi calcular a matriz de correlação, Tabela 38. Como as variáveis mais correlacionadas são CULT4 e CULT5, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

	CULT1	CULT2	CULT3	CULT4	CULT5
CULT1	1,000	-,044	,396	,602	,655
CULT2	-,044	1,000	-,001	-,043	-,191
CULT3	,396	-,001	1,000	,356	,353
CULT4	,602	-,043	,356	1,000	,699
CULT5	,655	-,191	,353	,699	1,000

Tabela 42 Matriz de correlação para as variáveis CULT1, CULT2, CULT3, CULT4 e CULT5.

Prioridade da segurança

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,485 (vide Tabela 43) que é considerado um valor inaceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,485	5

Tabela 43 Alfa de Cronbach para os cinco itens referentes à prioridade da segurança.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 44. Nela, pode-se perceber que o alfa irá para 0,637 em caso de exclusão da PRIO4.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PRIO1	11,70	7,065	,325	,504	,391
PRIO2	11,69	6,084	,427	,531	,306
PRIO3	11,98	6,958	,280	,211	,417
PRIO4	11,61	8,896	-,065	,031	,655
PRIO5	11,76	6,366	,427	,260	,316

Tabela 44 Cálculo do alfa de Cronbach no SPSS com a opção de "Scale if item deleted" para as variáveis PRIO1, PRIO2, PRIO3, PRIO4 e PRIO5

Então, como o alfa foi recalculado retirando à variável PRIO4, e assim, obteve-se o valor de 0,655 (Tabela 45), que é um valor fraco do alfa, mas aceitável. Então, as variáveis PRIO1, PRIO2, PRIO3, PRIO5 são consideradas como possuindo confiabilidade interna.

Alfa de Cronbach	Número de itens
0,655	5

Tabela 45 Alfa de Cronbach para os itens referentes à prioridade da segurança

Por fim, a matriz de correlação é calculada, Tabela 36.

	PRIO1	PRIO2	PRIO3	PRIO5
PRIO1	1,000	,695	,068	,213
PRIO2	,695	1,000	,188	,331
PRIO3	,068	,188	1,000	,438
PRIO5	,213	,331	,438	1,000

Tabela 46 Matriz de correlação para as variáveis PRIO1, PRIO2, PRIO3, PRIO5

Como as variáveis mais correlacionadas são PRIO1 e PRIO2, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

Participação nas atividades de segurança

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,769 (vide Tabela 47) que é considerado um valor aceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,769	5

Tabela 47 Alfa de Cronbach para os cinco itens referentes à participação nas atividades de segurança.

Assim, o próximo passo foi calcular a matriz de correlação, Tabela 48. Como as variáveis mais correlacionadas são PART1 e PART4, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

	PART1	PART2	PART3	PART4	PART5
PART1	1,000	,460	,279	,612	,441
PART2	,460	1,000	,287	,378	,304
PART3	,279	,287	1,000	,210	,476
PART4	,612	,378	,210	1,000	,339
PART5	,441	,304	,476	,339	1,000

Tabela 48 Matriz de correlação para as variáveis PART1, PART2, PART3, PART4 e PART5.

Programas de conscientização

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,494 (vide Tabela 49) que é considerado um valor inaceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,494	5

Tabela 49 Alfa de Cronbach para os cinco itens referentes a programas de conscientização.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 50. Nela, pode-se perceber que o alfa irá para 0,489 em caso de exclusão da CONS3.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
CONS1	10,75	5,906	,423	,244	,331
CONS2	10,39	6,290	,303	,232	,414
CONS3	10,16	6,777	,194	,190	,489
CONS4	10,36	6,712	,240	,369	,457
CONS5	10,43	7,173	,193	,377	,483

Tabela 50 Cálculo do alfa de Cronbach no SPSS com a opção de "Scale if item deleted" para as variáveis CONS1, CONS2, CONS3, CONS4 e CONS5.

Então, como o alfa foi recalculado retirando à variável CONS3, e assim, obteve-se o valor de 0,489 (Tabela 51), que ainda é um valor inaceitável.

Alfa de Cronbach	Número de itens
0,489	5

Tabela 51 Alfa de Cronbach para as variáveis CONS1, CONS2, CONS4 e CONS5.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 52. Nela, pode-se perceber que o alfa irá para 0,513 em caso de exclusão da CONS2.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
CONS1	7,89	4,383	,304	,181	,400
CONS2	7,52	4,731	,184	,196	,513
CONS4	7,49	4,120	,365	,361	,339
CONS5	7,57	4,611	,295	,377	,409

Tabela 52 Cálculo do alfa de Cronbach no SPSS com a opção de "Scale if item deleted" para as variáveis CONS1, CONS2, CONS4 e CONS5.

Então, como o alfa foi recalculado retirando à variável CONS2, e assim, obteve-se o valor de 0,513 (Tabela 53), que ainda é um valor inaceitável.

Alfa de Cronbach	Número de itens
0,513	5

Tabela 53 Alfa de Cronbach para as variáveis CONS1, CONS4 e CONS5.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 54. Nela, pode-se perceber que o alfa irá para 0,738 em caso de exclusão da CONS1.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
CONS1	5,25	3,232	,114	,013	,738
CONS4	4,86	2,237	,444	,345	,200
CONS5	4,93	2,376	,475	,348	,168

Tabela 54 Cálculo do alfa de Cronbach no SPSS com a opção de "Scale if item deleted" para as variáveis CONS1, CONS4 e CONS5.

Então, como o alfa foi recalculado retirando à variável CONS1, e assim, obteve-se o valor de 0,738 (Tabela 55), que é um valor fraco do alfa, mas aceitável. Então, as variáveis CONS4 e CONS5 são consideradas como possuindo confiabilidade interna.

Alfa de Cronbach	Número de itens
0,738	5

Tabela 55 Alfa de Cronbach para as variáveis CONS4 e CONS5.

Por fim, a matriz de correlação é calculada, Tabela 56. Como as variáveis mais correlacionadas são CONS4 e CONS5, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

Estatísticas Item-Total

	CONS4	CONS5
CONS4	1,000	,587
CONS5	,587	1,000

Tabela 56 Matriz de correlação para as variáveis CONS4 e CONS5.

Atribuição de Responsabilidade

Neste fator foi calculado o valor de alfa de Cronbach para as cinco variáveis. O resultado do alfa foi 0,353 (vide Tabela 57) que é considerado um valor inaceitável para confiança interna (Tabela 1).

Alfa de Cronbach	Número de itens
0,353	5

Tabela 57 Alfa de Cronbach para os cinco itens referentes atribuição de resposanbilidade.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 58. Nela, pode-se perceber que o alfa irá para 0,495 em caso de exclusão da RESP5.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
RESP1	13,91	4,771	,288	,119	,199
RESP2	13,65	5,819	,067	,042	,390
RESP3	13,88	5,337	,206	,270	,278
RESP4	13,76	4,460	,451	,324	,063
RESP5	14,49	6,367	-,061	,063	,495

Tabela 58 Cálculo do alfa de Cronbach no SPSS com a opção de "Scale if item deleted" para as variáveis RESP1, RESP2, RESP3, RESP4 e RESP5.

Então, como o alfa foi recalculado retirando à variável RESP5, e assim, obteve-se o valor de 0,495 (Tabela 59), que ainda é um valor inaceitável.

Alfa de Cronbach	Número de itens
0,495	5

Tabela 59 Alfa de Cronbach para as variáveis RESP1, RESP2, RESP3 e RESP4.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 60. Nela, pode-se perceber que o alfa irá para 0,559 em caso de exclusão da RESP2.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
RESP1	10,98	4,204	,245	,106	,465
RESP2	10,72	4,713	,137	,023	,559
RESP3	10,94	4,185	,314	,247	,401
RESP4	10,83	3,635	,498	,321	,225

Tabela 60 Cálculo do alfa de Cronbach no SPSS com a opção de "Scale if item deleted" para as variáveis RESP1, RESP2, RESP3 e RESP4.

Então, como o alfa foi recalculado retirando à variável RESP2, e assim, obteve-se o valor de 0,559 (Tabela 61), que ainda é um valor inaceitável.

Alfa de Cronbach	Número de itens
0,559	5

Tabela 61 Alfa de Cronbach para as variáveis CONS1, CONS4 e CONS5.

Ciente disto, foi utilizado o SPSS com a opção de "*Scale if item deleted*" que calcula o valor de alfa *n* vezes, onde *n* representa o número de itens da variável componente no questionário. O resultado é exposto na Tabela 62. Nela, pode-se perceber que o alfa irá para 0,661 em caso de exclusão da RESP1.

Estatísticas Item-Total

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
RESP1	7,20	2,770	,240	,102	,661
RESP3	7,17	2,651	,356	,247	,476
RESP4	7,06	2,251	,539	,314	,185

Tabela 62 Cálculo do alfa de Cronbach no SPSS com a opção de "Scale if item deleted" para as variáveis RESP1, RESP3 e RESP4.

Então, como o alfa foi recalculado retirando à variável RESP1, e assim, obteve-se o valor de 0,661 (Tabela 63), que é um valor fraco mas aceitável.

Alfa de Cronbach	Número de itens
0,661	5

Tabela 63 Alfa de Cronbach para as variáveis RESP3 e RESP4.

Por fim, a matriz de correlação é calculada, Tabela 64. Como as variáveis mais correlacionadas são RESP3 e RESP4, elas serão utilizadas no cálculo da análise fatorial, na perspectiva exploratória.

Estatísticas Item-Total

	RESP3	RESP4
RESP3	1,000	,485
RESP4	,485	1,000

Tabela 64 Matriz de correlação para as variáveis RESP3 e RESP4.

Apêndice H

O Apêndice H apresenta as três partes do questionário *on-line* sobre a percepção da segurança da informação dos usuários (discentes, docentes e técnicos administrativos): o convite para pesquisa (Figura 6); a caracterização do respondente (Figura 7); e a investigação dos fatores.

Convite para participação do questionário *on-line*

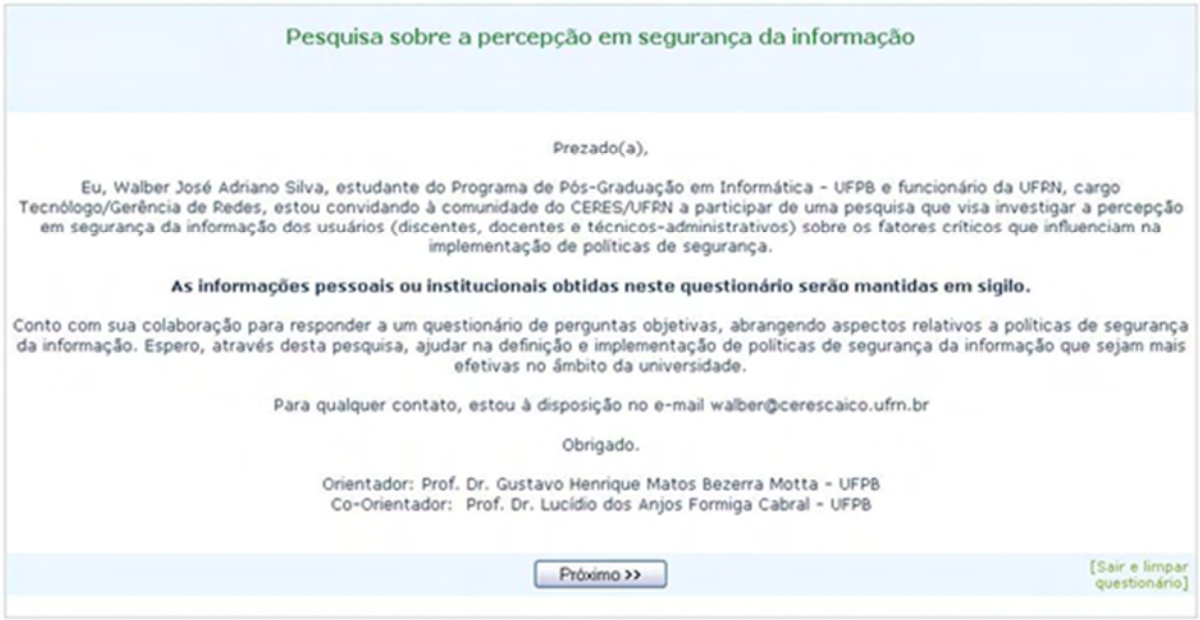

Figura 6 Convite para participação da pesquisa sobre a percepção em segurança da informação.

Descrição do respondente

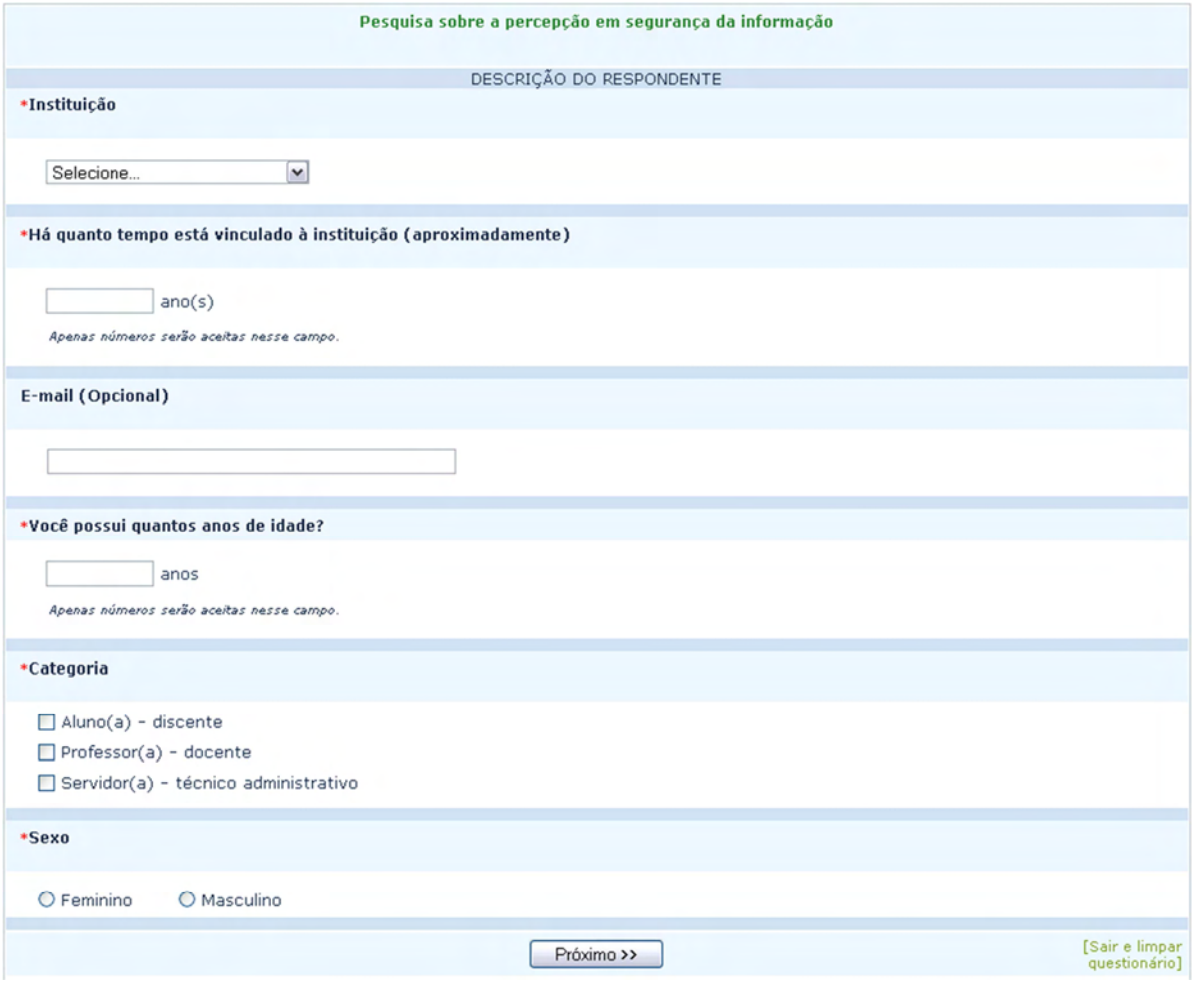

Figura 7 Parte do questionário sobre a descrição do respondente. As perguntas sobre vínculo com o curso e titulação não estão nessa figura por causa deles serem condicionados ao item sobre a categoria do respondente..

Fatores sobre a investigação dos fatores

Ambiente de liberdade acadêmica

A Figura 8 mostra os itens sobre ambiente de liberdade acadêmica no questionário *on-line*.

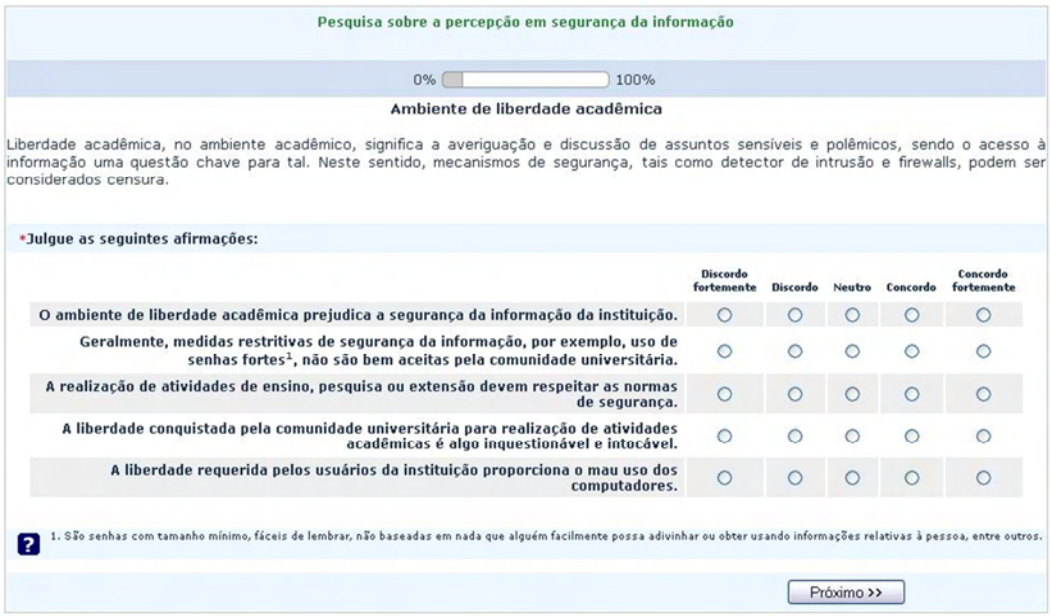

Figura 8 Questionário on-line sobre o grupo de itens do fator ambiente de liberdade acadêmica.

Apoio da administração

A Figura 9 mostra os itens sobre o apoio da administração no questionário *on-line*.

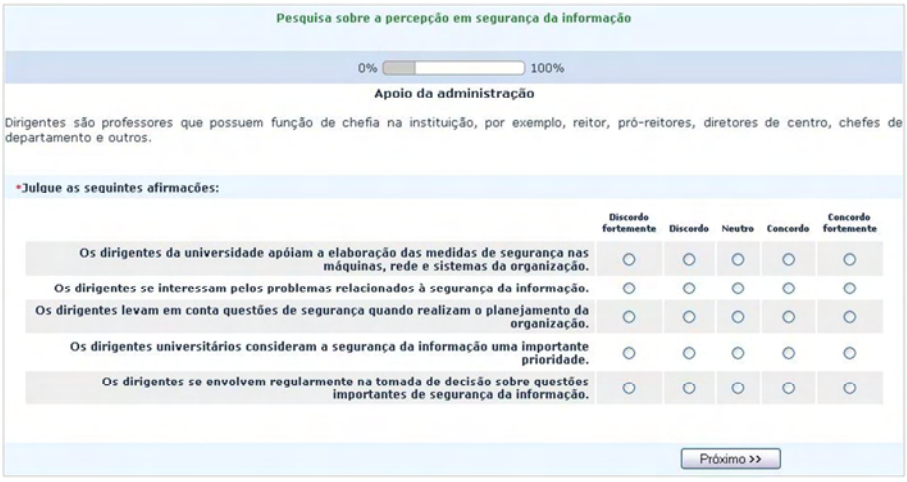

Figura 9 Questionário on-line sobre o grupo de itens que abordam o fator apoio da administração.

Comunicação

A Figura 10 mostra os itens sobre o fator comunicação no questionário *on-line*.

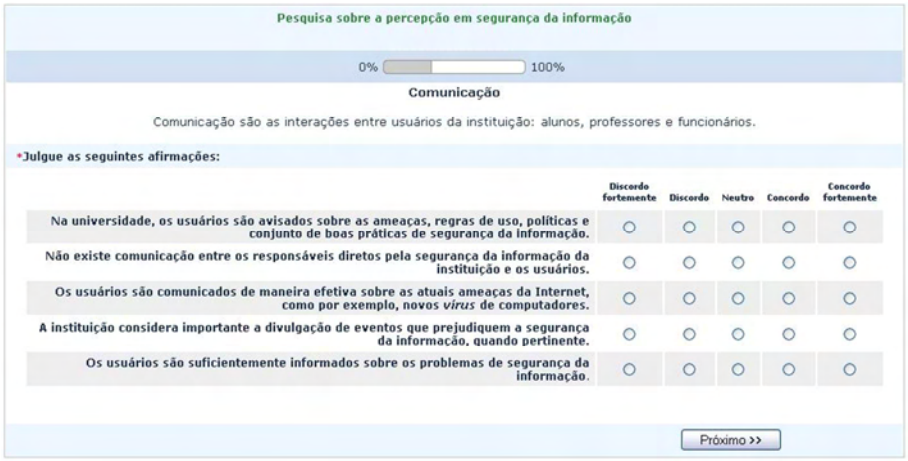

Figura 10 Questionário on-line sobre o grupo de itens que abordam o fator comunicação.

Cultura da segurança

A Figura 11 mostra os itens sobre a cultura da segurança.

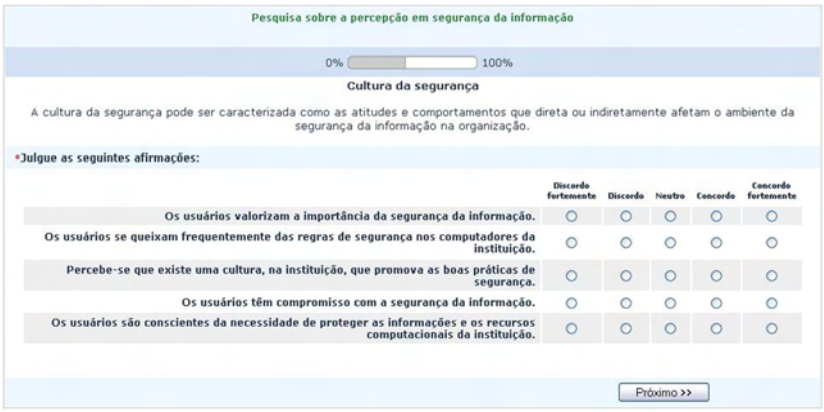

Figura 11 Questionário on-line sobre o grupo de itens que abordam o fator cultura da segurança.

Prioridade da segurança

A Figura 12 mostra os itens sobre a prioridade da segurança no questionário.

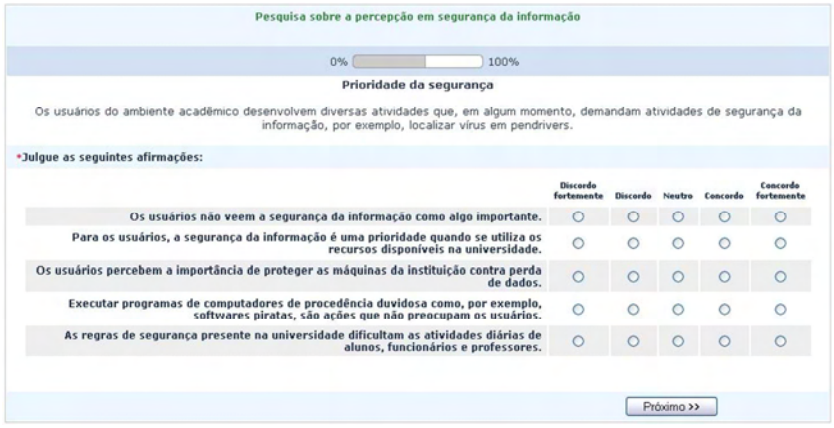

Figura 12 Questionário on-line sobre o grupo de itens que abordam o fator prioridade da segurança.

Participação na segurança da informação

A Figura 13 mostra os itens sobre a participação na segurança da informação.

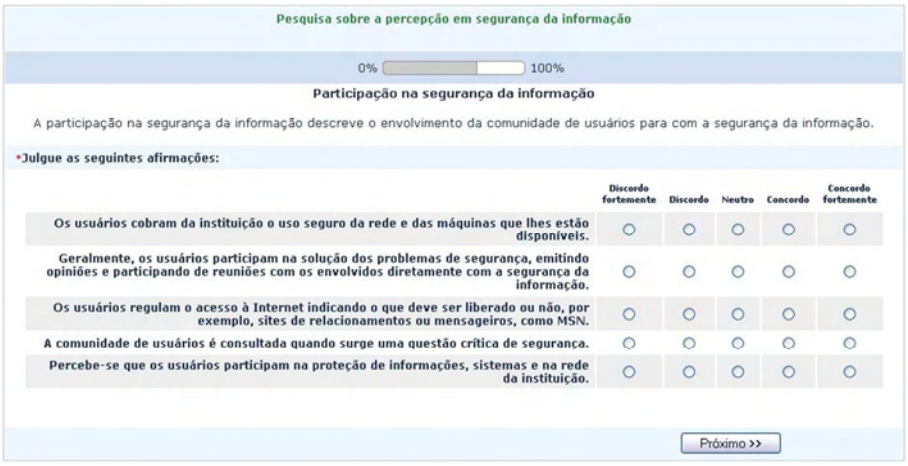

Figura 13 Questionário on-line do grupo de itens do fator participação na segurança da informação.

Programas de conscientização

A Figura 14 mostra os itens sobre o fator programas de conscientização.

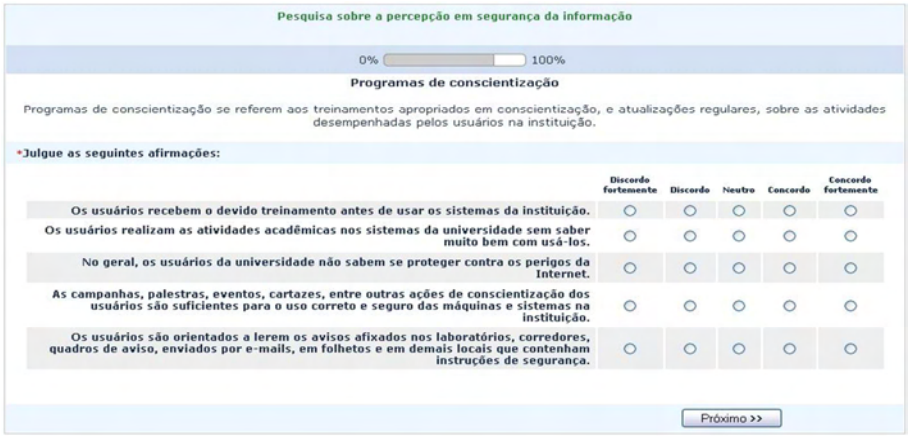

Figura 14 Questionário on-line do grupo de itens do fator programas de conscientização.

Atribuição de responsabilidade

A Figura 15 mostra os itens sobre o fator atribuição de responsabilidade no questionário *on-line*.

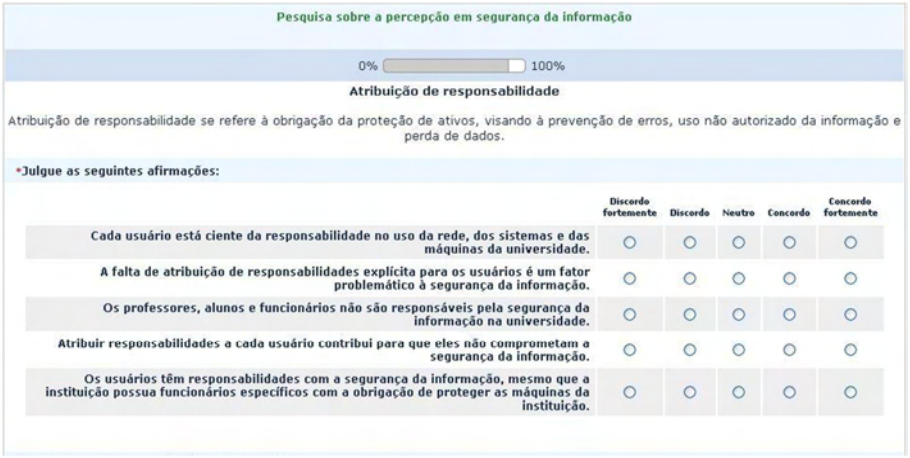

Figura 15 Questionário on-line do grupo de itens do fator atribuição de responsabilidade.