UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE PSICOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM PSICOLOGIA
SOCIAL, DO TRABALHO E DAS ORGANIZAÇÕES

Práticas organizacionais de estímulo à segurança da informação e percepção de mudança organizacional: influência nas atitudes e comportamentos de segurança

Mestrado

TALITA FREIRE ARANTES

Brasília-DF
Março, 2012

UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE PSICOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM PSICOLOGIA
SOCIAL, DO TRABALHO E DAS ORGANIZAÇÕES

TALITA FREIRE ARANTES

Práticas organizacionais de estímulo à segurança da informação e percepção de mudança organizacional: influência nas atitudes e comportamentos de segurança

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Psicologia Social, do Trabalho e das Organizações, Universidade de Brasília, como requisito à obtenção do título de Mestre em Psicologia Social, do Trabalho e das Organizações.

Orientadora:

Prof[a] Dr[a] Elaine Rabelo Neiva

Brasília-DF
Março, 2012

Práticas organizacionais de estímulo à segurança da informação e percepção de mudança organizacional: influência nas atitudes e comportamentos de segurança

Dissertação defendida aprovada pela banca examinadora constituída por:

Prof[a] Dr[a] **Elaine Rabelo Neiva** (Presidenta)
Departamento de Administração e Programa de Pós-graduação em Psicologia Social, do Trabalho e das Organizações - Unb

---

Prof[a] Dra **Gardênia Abbad** (Membro Titular)
Programa de Pós-graduação em Psicologia Social, do Trabalho e das Organizações - Unb

---

Prof. Dr. **Francisco Antônio Coelho** (Membro Titular)
Departamento de Adminsitração – Unb

Prof[a]. Dr[a]. **Catarina Odelius**(Membro Suplente)
Departamento de Adminsitração – Unb

a Deus, que meu deu asas para voar.

AGRADECIMENTOS

Agradeço a todas as pessoas que me ajudaram direta ou indiretamente na realização desse sonho.

Aos meus pais e irmãos, meu porto seguro.

A minha orientadora Elaine que me acolheu desde o primeiro momento e me ensinou a ter visão de pesquisadora.

As minhas amigas de infância por sempre estarem presentes em minha vida, me dando apoio e força.

A todos os membros do grupo de pesquisa Inovare, com quem aprendi muito.

Aos meus professores e colegas de disciplinas.

A Vanessa , colega de mestrado, que me deu auxilio na utilização do Limeservice.

Aos participantes da pesquisa, por terem dedicado um pouco de seu tempo para o preenchimento do questionário.

A Isamir por ter me ajudado enormemente com a coleta de dados.

Ao meu colega Gilmar que tanto me ajudou quando precisei.

SUMARIO

FIGURAS

TABELAS

RESUMO

A informação possui um papel estratégico no âmbito organizacional e, por isso, assegurá-la tornou-se essencial para que as organizações se mantenham competitivas no mercado. No entanto, não basta apenas investir em recursos tecnológicos, é preciso investir nas pessoas, fator fundamental da segurança da informação. Nesse sentido, essa dissertação teve como objetivo investigar como as práticas de segurança adotadas no nível organizacional e a percepção de mudança decorrente dessas geram efeitos nas atitudes e nos comportamentos dos indivíduos com relação à segurança da informação. Para tanto, foi aplicado um questionário, composto de quatro instrumentos, em uma empresa pública, totalizando 423 casos. Os seguintes instrumentos apresentaram estrutura bifatorial: Praticas Organizacionais voltadas para a rotina organizacional(α =0,90) e Práticas Organizacionais voltadas para os indivíduos(α =0,91); Percepção de Mudança Organizacional Radical (α = 0,95) e Percepção de Mudança Organizacional Incremental (α = 0,87); Atitudes negativas perante as práticas (α = 0,88) e Atitudes positivas (α = 0,81);o instrumento Comportamentos de segurança voltados para o computador de trabalho apresentou estrutura unifatorial com α = 0,89. Foram realizadas análises estatísticas dos eixos principais (PAF) e teste de mediação por meio de regressão múltipla. Os resultados evidenciaram a existência de relações entre as práticas organizacionais de segurança (R^2 = 0,28), a percepção de mudança organizacional radical atribuída à segurança (R^2 = 0,27) e comportamento de segurança relacionada ao computador de trabalho (R^2 = 0,12) mediada pelas atitudes positivas frete as práticas de segurança (R^2 = 0,17). Foram encontradas as seguintes limitações: as medidas utilizadas foram adaptadas para a realidade da organização e se limitaram a autoavaliação dos participantes. Os achados nessa pesquisa podem ser utilizados na elaboração de programas de Segurança da Informação nas organizações.

Palavras-chave: Segurança da Informação, Práticas Organizacionais de Segurança da Informação, Percepção de mudança organizacional, Atitudes perante as práticas de segurança e Comportamentos de Segurança da Informação.

ABSTRACT

Information plays a strategic role in the organizational environment, therefore its security is crucial to remain organizations competitive. In this context, it is important to pay attention not only to technology resources, but also to people that are an essential factor of the information security. This paper aims to understand the individual security behavior in the work environment, testing a mediation model which identifies two antecedents of security behavior: organizational practices of information security and organizational change perception toward practices, and security practices-related attitudes as the mediator variable. For this study, an instrument composed by four ten-point Likert scales was used. Three scales were developed and validated to measure the practices, attitudes and behavior toward 61 statements. A ten-point scale was revalidate to measure the organizational change perception toward 30 statements. The scales presented a two-dimensional structure: organizational routine practices-related α =0,90, individual practices-related α = 0,91 , incremental change α= 0,80, radical change α= 0,89,negative attitudes α = 0,87, positive attitudes α = 0,80. Computer behavior-related presented a one-dimensional structure α = 0,71. Data were collect from 623 cases in a Brazilian public organization by on-line survey. Descriptive analyses, exploratory factor analysis and regression analysis were done. The results showed that security practices-related attitudes mediated the relation between the organizational and individual levels, that is, in so far as the organization implements security practices the individuals perceive radical organizational change (R^2=0,28) and present positive security practices-related attitudes , which in turn, impact information security behavior (R^2=0,15).

Key-words: Information Security, Information Security Organizational Practices, Percepção de mudança organizacional Organizational Change Perception, Attitudes toward security pratices and Information Security Behavior

APRESENTAÇÃO

A informação possui um papel estratégico no âmbito organizacional e, por isso, assegurá-la tornou-se essencial para que as organizações se mantenham competitivas no mercado. Os recursos tecnológicos, tais como *firewall, IDS* e antivírus representam uma proteção às informações. No entanto, não são suficientes para garantir integralmente a segurança, sendo necessário que seja dada importância, igualmente, aos recursos humanos. Portanto, este estudo abordará a Segurança da Informação nas organizações com enfoque nos indivíduos envolvidos.

A adoção de práticas e procedimentos de Segurança da Informação (SI) tornou-se uma necessidade inevitável para as organizações públicas e privadas. Por meio dessas, obtêm-se a confidencialidade, integridade e disponibilidade – três pilares fundamentais à segurança. Dessa forma, na tentativa de se prover segurança nas organizações, altas somas são investidas em sistemas criptográficos, equipamentos de redes de computadores e, até mesmo, elaboração de normas e políticas. No entanto, pesquisas demonstram que os maiores danos na área são ocasionados por indivíduos e não pelos recursos tecnológicos.

De acordo com Dias (2001), os danos mais comuns em instituições do Reino Unido são provocados por erros humanos (52%); incêndios (15%); atividades desonestas (10%); sabotagem (10%); água (10%); e terrorismo (3%). Além disso, as causas de tais danos são funcionários internos (81%), pessoas externas à organização (13%) e ex-funcionários (6%). Apesar das porcentagens mostrarem a importância da adoção de comportamento de segurança por parte dos indivíduos, muitas organizações ainda tendem a ignorar tais estatísticas. O resultado é que os investimentos em segurança da informação são, em sua maioria, voltados para a tecnologia e pouco ou nada é direcionado para o aspecto humano.

É possível, porém, utilizar o aspecto humano para compensar as deficiências dos processos e da tecnologia da segurança da informação, conforme dispõe Zafra et al. (1998). Para tanto, faz-se necessário conscientizar os indivíduos dos riscos ao qual a informação está exposta e da importância em assegurá-la, de forma a motivá-los a adotar as práticas e

procedimentos de segurança da organização e, consequentemente, passar a ter um comportamento voltado para a segurança.

Consoante Vieira (2009), a adoção das práticas de segurança gera mudanças na organização, nos comportamentos de seus funcionários e em sua cultura. No entanto, as mudanças resultantes desse processo podem gerar resistências de certos indivíduos ou grupos, levando-os adotarem parcialmente as práticas, ou mesmo, não as adotarem. Por isso, ao se falar em segurança da informação é importante levar em conta a mudança organizacional por ela ocasionada. Para Neiva (2004), uma das maneiras de se avaliar a mudança é mensurar o que os indivíduos percebem ter mudado na organização.

É importante, também, considerar o impacto das práticas de segurança e da mudança organizacional nas atitudes e comportamentos dos indivíduos, já que as atitudes podem levar um indivíduo a um comportamento desejável ou não. Para Robins (2005), os indivíduos buscam a consistência entre a atitude e o comportamento, ou seja, as pessoas tendem a moldar seu comportamento de acordo com as suas atitudes. Além disso, esse construto apresenta forte relação com mudanças nas organizações, ou seja, para que se tenha sucesso em uma mudança é necessário que os indivíduos envolvidos mudem seu comportamento.

Diante do acima exposto, a presente pesquisa se justifica pela importância em se avaliar como as práticas de segurança da informação e as mudanças ocasionadas por elas afetam as atitudes e comportamentos dos indivíduos. Justifica-se, também, pela falta de estudos com abordagem quantitativa que investiguem as práticas de segurança da informação e sua relação com variáveis individuais. Além disso, buscou-se lançar luz à importância em se trabalhar de forma integrada os aspectos tecnológicos e humanos da segurança nas organizações.

Nesse sentido, propôs-se a seguinte pergunta de pesquisa:

As práticas organizacionais de segurança da informação e a percepção de mudanças atribuídas a essas práticas influenciam as atitudes e a adoção de comportamentos de segurança da informação nas organizações?

O objetivo principal da presente pesquisa foi investigar a interferência das práticas de segurança adotadas no nível organizacional e a percepção de mudança delas decorrente nas

atitudes e nos comportamentos dos indivíduos com relação à segurança da informação. Para tanto, foram delimitados os seguintes objetivos específicos:

a) Identificar as práticas de segurança da informação adotadas pela organização;
b) Identificar a percepção de mudança organizacional dos indivíduos após a adoção de práticas de segurança da informação;
c) Descrever as atitudes dos indivíduos com relação às práticas de segurança da informação;
d) Identificar o comportamento dos indivíduos com relação à segurança da informação;
e) Construir e validar as escalas de Práticas Organizacionais de Segurança da Informação, Percepção de Mudança Organizacional atribuída às Práticas de Segurança, Atitudes frente às Práticas de Segurança da Informação e Comportamentos de Segurança da Informação;
f) Testar o modelo de mediação entre as variáveis independentes Práticas Organizacionais de Segurança da Informação e Percepção de Mudança Organizacional atribuída às práticas e a variável dependente Comportamento de Segurança da Informação, tendo como variável mediadora Atitudes frente às práticas.

1 SEGURANÇA DA INFORMAÇÃO

Na era do conhecimento, a informação tornou-se um dos principais patrimônios das organizações, haja vista que é considerada um recurso crítico para os negócios (Dias, 2001). Consequentemente, esse ativo organizacional encontra-se em constante risco de ataques, seja por pessoas internas ou externas à organização e, por isso, a sua segurança representa um fator essencial para a sobrevivência das instituições (Dias, 2001). Nesta seção, será apresentada uma análise dos principais conceitos de segurança da informação.

1.1 Conceitos em Segurança da Informação

Para se compreender a segurança da informação, é fundamental entender o que vem a ser informação, ameaça e vulnerabilidade. O conceito de informação difere-se dos conceitos de dados e conhecimento. Consoante explanações de Passos (2005), dados são simples observações acerca do mundo que por si só nada representam. A informação, por sua vez, é um conjunto de dados que possui um significado por si só. E o conhecimento é algo tácito do ser humano, resultado de informações que este absorveu em um determinado momento.

Dessa forma, o que se espera hoje do indivíduo é que ele tenha capacidade de produzir conhecimentos a partir das informações que possui e que serão utilizados em prol da evolução. Já a informação é um ativo para qualquer organização, independente da atividade.

Vale ressaltar que o valor da informação varia conforme suas características. Quando suas características mudam, o valor da informação pode aumentar ou diminuir. Algumas características afetam o valor da informação para seus usuários mais do que outras. Isso depende das circunstâncias como, por exemplo, o fator tempo, que pode ser critico para a informação, já que muito do valor da informação pode ser perdido se esta for entregue ao destino com grande atraso (Whitman & Mattord, 2011).

O ativo informação está sobre constante risco de ataques que são provocados por ameaças. Nesse contexto, define-se ameaça como fatos que podem vir a ocorrer e causar algum dano para a organização. Podem ser classificadas como ameaças intencionais, tais como furto e vandalismo; e não intencionais, como erros humanos. Ademais, quando exploram vulnerabilidades geram incidentes de segurança. As vulnerabilidades, por sua vez,

representam fragilidades nos ativos organizacionais, fraquezas ou falta de proteção contra ameaças (ABNT ISO/IEC 27002:2007). Pode-se, portanto, dizer que o papel da segurança da informação nas organizações é reduzir o risco, ou seja, a probabilidade de uma ameaça ocorrer, por meio de práticas e procedimentos que visam reduzir as vulnerabilidades, evitando que essas sejam exploradas por ameaças.

Conforme disposto na norma ABNT NBR ISO/IEC 27002 (2007), a segurança da informação visa prover proteção contra ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio; maximizar o retorno sobre os investimentos; e as oportunidades de negócio. Dias (2001) acrescenta que o termo se refere à proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, reduzindo a probabilidade e o impacto de incidentes de segurança.

Consoante Whitman e Mattord (2011) risco consiste na probabilidade que alguma coisa não desejada irá acontecer. Os autores conceituam, também, sujeitos ou objetos, como um computador, que pode ser tanto um sujeito de um ataque (utilizado para realizar um ataque) ou o objeto (entidade alvo de um ataque). Já ameaça representa a categoria de objetos, pessoas ou entidades que representam um risco para um ativo e vulnerabilidade a fraqueza ou falha em um sistema ou mecanismo de proteção que pode sofrer um ataque ou risco.

Para Whitman e Mattord (2011), entende-se como informação segura, aquela que se encontra protegida inicialmente, quanto a três principais aspectos, a saber:

a) Integridade – as informações não podem sofrer alterações, supressões ou adições sem autorização;
b) Disponibilidade – a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado;
c) Confidencialidade – somente pessoas autorizadas pela empresa devem ter acesso à informação.

Além desses, outros aspectos importantes que a segurança visa prover são a autenticidade e irretratabilidade ou legalidade. De acordo com Dias (2001), a autenticidade é a capacidade de identificar e reconhecer formalmente a identidade dos elementos de uma

comunicação eletrônica ou comércio. Legalidade, por sua vez, refere-se a característica das informações que possuem valor legal dentro de um processo de comunicação. Tais aspectos são alcançados por meio da adoção de controles de segurança adequados, que podem envolver processos, *softwares* e *hardwares*. Esses controles são, por sua vez, classificados como físicos ou lógicos e incluem políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais.

Para Whitman e Mattord (2011), para que uma organização obtenha sucesso, deve implantar as seguintes camadas de segurança a fim de proteger suas operações:

a) Segurança Física - para proteger itens físicos, objeto ou infraestrutura de acesso ou uso não autorizado;
b) Segurança pessoal – proteger o indivíduo ou um grupo de indivíduos que são autorizados a acessar a organização e suas operações;
c) Segurança de operações – para proteger detalhes de uma operação particular ou séries de atividades;
d) Segurança das comunicações – para proteger comunicações de mídia, tecnologia e conteúdo.
e) Segurança de redes – para proteger os componentes de rede, conexões e conteúdos.
f) Segurança da informação – para proteger a confidencialidade, integridade e disponibilidade dos ativos de informação, estando armazenados, em processamento ou transmissão. Isso é alcançado por meio de aplicação de políticas, educação, treinamento e conscientização, e tecnologias.

O Comitê de Segurança Nacional de Sistemas (CNSS) dos Estados Unidos define segurança da informação como proteção de informação e seus elementos críticos, incluindo os sistemas e *hardwares* que utiliza, armazena e transmite a informação (Whitman & Lattord,2011). Para os autores, a tríade confidencialidade, disponibilidade e Integridade, já citada anteriormente, baseia-se nas características da informação e seu valor para as organizações. No entanto, esta tríade já não é mais adequada para as constantes mudanças que o mundo vive. Isso porque as ameaças à confidencialidade, integridade e disponibilidade da informação incluem uma vasta gama de eventos, como danos acidentais ou intencionais,

destruição, roubo, modificação não autorizada, ou falta de conhecimento dos indivíduos. Este novo ambiente de várias constantes envolvem ameaças que exigem o desenvolvimento de um modelo mais robusto voltado para a complexidade do atual ambiente da segurança da informação.

Devido a sua importância para o cotidiano das pessoas e para contexto organizacional, surgiram padrões de fato que visam auxiliar a adoção da segurança da informação nas organizações. Dentre eles, destacam-se as normas internacionais ISO/IEC 27001 e ISO/IEC 27002. A primeira dispõe sobre o sistema de gestão da segurança da informação, já a segunda consiste em um conjunto de boas práticas de segurança, ambas voltadas para as organizações. Estas normas já possuem versão em português e foram transformadas em normas da ABNT. A ISO/IEC 27002 será descrita mais adiante tendo em vista que foi utilizada como base teórica para elaboração de um dos instrumentos desta pesquisa.

1.2 O papel do indivíduo na segurança da informação

Os indivíduos constituem um importante fator da segurança da informação. Na literatura, são conhecidos como o elo fraco que compõe a corrente da segurança (Dias, 2001), já que podem representar uma ameaça à segurança quando burlam esquemas de segurança ou adotam comportamentos maliciosos. No entanto, podem representar uma barreira para prevenir incidentes na medida em que adotam práticas preventivas, como etiqueta de senhas e cuidado com manuseio de e-mails. Tais comportamentos são influenciados por diversos fatores, a saber: características pessoais; estruturas administrativas; ativos físicos e tecnológicos; e normas sociais.

Nesse sentido, o elo fraco da segurança não deve ser explicado apenas por falhas e violações do indivíduo, como também, por fatores do contexto de seu ambiente de trabalho que podem gerar comportamentos negativos (Albrechtsen, 2007). Lidar com barreiras humanas é muito mais complexo do que lidar com medidas tecnológicas, sendo esse um desafio para os gerentes de segurança da informação. Afinal, como as organizações podem influenciar o comportamento e atitudes de seus funcionários?

A literatura da área tem enfatizado a importância em se adotar ações voltadas para os indivíduos nas organizações, tais como programas de conscientização, treinamento e educação. Albrechtsen (2007) afirma que fatores organizacionais e culturais também devem ser considerados ao se tratar de comportamentos e atitudes em segurança da informação.

Albrechtsen (2007) aponta que o principal problema com relação ao papel do usuário na Segurança da Informação é a falta de motivação e conhecimento com relação ao assunto, o que pode ser explicado por características individuais ou mesmo por valores do grupo. Embora os indivíduos estejam cientes de seu papel na segurança da informação no trabalho, existe uma lacuna entre o comportamento real e intencional, pois, na prática, não desempenham muitas ações de SI e nem, ao menos, estão familiarizados com suas práticas e procedimentos.

1.3 Práticas organizacionais em Segurança da Informação

As práticas organizacionais, uma das variáveis que serão analisadas na presente pesquisa, se referem a intervenções adotadas na organização que estimulem os indivíduos a adotarem novos comportamentos e atitudes de segurança da informação. A norma internacional ISO/IEC 27002 de 2007, que possui uma versão traduzida da ABNT, constitui um guia de melhores práticas em segurança da informação mundialmente aceito. Tais práticas são agrupadas pela norma em sete grupos representados na Figura 1.

GRUPOS	**PRÁTICAS RELACIONADAS**
Documento da Política de Segurança da Informação	- Divulgar a política de segurança da informação para todos.
	- Manter os funcionários atualizados sobre mudanças na política.
Atribuição de responsabilidades para a Segurança da Informação	-Definir ativos e processos de segurança da informação associados com cada sistema;
	-Atribuir responsabilidades para o gestor responsável por cada ativo ou processo de segurança da informação.
	-Definir níveis de autorização para acessos às informações.
Conscientização, educação e treinamento em segurança da	- Realizar workshops e palestras sobre segurança da informação

GRUPOS	PRÁTICAS RELACIONADAS
informação	-Oferecer treinamento em segurança da informação para todos os funcionários da organização.
Processamento correto nas aplicações	-Definir responsabilidade de todo o pessoal envolvido no processo de entrada de dados.
	- Implementação de sistema ou diretriz de classificação da informação.
	- Criptografar mensagens cujo conteúdo seja sensível.
	- Implementação de controles de acesso apropriados aos ativos de informação.
Gestão de vulnerabilidades técnicas	-Manter um inventário completo e atualizado dos ativos de informação.
	-Realizar análise/avaliação de riscos de vulnerabilidades.
	-Definir ações para tratamento de vulnerabilidades técnicas.
Gestão de continuidade do negócio	-Contratar serviços de seguradora para manter a continuidade dos serviços em caso de incidentes.
	-Adotar um plano de continuidade do negócio que esteja alinhado com a estratégia organizacional.
Gestão de incidentes de segurança da informação e melhorias.	-Adotar procedimentos para manusear diferentes tipos de incidentes como falhas de sistemas, código malicioso, violação de confidencialidade e integridade, dentre outros.

Figura 1. Grupos de práticas em segurança da informação da Norma ISO/IEC 27002 : 2007

As práticas de segurança, quando adotadas pela organização, podem influenciar nas atitudes dos indivíduos quanto à segurança da informação. Portanto, no próximo tópico será analisado o construto atitudes.

1.4 Atitudes frente à segurança da informação

Atitude é um construto que têm sido objeto de inúmeros estudos na área de psicologia, tendo como foco, principalmente, sua capacidade para predizer comportamentos (Ajzen, 1991). A história da pesquisa em atitudes originou-se do século passado, a partir de estudos nos anos vinte, que geraram muitas implicações para as medidas e para seu desenvolvimento teórico, conforme dispõe Neiva e Mauro (2011).

Muitas são as definições encontradas na literatura para esse construto. No entanto, Neiva e Mauro (2011) alertam que o termo tem sido utilizado de forma indiscriminada do significado que este assume na linguagem cotidiana, sendo um grave equívoco. Faz-se, portanto, importante conhecer as diferentes conceituações de atitude.

Segundo Santos (2001), atitude é uma reação ou maneira como cada indivíduo responde, favoravelmente ou não, a determinados objetos ou situações. Atitudes podem predizer a intenção de um indivíduo para desenvolver um comportamento em relação ao objeto conhecido. Nesse contexto, atitudes afetam a escolha de ação ou comportamento em relação a pessoas, objetos ou eventos. Por exemplo, uma atitude favorável, geralmente, eleva a probabilidade do indivíduo de estudar e reter informações em uma dada situação.

Por outro lado, uma atitude negativa pode bloquear o aprendizado e a retenção de novas informações. Dessa forma, qualquer que seja a atitude, ela pode influenciar no desenvolvimento de um comportamento que exija respostas a determinadas situações. Azjen (1991) classifica a atitude em dois tipos, a saber: atitudes em face de objetos físicos (racial, éticos e outros grupos, instituições, policias, eventos, dentre outros) e atitudes frente à execução de um comportamento específico relacionado a um objeto ou meta, ou seja, atitudes relacionadas a comportamento. O autor, portanto, dispõe que atitudes podem ser específicas ou genéricas.

Dentre as várias definições de atitudes, observa-se que estas tendem a caracterizar as atitudes sociais como variáveis não observáveis, porém diretamente inferíveis de observações e como sendo integradas a partir dos seguintes componentes: cognitivo, afetivo e comportamental. Há, no entanto, divergência na literatura sobre os componentes que formam a

estrutura do construto, tais como : bicomponente (afeto e cognição), unicomponente (afeto) e tricomponente (afeto, cognição e comportamento). Neiva e Mauro (2011) destacam que o modelo de três componentes é um dos mais adotados na área. Nesse sentido, afeto constitui a forma como uma pessoa se sente em relação a um objeto e apresentam estados agradáveis ou desagradáveis quanto a ele. O componente cognitivo, por sua vez, inclui percepções, conceitos e crenças acerca do objeto da atitude. Já o componente comportamental pode ser entendido por meio das teorias da relação atitude-relacionamento presentes na literatura, tais como a teoria da ação planejada de Azjen (1988) e a teoria da ação racional de Fishbein e Azjen (1975), já que existe uma pré-disposição no indivíduo para realizar uma ação, que ao se combinar com uma situação específica desencadeante, resulta em um comportamento (Neiva & Mauro, 2011).

Segundo Azjen (1991), algumas pesquisas demonstraram que o construto atitude apresentava-se como um baixo preditor do comportamento real, e por isso, muitos psicólogos sociais começaram a rever a utilidade de tal construto na predição do comportamento, já que existem outras variáveis que podem interferir no construto. Ou seja, o simples fato de o indivíduo possuir uma atitude positiva com relação a um alimento não significa que este irá consumí-lo.

Além disso, essa descrença quanto à utilidade do construto atitude ocorreu, também, pois as medidas empregadas eram sistematicamente distorcidas ou enviesadas e não refletiam a verdadeira atitude de uma pessoa. Foram criadas, então, medidas menos subjetivas para evitar vieses, tal como o da desejabilidade social. Outra preocupação com a medição desse construto é que todas as técnicas resultavam em único escore representando a atitude negativa ou positiva do indivíduo, e muitos teóricos acreditavam que esta forma não contemplava a complexidade da atitude.

Quanto à forma de mensuração das atitudes, destacam-se as medidas autodescritivas – modelo adotado neste estudo, sendo as escalas mais comuns: a escala Likert, escala de diferencial semântico, escala de Guttman e escala de distância social. No entanto, Neiva e Mauro (2011) alertam para o fato de que, algumas vezes, as pessoas não estão dispostas a

revelar suas verdadeiras atitudes e, por isso, nem sempre esse tipo de escala fornece as melhores informações.

Gouveia et al.(2007) realizaram um estudo com objetivo de conhecer evidências de validade fatorial e preditiva de uma medida de atitudes ante o uso de drogas em geral. A medida era composta por quatro itens bipolares (positivo/negativo, gosto/desgosto, bom/ruim e desejável/indesejável) em uma escala do tipo diferencial semântico de 9 pontos, variando de -4 a +4 e estrutura unifatorial. Com a regressão logística, pôde-se comprovar que as pontuações no instrumento predisseram significativamente a condição de ser um usuário de drogas. Os autores destacaram que a medida pode ser utilizada como uma forma de se conhecer o potencial envolvimento dos jovens com drogas. No entanto, alertam que os resultados não podem ser extrapolados para outros grupos, já que a amostra foi constituída essencialmente de estudantes universitários.

Outro estudo sobre atitudes, realizado por Gouveia et al. (2002), verificou a relação desse construto com a avaliação psicológica para condutores. Para tanto, foi desenvolvida uma escala composta por 20 itens do tipo Likert 9 pontos (0= Nada Eficiente e 9 = Totalmente Eficiente), na qual era perguntado se o respondente acreditava na eficiência do serviço de avaliação psicológica que o DETRAN realizava. Ao realizar a análise fatorial dos Eixos Principais, com rotação varimax, foram retidos três fatores: processo de avaliação, eficácia da avaliação e descrédito do profissional. Ao final, os respondentes apresentaram uma atitude positiva frente à eficácia da avaliação. A amostra foi dividida em grupos de usuários do DETRAN, estudantes de Técnicas de Exame Psicológico, profissionais que trabalham na avaliação psicológica e as médias dos fatores foram comparadas a eles. Nesse sentido, houve diferença entre as médias no fator processo de avaliação. Já no fator eficácia de avaliação e descrédito do profissional, não houve diferença estatisticamente significativa.

Com relação à Segurança da Informação, não existe na literatura uma conceituação específica do que seja atitudes frente a segurança. No entanto, existem alguns conceitos sobre atitudes relacionadas a tecnologias computacionais, como o conceito de Smith et al. (2000) que tem como base o estudo de Fishbein e Ajzen (1975), no qual a atitude ante o computador é definida como a avaliação geral de uma pessoa ou sentimento favorável ou não em face das

tecnologias computacionais (e.g.. atitudes frente a objetos) e atividades específicas relacionadas a computador (e.g. atitude frente a comportamento).

Em seu estudo, Smith et al. (2000) utilizaram duas escalas para mensurar as atitudes dos usuários sobre computador. Uma foi desenvolvida por Dambrot et al. (1985) e apresentava 20 itens, sendo que 9 se referiam a atitudes positivas - como " Acho que computadores são facilitadores" – , e 11 negativos – como " Em geral, tenho sentimentos negativos com relação a computador". Já a outra escala, elaborada por Loyd e Gressard (1984) possui três fatores, quais sejam: ansiedade com relação ao computador, gosto pelo computador e confiança no computador.

De acordo com os resultados alcançados pelos autores, atitudes frente ao uso de correio eletrônico, que pertence à escala Experiência Subjetiva com relação ao computador, se apresentou um construto independente dos demais. Os autores concluíram, portanto, que experiência subjetiva com relação a computador e atitudes frente ao uso de computador são construtos distintos.

Em outra pesquisa sobre atitudes, agora, no contexto da segurança da informação, Thomson e Solms (1998) apresentam um sistema de atitudes de Zimbardo e Leippe (1991) para explicar a forma como diferentes aspectos determinam o comportamento de um indivíduo e como estes podem ser utilizados no processo de conscientização e treinamento de usuários em segurança.

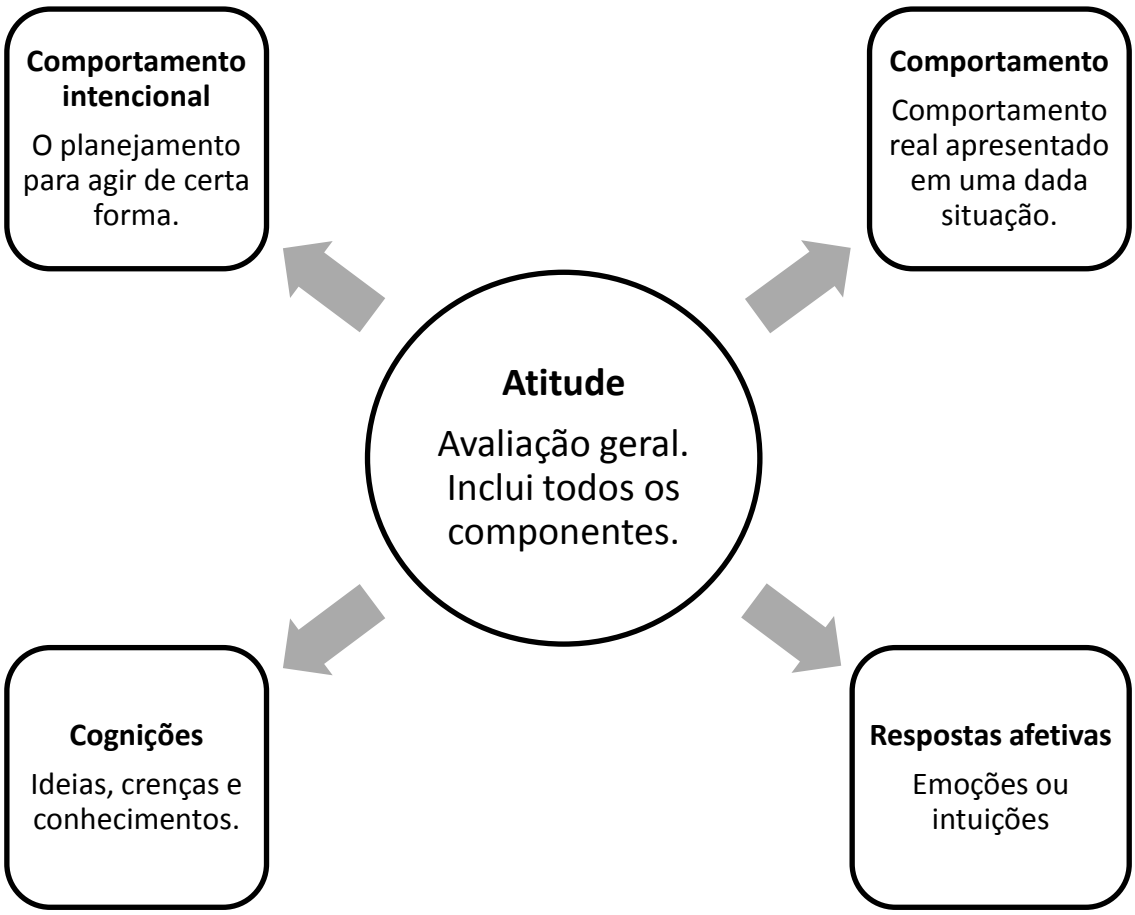


Figura 2. Aspectos que determinam o comportamento do indivíduo.

No modelo (Figura 2), todas as áreas estão inter-relacionadas e, como consequência, uma mudança em uma pode afetar todas as outras. Para os autores, a mudança na atitude gera um resultado de modificação em longo prazo no comportamento. Dessa forma, métodos que utilizem, por exemplo, o aprendizado instrumental e o comprometimento podem tornar programas de conscientização em Segurança da Informação mais efetivos de forma a mudar as atitudes e comportamentos dos indivíduos.

Devido ao poder preditivo do construto atitude com relação ao comportamento demonstrado na literatura, o tópico seguinte abordará a relação entre esses dois construtos.

1.5 Relação Atitude-Comportamento

Atualmente, umas das mais respeitadas teorias sobre a relação atitude-comportamento é a Teoria do Comportamento Planejado (TCP) de Azjen (1985). Tal teoria dispõe que as intenções para desempenhar comportamentos de diferentes tipos podem ser determinadas

com alta acurácia por meio de atitudes ante um comportamento, normas subjetivas, e controle do comportamento percebido; e estas intenções juntamente com percepções de controle comportamental, produzem considerável variância no comportamento real.

Na TCP, as intenções comportamentais são determinadas por três construtos independentes, a saber: atitude do sujeito em relação ao comportamento – avaliação favorável ou desfavorável quanto ao objeto, pessoa, instituição ou evento em questão; norma subjetiva – pressão social, percebida pelo sujeito, para se comportar ou não de tal maneira; grau de controle comportamental percebido – associado à facilidade ou dificuldade percebida pelo sujeito para manifestar o comportamento (Azjen, 1991).

A teoria do comportamento planejado é uma extensão da teoria da ação razoável de Fishbein e Ajzen (1975) criada devido às limitações do modelo original em lidar com comportamentos sobre os quais as pessoas possuem controle volicional incompleto. Portanto, um fator central na teoria do comportamento planejado é a intenção do indivíduo em desempenhar um dado comportamento. As intenções capturam fatores motivacionais que influenciam o comportamento de como pessoas desejam tentar e de quanto esforço estão planejando empregar a fim de desempenhar o comportamento. Como regra geral, quanto maior a intenção para adotar um comportamento, maior a probabilidade deste ser desempenhado (Azjen, 1991).

Consoante Azjen (1991), para modificar o comportamento, intervenções podem ser direcionadas a um ou mais de seus três determinantes: atitudes, normas subjetivas ou controle percebido. Uma vez que os indivíduos tenham verdadeiro controle sobre o comportamento, novas intenções comportamentais podem ser produzidas e convertidas em comportamento real.

Para Fishbein e Azjen (1975) as ações dos indivíduos são sistematicamente relacionadas à suas atitudes quando a natureza dos preditores atitudinais e o critério comportamental são levados em consideração. Segundo os autores, a atitude de um indivíduo é considerada uma avaliação de uma entidade em questão. Já o critério comportamental é considerado uma ou mais ações observáveis desempenhadas por um indivíduo e registradas

de alguma forma pelo observador. Assim, ações comportamentais incluem participação em reunião, uso de anticoncepcional, aquisição de um produto, dentre outros.

Há fortes evidências de que o envolvimento e experiências diretas com o objeto atitude tendem a melhorar a predição de um comportamento específico a partir de atitudes gerais, conforme dispõe Fishbein e Ajzen (1975). Os autores destacam que atitudes baseadas na experiência direta (e.g., observação das atitudes e comportamento dos indivíduos) têm maior poder preditivo do comportamento subsequente do que atitudes baseadas em informação de segunda mão (e.g., indivíduos descrevem suas atitudes e comportamentos).

Fishbein e Ajzen (1975) realizaram uma revisão de literatura com estudos empíricos a fim de demonstrar que atitudes gerais não são boas preditoras de um comportamento específico. Nesse sentido, para que um preditor atitudinal corresponda ao critério comportamental é necessário que a entidade atitudinal seja idêntica em todos os quatro elementos (alvo, ação, contexto e tempo) aos da entidade comportamental. Por exemplo, uma atitude frente ao alvo “minha igreja” (sem especificação da ação, contexto ou tempo) corresponde diretamente apenas ao critério comportamental baseado na observação de diferentes comportamentos com relação à igreja do indivíduo (e.g., doação de dinheiro, participação aos domingos, participação em atividades da igreja,etc.), em diferentes contextos, e em diferentes pontos do tempo.

Similarmente, quando a medida de atitude é uma avaliação de uma ação especifica frente a um dado alvo, tal como atitude frente a “ doação de dinheiro em minha igreja”, o critério comportamental correspondente é um índice de doações monetárias do indivíduo baseada em observações múltiplas do comportamento em diferentes contextos (e.g., em casa, na igreja,etc.) e em diferentes ocasiões. Alternativamente, quando o critério comportamental é um ato único, tal como participação ou não no culto da igreja no próximo domingo às 10 horas da manhã, o preditor atitudinal poderia ser medida por meio da avaliação do indivíduo sobre “participação no culto da minha igreja no domingo às 10 horas da manhã”.

Fishbein e Azjen (1975) asseveram que a força da relação atitude-comportamento depende, em grande parte, do grau de correspondência entre as entidades comportamentais e

atitudinais. Nesse sentido, alta correlação entre atitude-comportamento não existe na ausência de correspondência entre as duas entidades envolvidas.

Os autores afirmam que, de acordo com o modelo de Fazio (1990), os indivíduos que possuem atitudes favoráveis com relação ao objeto têm maior probabilidade de perceber seus atributos positivos, já os indivíduos com atitudes desfavoráveis direcionam, em geral, sua atenção para as qualidades negativas do objeto. Tais percepções do objeto influenciam as definições da pessoa acerca do evento, possivelmente direcionando sua atenção para consequências negativas ou positivas e, consequentemente, influenciando seu comportamento com relação ao objeto. Nesse caso, o comportamento é guiado por uma atitude geral. O modelo de Fazio (1990) mostrou, igualmente, que a experiência direta com o objeto relacionado à atitude produz maior relação comportamento-atitude do que a informação de segunda mão.

A teoria do comportamento planejado de Azjen (1990) apresenta algumas variáveis antecedentes do comportamento, conforme as seguintes hipóteses:

1. Intenção é a variável antecedente do comportamento real.
2. Intenção, por sua vez, é determinada pela atitude em face o comportamento, norma subjetiva e controle comportamental percebido.
3. Esses determinantes são uma função, respectivamente, de crenças de controle, normativas e comportamentais.
4. Crenças de controle, normativas e comportamentais podem variar em função de diversos fatores.

Como variáveis preditoras de intenções, os autores destacam a auto-eficácia, as normas subjetivas e as atitudes, podendo variar conforme a função do comportamento e a população sob investigação.

A maioria dos estudos que investigam a relação atitude-comportamento focam-se nas atitudes frente a instituições, políticas, grupos étnicos, dentre outros. No entanto, estes tendem a ser baixos preditores de comportamento específico, o que levou pesquisadores a acreditarem

que atitudes ante um comportamento é muito especifico para ter alguma significância psicológica.

No entanto, sob a ótica do princípio da compatibilidade, os preditores e critério comportamental devem ser definidos com o mesmo nível de generalidade e especificidade. A operacionalização do critério comportamental determina o quão especifico ou genérico deve ser a medida de atitude. Por exemplo, se o pesquisador estiver estudando a conservação de energia, o instrumento de medida de atitudes deve estar relacionado a um construto genérico de conservação de energia. Se, por outro lado, o critério comportamental é operacionalizado como sendo a reciclagem semanal de papel, então a medida deve ter atitudes ante a reciclagem semanal de papel. Cabe, portanto, ao pesquisador decidir o nível de generalidade ou especificidade em que vai operar (Fishbein & Azjen,1975).

Os autores diferenciam atitude implícita de explicita para melhor explicar a relação atitude-comportamento. Pode-se dizer que a primeira é automaticamente ativada, enquanto que a segunda requer um esforço cognitivo. Ambas são igualmente preditoras do comportamento real. As atitudes implícitas guiam o comportamento por padrão, a menos que sejam inibidas por processos controlados. Tal tipo de atitude mostrou-se melhor preditora de comportamentos não-verbais do que a explícita.

Para os autores, o problema da baixa correlação entre comportamento-atitude foi solucionado em parte quando se percebeu que, embora as atitudes genéricas sejam fracas preditoras de comportamentos, mostram-se fortemente correlacionadas com múltiplos critérios ou comportamentos agregados.

Outro estudo que visa à análise da relação atitude-comportamento foi realizado por Fishbein e Azjen (1975). Dentre os estudos analisados relacionados à atitude-comportamento, a maioria apresentou correspondência com apenas um de seus dois principais elementos (alvo e ação). Dez investigações utilizaram medidas que correspondiam somente a ação e 37 avaliaram os elementos alvo e falharam em analisar seus elementos de ação. A análise dos autores sobre a natureza das relações atitude-comportamento sugere que quando há correspondência parcial entre as entidades atitudinais e comportamentais, não é possível atingir consistentemente um forte relacionamento.

Os autores analisaram, também, medidas questionáveis de atitude-comportamento. Foi citado um exemplo de estudo cujos estudantes relataram sua atitude com relação ao tempo gasto nas atividades acadêmicas. No entanto, as escalas de atitudes não apresentavam o tempo realmente gasto em tais atividades. Já a medida de comportamento apresentava a quantidade de tempo realmente gasto, o que resultou em uma baixa correlação entre atitude-comportamento.

Os autores concluíram que quando os elementos alvo e ação de uma entidade atitudinal correspondem aos elementos alvo e ação de uma entidade comportamental, as correlações atitude-comportamento apresentam-se altas e significativas, mesmo quando a validade das medidas empregadas é duvidosa.

Os autores ressaltam, ainda, que as diferenças na magnitude das relações entre atitude e comportamento podem, então, ser atribuídas com confiança a diferentes graus de correspondência, como o caso da correspondência parcial e a falta de correspondência. Dos estudos que se enquadravam nesse caso, 29 medidas de atitude correspondiam no mínimo em parte ao critério comportamental – um em seu elemento alvo e outro em seu elemento ação. Das 58 correlações entre atitude e comportamento, nenhuma foi mais alta que 0,30 e cerca de 80% das correlações ficaram abaixo de 0,15. Além disso, alguns desses estudos apresentaram medidas cuja validade é questionável, apresentando um grau de correspondência variável e alguns de seus preditores eram muito mais crenças do que atitudes.

Em suma, Azben e Freisben (1975) enfatizam que a atitude de uma pessoa tem forte correlação com o seu comportamento quando ambos possuem o mesmo alvo e quando envolvem a mesma ação. Em geral, relações baixas e inconsistentes são observadas quando as entidades comportamentais e atitudinais falham na correspondência de um ou ambos os elementos. Ou seja, baixa correspondência produz relações atitude-comportamento não significativas.

Glasman e Albarracin (2006), por sua vez, verificaram a relação atitude-comportamento por meio de uma meta-análise, partindo da suposição de que a formação de atitudes prediz o comportamento futuro. De acordo com os autores, as atitudes são mais fortemente correlacionadas com o comportamento futuro quando são mais acessíveis e estáveis. Nesse

sentido, quando participantes tem experiência direta com o objeto relacionado à atitude e reportam suas atitudes frequentemente, a relação preditiva do construto tende a ser maior.

Para os autores, os seguintes processos estão envolvidos com a relação atitude-comportamento: acessibilidade da atitude quando são fáceis de serem recuperadas da memória; estabilidade da atitude e informação associada à atitude pode aumentar a correspondência entre atitude-comportamento.

Décadas de pesquisa têm mostrado a importância de entender como atitudes influenciam comportamentos. Dada à importância desse assunto, diversas meta-análises foram realizada mostrando os moderadores múltiplos da relação atitude-comportamento. No entanto, nenhuma dessas meta-análises tem apresentado o grau com o qual atitudes formadas predizem um comportamento futuro, nem identificam os fatores que moderam as correlações entre atitude-comportamento. E, principalmente, nenhuma delas tem focado em como os fatores influenciam o processo envolvido na predição do comportamento por meio das atitudes (Glassman & Albarracín, 2006).

No estudo de Glassman e Albarracín (2006), a correlação atitude-comportamento foi de 0,52, sendo mais alta do que a identificada em outros estudos que incluíam baixa correspondência entre atitude-comportamento no objeto, contexto e tempo. No entanto, é idêntica a estudos que mensuravam atitudes e comportamentos com alta correspondência. Para os autores, a maior contribuição da meta-análise foi a análise dos moderadores relacionados à acessibilidade e estabilidade da atitude.

Nesse sentido, o estudo mostrou que pessoas formam atitudes com maior poder preditor com relação a comportamento quando estão motivadas a pensar no objeto que está sendo considerado, quando tem uma experiência direta com o objeto, relatam suas atitudes frequentemente, constroem suas atitudes com base em informações relevantes para o comportamento, recebem ou geram informação positiva ou negativa sobre o objeto e acreditam que suas atitudes estão corretas.

A relevância comportamental da atitude ante a informação é considerada no estudo por meio da análise da congruência entre informação que direciona atitudes iniciais e informações

usadas posteriormente por uma decisão comportamental. Outro achado dos autores foi o fato de que seus resultados demonstram que atitudes são melhores preditoras de comportamento quando se baseiam em informação relevante para a decisão comportamental. Por exemplo, se o comportamento é instrumental, crenças são mais relevantes que o afeto; por outro lado, se o comportamento é público, atitudes expressas em público são mais relevantes que atitudes expressas em particular.

Buscando verificar a eficácia da teoria do comportamento planejado, Armitage e Conner (2001) realizaram uma revisão meta-analítica com 185 estudos. O TCP apresentou uma variância de 27% a 39%, respectivamente, nas variáveis comportamento e intenção. O construto controle comportamental percebido foi responsável por quantidade significativa da variância. Já as atitudes, normas subjetivas e controle comportamental percebido foi significativamente responsável mais pela variância nos desejos individuais do que nas intenções, no entanto intenções se mostraram melhores preditores de comportamento. Já o construto norma subjetiva apresentou-se como um fraco preditor de intenções, resultado atribuído parcialmente à combinação de medidas falhas e necessidade de expansão no componente normativo.

Os autores concluíram que, embora o modelo de TCP tenha maior valor preditivo sob auto-relato do que sobre o comportamento observado, este é capaz de explicar 20% da variância em medidas prospectivas de comportamento real. E acrescentaram, também, que trabalhar com variáveis normativas adicionais, como normas descritivas e morais, pode aumentar o poder preditivo do componente normativo do modelo.

Como o objeto principal desse estudo está relacionado com comportamentos dos indivíduos voltados para a segurança da informação, será apresentado algumas conceituações relacionadas ao construto com enfoque na segurança.

1.6 Comportamento em segurança da informação

Para Vroom e Solms (2004), quando a organização passa a se preocupar com a segurança da informação e adota práticas e procedimentos, o comportamento do funcionário se adapta à nova situação. Tal conscientização é o resultado de uma mudança cultural que

ocorre no nível do indivíduo, do grupo e da organização. Os autores enfatizam que como cada pessoa é única e traz consigo características diferentes para a empresa, ao se estudar o comportamento em segurança da informação é importante entender como as características individuais influenciam e são influenciadas pelo ambiente de trabalho. Os valores e normas dos grupos precisam, igualmente, ser analisados, pois influenciam a forma como indivíduos agem e se comportam nas tarefas do trabalho.

Consoante os autores, para que a organização incorpore comportamentos de segurança da informação na rotina de seus funcionários é preciso que haja uma mudança cultural nos níveis do indivíduo, do grupo e da organização. Nessa linha de raciocínio, o comportamento influencia a mudança cultural na medida em que provoca alterações no comportamento do indivíduo, do grupo, e posteriormente na organização. Pode-se dizer, portanto, que comportamento de segurança da informação é aquele que está em conformidade com as diretrizes, normas e procedimentos de segurança; já a cultura de segurança é alcançada quando tais comportamentos são adotados pelo grupo de forma natural, como parte de sua rotina.

Consoante Leach (2003), os seguintes fatores podem afetar o comportamento dos indivíduos quanto à segurança da informação: informação sobre o assunto (conscientização); relação custo-benefício de proteger ou revelar a informação; ideologia e falta de motivação. Para o autor, a visão do indivíduo sobre SI é criada por diversos fatores individuais, tecnológicos e organizacionais. Já os fatores organizacionais se referem às normas sociais e interações no trabalho, políticas e qualidade da gestão de SI, que influenciam a compreensão acerca do tema, bem como, a conscientização e comportamento do indivíduo.

As soluções de tecnologia da informação voltadas para segurança, por sua vez, influenciam o comportamento na medida em que restringem o que é possível realizar nos sistemas de informação, por meio de mecanismos de segurança para controlar as ações dos usuários. Os fatores individuais, tais como motivação, conhecimento, atitudes e valores influenciam as visões individuais de SI e sua percepção de risco, influenciando, igualmente, no comportamento por eles apresentado. Para Leach (2003), diversas medidas podem ser adotadas para influenciar o comportamento e conscientização dos indivíduos nas organizações

em relação à segurança da informação, tais como: campanhas, programas educacionais, recompensas, medidas de proteção físicas e tecnológicas e legislação.

Leach (2003) ressalta que comportamentos adversos à segurança nas organizações podem representar uma ameaça interna a ela devido, dentre outros, aos erros e falhas dos indivíduos, à falta de atenção, à negligência e aos ataques. Para gerenciar tal ameaça, é necessário entender como a cultura e as práticas organizacionais afetam o comportamento dos funcionários.

O autor apresenta os fatores influenciadores em um modelo dividido em duas áreas. Na primeira, são apresentadas variáveis relacionadas à compreensão do indivíduo quanto ao comportamento de segurança que é esperado pela organização, tais como: valores, políticas, padrões, procedimentos, comportamento demonstrado pelos gerentes e colegas de trabalho, senso comum de segurança da informação e habilidades para tomada de decisão. A combinação desses fatores gera a compreensão do usuário de aceitação e aprovação comportamental de normas no trabalho.

A segunda área, por sua vez, se refere à disposição em mudar o comportamento com o intuito de se adequar as normas aceitáveis e os fatores relacionados são: valores pessoais e padrões de conduta, contrato psicológico com o empregador, esforço requerido para estar em conformidade e para não estar.

No entanto, a organização não pode gerenciar todos os fatores que afetam o comportamento dos indivíduos como, por exemplo, valores pessoais ou padrões de conduta. Por isso, esta deve focar primeiramente nos fatores que estão, de fato, sob seu controle. Para tanto, a organização deve fazer um esforço continuo para assegurar que seus controles sejam eficientes, efetivos e propriamente implementados (Leach, 2003).

Para o autor, existem três fatores chaves para melhorar o comportamento de segurança dos usuários. O primeiro é o comportamento demonstrado pelo gerente e colegas, afinal os indivíduos tendem a ser guiados mais pelo que eles veem do que pelo que é dito a eles. Formas de melhorar o comportamento da equipe consistem em fornecer gratificação pelo bom comportamento em segurança e oferecimento de treinamentos, demonstrando quais são os

comportamentos inaceitáveis. Outro fator chave é o senso comum de segurança do indivíduo e habilidades para tomada de decisão (o senso comum é algo que pode ser ensinado por meio de princípios que guiam a tomada de decisão.) e, por fim, a força do contrato psicológico com a instituição.

Para Leach (2003), a criação de uma cultura de segurança é a melhor forma de motivar a equipe a se comportar de uma forma consciente em relação a Segurança da Informação. A importância da alta direção na criação dessa cultura é fundamental, afinal uma liderança forte cria uma cultura forte e uma cultura forte fornece uma direção clara para a equipe em todos os níveis. O autor ressalta, ainda, que um comportamento de segurança fraco é um fator determinante de incidentes na empresa. Por isso, a organização deve criar uma cultura de segurança e fortalecer a sua influência no comportamento dos indivíduos.

Stanton et al.(2005) criaram uma taxonomia composta por dois fatores e seis categorias a fim de organizar comportamentos em segurança da informação. Para os autores, uma liderança que apoie a segurança, sistema de recompensas, intervenções motivacionais e designação clara do papel e responsabilidades dos indivíduos em relação à segurança são fatores relacionados com os comportamentos classificados como benéficos. Nesse sentido, a análise do comportamento dos indivíduos em segurança pode ajudar a assegurar que trabalhadores tenham motivação e conhecimento para seguir as políticas que a organização promove em sua agenda de segurança.

Furnell e Thomson (2009), por sua vez, apresentam níveis de aceitação de segurança da informação por meio de uma escala de compromisso dos indivíduos com a segurança. Tais categorias foram extraídas dos comportamentos observados no ambiente de trabalho. Na figura 3, pode-se observar que existe uma clara barreira entre o comportamento de conformidade e não conformidade com a segurança. O autor afirma que se o funcionário encontra-se no nível “cultura”, ele estará alinhado com as práticas corretas de segurança. Por outro lado, se o indivíduo estiver no nível de “desobediência”, ele não estará alinhado com os valores de segurança da organização. O autor acrescenta, que no nível “ignorância”, o indivíduo não tem a intenção de trabalhar contra a segurança, no entanto, falta-lhe base para saber o que é preciso ser feito.

Já no nível de conscientização, o indivíduo é consciente das práticas corretas, mas estas ainda não refletem completamente nos conhecimentos e comportamento deste. Isto demonstra que apenas dizer o que a pessoa tem que fazer não é o suficiente para que se alcance um nível satisfatório de conformidade com a segurança da informação. O autor ressalta, ainda, que o grau de conformidade com a SI raramente é homogêneo entre os funcionários de uma mesma organização.

Conformidade	**Cultura**	Estado ideal no qual a segurança faz parte do comportamento natural do usuário.
	Comprometimento	A segurança não é parte do comportamento natural do usuário, mas se conduzida de forma correta por uma liderança pode levar os usuários a aceitarem sua necessidade.
	Obediência	Usuários podem não estar de acordo com os princípios de segurança, mas podem aderir a eles via uma autoridade apropriada.
	Conscientização	Usuários estão conscientes de seu papel na segurança, mas não necessariamente aderem às práticas e regras.
Não Conformidade	**Ignorância**	Usuários não estão conscientes da segurança e podem gerar incidentes.
	Apatia	Usuários estão conscientes de seu papel em proteger os ativos, mas não estão motivados a aderir as práticas de segurança.
	Resistência	Usuários trabalham passivamente contra a segurança, se opondo a práticas com as quais não concordam.
	Desobediência	Usuários trabalham ativamente contra a segurança, quebrando intencionalmente regras e burlando controles.

Figura 3. Categorias de comportamentos de segurança da informação.

No presente estudo, a variável mudança organizacional foi incluída no modelo empírico como uma das preditoras da relação atitude-comportamento. O próximo tópico aborda este construto.

2 Mudança Organizacional

Mudanças são cada vez mais frequentes nas organizações. Para Wood Jr. (1992), a maior parte da literatura sobre mudança organizacional é iniciada por comentários sobre a velocidade fantástica das mudanças sociais, econômicas, políticas e tecnológicas do fim deste século e da importância das organizações em se adaptarem às mudanças.

Dentre as mudanças observadas, destaca-se a substituição da sociedade industrial pela sociedade de informações, cujo capital humano é o recurso mais importante. Ademais, a tecnologia da informação que agora possui um papel estratégico para as empresas, está fazendo desaparecer a burocracia, os controles e os níveis intermediários das organizações (Wood Jr,1992). A tecnologia e as inovações dela decorrentes, o comportamento social, instituições e estruturas são os principais elementos da mudança organizacional.

A mudança resulta em alterações fundamentais no comportamento humano, sendo, por isso, fundamental o gerenciamento das pessoas envolvidas durante todo o processo. Nesse sentido, o grande desafio não é a mudança tecnológica, mas a mudança do comportamento e da cultura organizacional (Wood Jr,1992).

Diversos são os conceitos de mudança organizacional na literatura. Consoante Wood Jr.(1992), mudança organizacional é qualquer alteração significativa, articulada, planejada e operacionalizada por pessoal interno ou externo à organização, que tenha o apoio e supervisão da administração superior e atinja os componentes comportamentais, tecnológicos e estratégicos.

Neiva (2004), por sua vez, advoga que mudança organizacional é qualquer alteração, planejada ou não, em componentes que caracterizam a organização como um todo decorrente de fatores internos ou externos à organização, que traz alguma consequência, positiva ou negativa, para os resultados organizacionais ou para sua sobrevivência. Lima e Bressan (2003) acrescentam que a modificação ocasionada pela mudança deve ser significativa, atingir a

maioria dos membros da organização e ter como objetivo a melhoria do desempenho organizacional em resposta às demandas internas e externas.

Para Lima e Bressan (2003), embora não exista um eixo que norteie as diversas definições de mudança organizacional, existe uma convergência nas seguintes dimensões: intencionalidade; transformação/ congruência sistêmica entre componentes; relevância do impacto da mudança; temporalidade; construção social da mudança; e resposta à demanda interna.

Para melhor compreender a mudança organizacional, é importante conhecer a sua classificação quanto à tipologia.

2.1 Tipologias de mudança organizacional

Lima e Bressan (2003), organizaram as diversas tipologias de mudança organizacional existentes na literatura (Figura 4), que apresentam duas formas principais de mudança: alteração de poucos aspectos da organização, faz mínimos ajustes continuamente e acontece em situações em que o ambiente é mais estável e mudança que rompe com os padrões anteriores, atinge toda a organização e redireciona a organização em função de alterações no seu ambiente.

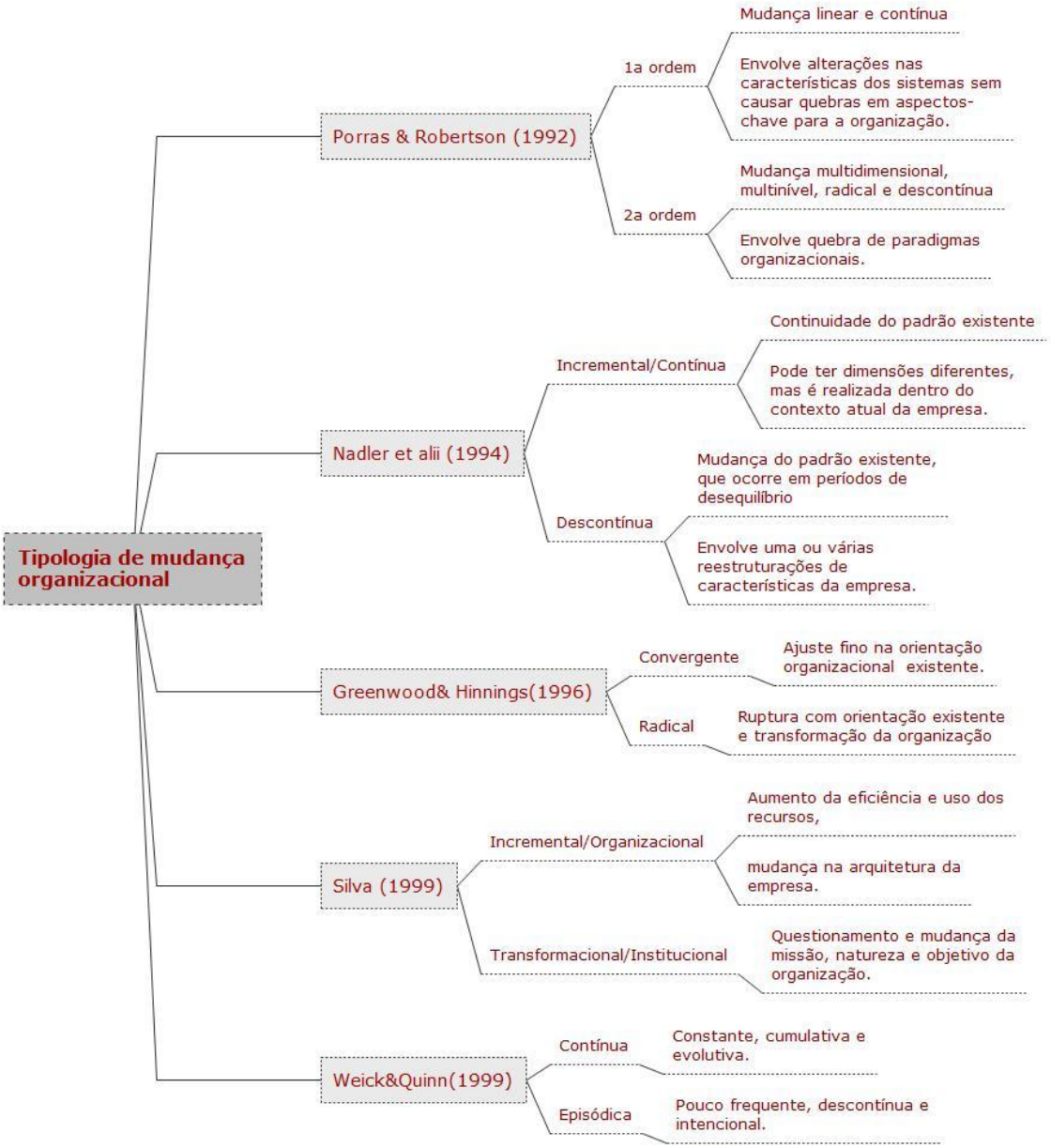


Figura 4. Tipologia de Mudança Organizacional (Lima & Bressan 2003)

Para Greenwood e Hinings (1996) a mudança pode ser classificada em radical e convergente. Dessa forma, a primeira representa uma ruptura no paradigma organizacional existente, o abandono da orientação até então vigente. Já a segunda é aquela que realiza ajustes nos padrões existentes. As mudanças incrementais/contínuas ou descontínuas foram classificadas por Nadler, Shaw e Walton (1994). Segundo os autores, as mudanças incrementais ocorrem em períodos de equilíbrio e as contínuas em função das exigências externas.

Weick e Quinn (1999), por sua vez, classificaram as mudanças em episódicas e contínuas. Para eles, as mudanças episódicas são pouco frequentes, descontínuas e intencionais. Em geral, ocorrem em organizações estáveis e que funcionam com padrões automatizados em que prepondera a inércia. Além disso, representam uma interrupção ocasional do equilíbrio e. constituem uma falha da organização em adaptar-se a um ambiente de mudança. A mudança contínua, por outro lado, ocorre em organizações que são emergentes e auto-organizáveis. Tem como característica a constância e são cumulativas. Representam um padrão de alteração contínua em processos de trabalho e práticas sociais.

Cabe ressaltar, que a classificação das mudanças em incrementais e descontínuas não impedem que essas ocorram ao mesmo tempo. Mudanças de naturezas distintas podem coexistir na mesma organização (Neiva, 2004; Lima & Bressan, 2003).

Para Vieira (2009), os diversos tipos de mudança organizacional, conceitos e definições sobre o assunto corroboram a complexidade do tema e implicam a compreensão dos processos de mudança nas organizações. Além disso, a tipologia de mudança auxilia a identificar quais conteúdos de mudança ocorreram no período, uma vez que o tipo de mudança indica o conteúdo que mudou.

2.2. Mudança organizacional sob a ótica do indivíduo

Os indivíduos constituem o elemento propulsor da mudança, podendo colaborar com o seu sucesso ou apresentar resistência a ela. Por isso, faz-se necessário analisar o processo de mudança não apenas no nível organizacional como, também, no nível do indivíduo (George & Jones, 2001).

Para Hannah e Freeman (1984), a inabilidade para mudar ou a inércia representam as primeiras forças opositoras, no nível organizacional, tanto quanto rotinas institucionalizadas, práticas, crenças e valores enquadrados na estrutura organizacional e cultura. Nessa perspectiva, o papel do indivíduo pode ficar minimizado a uma resposta às pressões ambientais. Somente a ação da inércia e da inabilidade para mudar torna a organização inábil para adaptar-se a um ambiente em mudança.

Dessa forma, compreender da inércia é fundamental para o estudo da mudança nas organizações. A compreensão de como a resistência à mudança e a inércia podem começar nos níveis individual e coletivo de análise e sedimentam-se no nível organizacional é crucial para os estudos da área (Weick & Quinn,1999).

George e Jones (2001) propõem um modelo de mudança e resistência nas organizações. De acordo com o modelo, a maneira com que os indivíduos constroem significados e atribuem sentido ao mundo social e organizacional, reproduz a dinâmica entre a cognição humana e os afetos no início do processo de mudança individual, bem como na determinação de sua natureza e consequências. Assim, as inconsistências e discrepâncias com esquemas cognitivos concorrentes ativam uma reação emocional que direciona o processo de mudança nos esquemas existentes.

Nessa perspectiva, os esquemas cognitivos dos indivíduos são mediadores das atitudes frente às mudanças genéricas e das atitudes frente às mudanças específicas. As atitudes funcionam, portanto, como preditores de comportamentos posteriores de participação no processo de mudança (Lau & Woodman ,1995 citado por Neiva, 2004).

Estudos e teorias da área apontam que o conflito cognitivo pode gerar alteração de valores, crenças e atitudes; sendo o conflito um antecedente da mudança comportamental. Dessa forma, os indivíduos necessitam manter uma congruência entre suas crenças e seus comportamentos para obter mudanças cognitivas e comportamentais (Neiva, 2004).

Teorias de mudança organizacional buscam analisar a interação entre as variáveis mudança organizacional e mudança comportamental. O modelo de Porras e Robertson (1994) aponta que a mudança individual é pré-requisito para a mudança organizacional.

Por outro lado, Neiva (2004) dispõe que sentir ou pensar diferentemente não é suficiente para que ocorra mudança organizacional haja vista que todas as mudanças organizacionais efetivas necessitam ter como resultado concreto uma mudança comportamental, ou seja, um comportamento desejado. Nesse contexto, alterações em condições ou características organizacionais não terão muito impacto nos resultados gerados pela organização se não envolverem alterações nos comportamentos individuais.

As intervenções realizadas nas organizações podem desencadear mudanças comportamentais. Ademais, a efetividade de tais intervenções depende da característica do comportamento a ser mudado, das pessoas, da intervenção e das condições que manterão o novo comportamento. Uma intervenção efetiva deve ter como primeira consequência a alteração do comportamento no trabalho e deve estar alinhada com as mudanças comportamentais desejadas.

Para Porras e Robertson (1992), os comportamentos individuais constituem o elo mediador entre a intervenção planejada e os resultados organizacionais. Dessa forma, os comportamentos requeridos por um tipo de mudança em uma organização específica não são generalizáveis.

Em suma, os achados na literatura demonstram a necessidade de se vincular intervenções a mudanças comportamentais desejadas. Além disso, as atitudes frente à mudança também apresentam um importante elo entre indivíduos e mudança organizacional, podendo constituir facilitadores dos processos de mudança organizacional. As atitudes dos gerentes frente à mudança, por exemplo, determinam a participação dos empregados e o sucesso da implantação do programa de mudanças, mostrando que o processo cognitivo dos indivíduos é determinante para que as intervenções logrem sucesso (Neiva, 2004).

Consoante Neiva (2004), a cognição possui grande papel no processo de mudança nas organizações. Por meio da análise de relações, o indivíduo percebe o evento da mudança quando comparadas duas situações. Dessa forma, seus componentes cognitivos e afetivos influenciarão no grau em que essa percepção existe, além de influenciar na possibilidade de manifestação de comportamentos necessários ao processo de mudança. Para a autora, a percepção de mudança organizacional é uma das formas de se avaliar a ocorrência da mudança nas organizações. No próximo tópico será abordado este construto.

2.3 Percepção de mudança organizacional

Durante o processo de mudança, é essencial preocupar-se com os sentimentos dos indivíduos, percebendo os significados que eles atribuem às mudanças e as possibilidades para que estes passem a ser sujeitos no processo. No entanto, para Silva e Vergara (2002),

pouca atenção tem sido dedicada aos indivíduos no processo de mudança. Ademais, os autores advogam que a mudança não pode ser entendida somente sob o ponto de vista de estratégias, processos ou tecnologias, afinal, o aspecto humano é fundamental para que as mudanças sejam bem sucedidas na organização.

Consoante Silva e Vergara (2002), para a compreensão sobre o comportamento dos indivíduos no âmbito da mudança organizacional é fundamental que se observe o processo por meio do qual eles interpretam e constroem significado para eventos nos quais estão envolvidos. Silva e Vergara (2002) ressaltam, ainda, que quando os indivíduos assumem um papel de sujeito no processo de mudança e não de vítima, é possível criar um processo em que haja pleno engajamento de todas as pessoas da organização.

Para Neiva (2004), o processo de percepção individual da mudança é composto por sete estágios, incluindo desde a exposição aos estímulos do ambiente até a adoção de um comportamento que, por sua vez, pode ser dividido em: adoção de um comportamento resistente, decisão para superar a resistência, indecisão ou adoção espontânea da mudança.

O indivíduo é, pois, peça fundamental no processo de mudança organizacional. Sendo assim, faz-se necessário investigar sua percepção de mudança para compreender suas atitudes, crenças e comportamentos com relação às intervenções realizadas na organização.

Com relação à segurança da informação, as práticas e procedimentos de segurança da informação quando adotadas representam intervenções que podem gerar mudanças organizacionais. Por isso, estudos já têm sido realizados a fim de verificar a relação entre as variáveis mudança organizacional e segurança da informação.

Vieira (2009) realizou uma pesquisa qualitativa na Petrobrás sobre o processo de mudança que a organização passou em decorrência da adoção de práticas e procedimentos em segurança da informação, bem como, sobre a consolidação de uma cultura de segurança.

Como base na análise do processo, a autora utilizou o modelo de Kotter (1995). As intervenções analisadas ocorreram em um período de cinco anos e abordavam aspectos comportamentais, tecnológicos, normativos e de gestão. Dentre as intervenções, destacam-se os diversos cursos e workshops oferecidos aos funcionários, implantação de uma política de

segurança e classificação da informação, normas e diretrizes de uso de correio eletrônico, serviço de internet, dentre outros.

O início do processo de mudança ocorreu devido a sucessivos vazamentos de informações sigilosas da organização para a mídia. Sua formalização foi feita por meio de uma carta do presidente, que mencionava a sua preocupação com relação ao incidente e a importância em se preservar o sigilo das práticas comerciais da Petrobrás (Vieira, 2009).

Com relação à classificação da mudança, a autora caracterizou-a como sendo programada, cultural e de natureza predominantemente humana/social. Além disso, o objetivo do processo foi alcançar uma transformação total, profunda e radical na organização. Pode-se, também, classificá-la como transformacional, de 2ª ordem, episódica, descontínua e radical.

Foram criadas a Gerência de Inteligência e Segurança da Informação e o Comitê de Segurança da Informação do Sistema Petrobrás (COMSEG), que ficaram à frente do processo de mudança. A autora destacou a importância da participação da alta direção durante o processo.

Em uma carta, o presidente da Petrobrás enfatizou a importância dos funcionários para o sucesso da mudança:“ Este é o primeiro passo de uma importante jornada, na qual você desempenha um papel fundamental. Depende de você a garantia do cumprimento das políticas e das normas de segurança da informação por parte de sua equipe.” O presidente ainda ressalta que “ como a segurança da informação depende, sobretudo, da atitude de cada pessoa, também devemos cuidar da vertente comportamental.”

Consoante Vieira (2009), o processo de comunicação da mudança foi feito por meio de campanhas anuais. Durante os cinco anos analisados, este processo passou por diversas ondas, a saber: uso de correio eletrônico, mesa e tela limpa, engenharia social, uso seguro de recursos, tratamento de informação, comunicação de incidentes, classificação das informações e comunicação de incidentes. Ademais, foram distribuídos cartazes com dicas de comportamentos seguros, uso de mídias e programas na TV corporativa abordando as boas práticas de segurança da informação.

O processo de mudança organizacional ocorrido na Petrobrás visava uma mudança cultural. No entanto, no próprio planejamento, este objetivo não foi amplamente declarado e no processo de comunicação da mudança não foi explícito o porquê da mudança (Vieira, 2009).

Ao final de cinco anos, houve uma valorização das práticas de segurança da informação pelos funcionários. Todavia, a autora afirma que devido ao tamanho e dispersão geográfica da Petrobrás, ainda é difícil afirmar que o programa faz parte da cultura da organização. Foram percebidas falhas na consolidação de uma cultura de segurança da informação, tais como: o senso de urgência que não foi explicitado com clareza, um Comitê de Segurança da Informação pouco atuante e a declaração de uma visão de longo prazo que não ficou explicita para a força de trabalho. A autora ressalta, ainda, que outro ponto fundamental para a não consolidação da cultura foi a falta de um trabalho proativo para identificar os grupos e indivíduos resistentes à mudança.

Os tópicos abordados na revisão de literatura apresentaram as principais variáveis que constituem o modelo empírico desse estudo, quais sejam: práticas organizacionais de segurança da informação, percepção de mudança organizacional atribuída às práticas, atitudes em face às práticas e comportamentos de segurança da informação. No próximo tópico, será apresentada a descrição do método utilizado.

3 Modelo de Pesquisa

Com o intuito de testar a relação entre as variáveis Práticas de Segurança da Informação e Percepção de Mudança atribuída a Segurança da Informação e seu impacto no nível individual (Atitudes frente às Práticas de Segurança e Comportamentos de Segurança), foi elaborado um modelo preliminar de investigação (Figura 5).

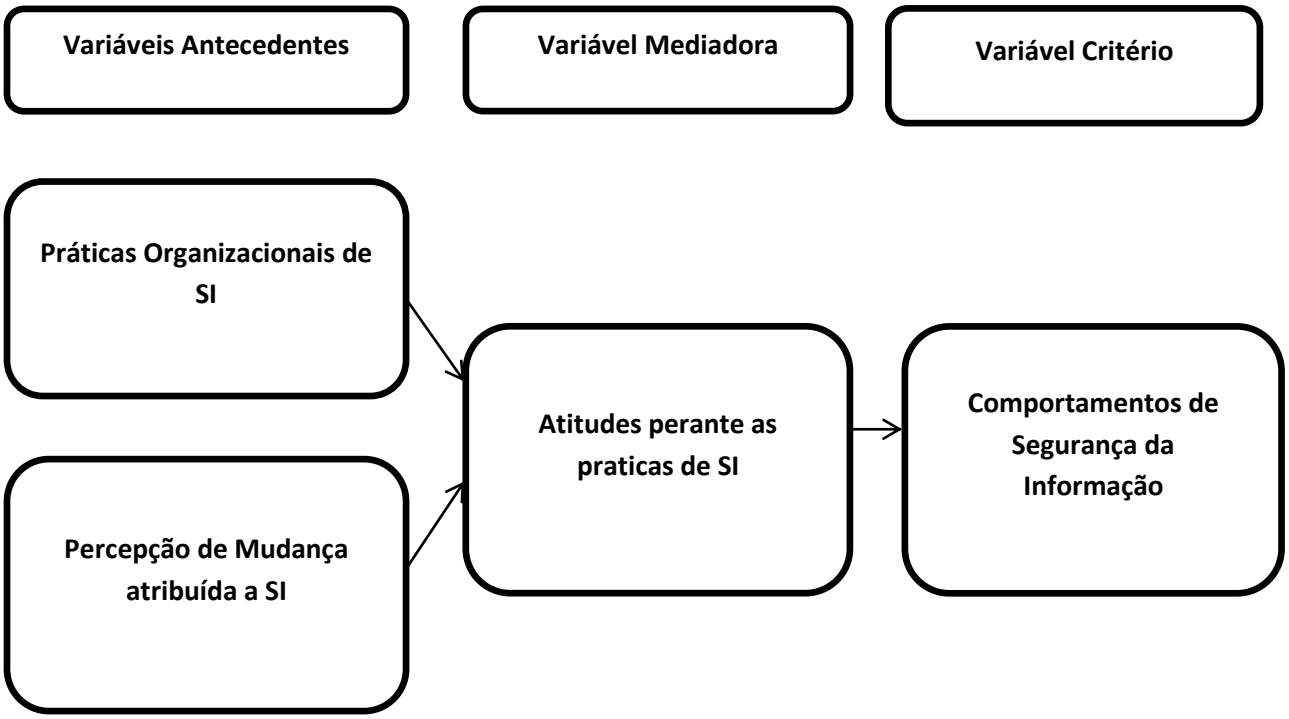


Figura 5. Modelo de Investigação

As variáveis são definidas a seguir:

a) **Práticas organizacionais de segurança da informação** se referem à percepção dos indivíduos quanto às intervenções realizadas pela organização que os estimulem a adotarem novos comportamentos e atitudes de segurança da informação.

b) **Percepção de mudanças atribuída à segurança da informação** avalia em que medida os indivíduos percebem que existiram mudanças na sua organização a partir da adoção de práticas de segurança da informação.

c) **Atitude perante as práticas de SI** se referem às respostas cognitivas, afetivas e intenções comportamentais, ou maneira como o indivíduo responde, favoravelmente ou não, às práticas segurança da informação.

d) **Comportamento de segurança da informação** se refere às ações de segurança que os indivíduos percebem adotar em seu ambiente de trabalho.

3.1 Hipóteses

Para responder a pergunta proposta, as seguintes hipóteses serão testadas:

H1 – Os indivíduos percebem a mudança organizacional como resultado da adoção de práticas de segurança da informação.
H2 – As atitudes dos indivíduos agem como variável mediadora da relação entre Práticas Organizacionais de Segurança da Informação e Comportamento de Segurança da Informação.
H3 – As atitudes dos indivíduos agem como variável mediadora da relação entre Percepção de Mudança atribuída às práticas de segurança da informação e Comportamento de Segurança da Informação.

As Práticas Organizacionais de Segurança da Informação quando implantadas na organização representam intervenções. Tais intervenções geram mudanças organizacionais, conforme achados de Vieira (2009), sustentando, portanto, a hipótese 1 desta pesquisa.

As hipótese 2 e 3 fundamentam-se em parte no que dispõe Neiva (2004) acerca da relação entre aspectos cognitivos e mudança organizacional. Nesse sentido, a cognição humana tem sido associada sempre a formulações sobre mudança organizacional. Dessa forma, o processo cognitivo é fundamental para inferência de mudança organizacional, ao mesmo tempo em que também se configura um dos impedimentos para que o indivíduo se vincule ao processo de mudança, o reconheça como tal e apresente novos comportamentos adequados às mudanças propostas. Por isso, essa cognição tem sido apontada como o vínculo entre aspectos organizacionais e aspectos individuais.

Os estudos de Azjen (1991) e Fishbein e Azjen (1975) sobre a relação atitude-comportamento, no qual atitude é variável preditora de comportamento serviram, também,

como base teórica para a formulação das hipóteses 2 e 3. Por fim, os achados de Thomson e Solms (1998) que realizaram um estudo a fim de explicar a forma como diferentes aspectos, tais como atitudes, determinam o comportamento de um indivíduo e como estes podem ser utilizados no processo de conscientização e treinamento de usuários em segurança, complementaram o embasamento teórico das hipóteses 2 e 3.

A seguir, será apresentado o método utilizado neste trabalho.

4 MÉTODO

Neste Capítulo é apresentado o delineamento metodológico da pesquisa. Para tanto, serão apresentados: a amostra; a caracterização da organização; o procedimento de construção dos instrumentos; de coleta e de análise dos dados.

4.1 Descrição da Organização

Empresa pública de grande porte da área de tecnologia da informação, composta por unidades regionais distribuídas em todo o território nacional. A empresa possui uma universidade corporativa que apoiou e auxiliou na realização da pesquisa. Cabe ressaltar que o critério para a escolha da empresa foi que essa adotasse práticas de segurança da informação em suas rotinas. Dentre as práticas de segurança da informação adotadas pela empresa, destacam-se as relacionadas ao controle de acesso (utilização de catracas, identificação biométrica, entrega de crachás para os visitantes, e etc.); relacionadas aos sistemas, como treinamento de usuários sobre a utilização segura dos sistemas, controle de contas, senhas, identificação e autenticação dos usuários, política da mesa e tela limpa, manipulação de documentos físicos e digitais.

Além disso, são adotadas práticas relacionadas ao ambiente de trabalho como, por exemplo, bloquear a máquina ao se ausentar da estação de trabalho e evitar comidas e bebidas perto dos computadores. Os funcionários são, também, orientados quanto à utilização adequada do correio eletrônico, restringindo-se a sua utilização para fins de trabalho.

A Empresa possui uma política de segurança da informação consolidada que começou a ser implantada em 1999, atendendo aos objetivos da pesquisa e já realizou programas de treinamento e conscientização envolvendo todos os seus funcionários. No entanto, devido a mudanças na diretoria, os programas de treinamento e conscientização não foram mais realizados. A consequência é que os funcionários mais recentes não foram adequadamente preparados para adotar as práticas e procedimentos de segurança da informação, embora tenham que assinar termo de ciência da política de segurança da informação no ato da contratação.

4.2 Amostra

A amostra foi aleatória, sendo que 650 funcionários de todas as regiões do Brasil responderam ao questionário. Este foi aplicado uma única vez entre agosto e setembro de 2011, cerca de 10 anos depois das primeiras intervenções na organização.

Sua aplicação se deu via link que ficou disponível para todos os funcionários durante 15 dias na intranet da empresa, dez anos após a realização das primeiras intervenções de segurança da informação. Não houve critério de escolha de sujeitos, já que a avaliação das atitudes e comportamentos de segurança independe da função exercida, idade, sexo ou outros fatores.

Os dados demográficos da amostra final (foram 423 sujeitos devido à limpeza do banco de dados para as análises) estão dispostos na Tabela 1. Por meio da análise dos dados, observa-se que grande parte dos respondentes é do sexo masculino (67,7%) e possui entre 46 e 55 anos. Quanto à escolaridade, a pesquisa mostrou que a maioria dos empregados possui nível superior (40,89%) ou, também, especialização (40,42%). Com relação à função exercida, grande parte das respostas vem de empregados que pertencem à área fim da empresa (58,86%). Ademais, houve um equilíbrio na percentagem de respondentes da região Sudeste (37, 89%) e Centro-Oeste (27,9%). Já com relação ao tempo de serviço, a maioria dos empregados participantes possuía entre 21 a 30 anos de empresa (27,42%), seguido de 31 ou mais (21,53%). No entanto, houve, também, um número expressivo de empregados com tempo de serviço variando entre 1 a 5 anos (20,80%), um indicador que pode influenciar nas atitudes e comportamentos frente a Segurança da Informação.

É importante ressaltar que a maior parte dos respondentes possuíam atribuições típicas relacionadas à Tecnologia da Informação, o que pode ter influenciado na adoção de práticas de Segurança da Informação.

Tabela 1. Caracterização da amostra quanto à escolaridade, função, sexo, região e tempo de serviço

Variável		Frequência	%
Escolaridade	Fundamental	1	0,29%
	Médio	41	9,26%
	Superior	171	40,89%
	Especialização	173	40,42%
	Mestrado	35	8,67%
	Doutorado	2	0,47%
	TOTAL	423	100,00%
Tipo de função	Diretoria	2	0,47%
	Assessoramento	26	6,14%
	Área de negócio	32	7,56%
	Área de desenvolvimento de sistemas	116	27,42%
	Área de infra-estrutura tecnológica	133	31,44%
	Área de gestão	114	26,97%
	TOTAL	423	100,00%
Idade	18 a 25 anos	8	1,89%
	26 a 35 anos	109	25,75%
	36 a 45 anos	84	19,89%
	46 a 55 anos	167	39,47%
	56 anos ou mais	55	13%
	TOTAL	423	100,00%
Região	Centro-Oeste	118	27,89%
	Norte	20	4,72%
	Nordeste	65	15,36%
	Sul	60	14,21%
	Sudeste	160	37,82%
	TOTAL	423	100,00%
Tempo de empresa	Menos de 1 (um) ano	36	8,51%
	1(um) a 5(cinco) anos	88	20,80%
	6(seis) a 10(dez) anos	68	16,07%
	11(onze) 20 (vinte) anos	24	5,67%
	21 (vinte e um) a 30 (trinta) anos	116	27,42%
	31(trinta e um) ou mais	91	21,53%
	TOTAL	423	100,00%

4.3 Coleta de Dados

Os dados coletados na organização foram transpostos para o software *Statistical Package for Social Sciences* (SPSS), versão 17.0, compondo um único arquivo de dados. A análise exploratória de dados resultou em três arquivos: o primeiro deles com 441 casos (excluídos casos omissos); o segundo com 438 (excluídos os casos extremos univariados) e o terceiro com 423 (excluídos extremos uni e multivariados). Para análise dos extremos

univariados, utilizou-se os escores padronizados das variáveis (score Z) e análise do desvio-padrão, adotando o critério de Hair et al. (2009), ou seja, se os casos estão entre 2,5 e 4,0. Já para análise dos extremos multivariados, optou-se pela distância de mahalanobis com o método enter.

Os pressupostos estatísticos de normalidade, linearidade e homoscedasticidade, necessários para análise de regressão múltipla foram testados.

4.4 Medidas

Para essa pesquisa foram utilizados 4 instrumentos: 1 já validado e 3 desenvolvidos pela própria autora. Em todos os instrumentos foram seguidos os seguintes passos no processo de construção/validação:

a) Revisão de literatura;
b) Operacionalização das definições e construção dos itens do instrumento;
c) Validação por juízes, semântica e empírica.

A seguir, será apresentada a caracterização dos instrumentos e processo de construção/validação.

4.5 Práticas Organizacionais de Segurança da Informação

Esse instrumento é composto por 18 itens associado a uma escala do tipo Likert de 10 pontos (1 = discordo plenamente;10= concordo plenamente).Para a construção dos itens utilizou-se como arcabouço teórico a norma ISO/IEC 27002 – Boas práticas em Segurança da Informação.

Os itens construídos abrangem todos os sete grupos de práticas da norma, a saber: documento da política de segurança da Informação; atribuição de responsabilidades para a segurança da informação; conscientização, educação e treinamento em segurança da informação; processamento correto nas aplicações; gestão de vulnerabilidades técnicas; gestão de continuidade do negócio e gestão de incidentes de segurança da informação e melhorias. Estes grupos de práticas foram descritos no referencial teórico.

Quanto à validação, o instrumento foi submetido para cerca de 5 juízes especialistas em Gestão de Pessoas e Administração. Os itens foram lidos em grupo e os juízes faziam comentários quanto à redação dos mesmos. Ao final, alguns itens foram retirados ou ajustados com índice de concordância mínimo entre juízes de 80%.

Com relação à validação semântica, a equipe responsável pela área de pesquisas acadêmicas da Empresa leu o questionário por várias vezes e solicitou ajustes na redação dos itens, buscando adequá-los à realidade da empresa. Posteriormente, o instrumento foi aplicado a um pequeno grupo de funcionários de uma das regionais, resultando em mais alguns ajustes nos itens.

4.6 Percepção de Mudança Organizacional atribuída a Segurança da Informação

Esse instrumento, elaborado por Domingos (2009) e revalidado por Pichi (2010), é composto por 33 itens e escala de concordância do tipo likert que varia de 0 a 10 pontos. No estudo de Domingos (2009), o instrumento apresentou estrutura bifatorial com as dimensões de Mudança Organizacional Transacional e Transformacional. No estudo de Pichi (2010), a autora relata que foi necessário acrescentar itens à escala de Mudança Transacional para melhorar seu índice de confiabilidade. Apresentaram estrutura bitaforial : mudança radical com 17 itens e alfa de *Cronbach* de 0,957 e mudança incremental, com 16 itens e alfa de 0,87 . Além disso, utilizou uma escala de concordância do tipo Likert de 10 pontos.

Na presente pesquisa, o instrumento passou por validação semântica, por juízes e revalidação, para comprovar a estrutura bifatorial encontrada nos estudos anteriores. Foi necessária uma adaptação quanto ao enunciado das escalas, no entanto, o conteúdo dos itens não sofreu alterações.

4.7 Atitudes frente às práticas de Segurança da Informação

Os 16 itens do instrumento foram desenvolvidos com base em estudos sobre atitudes (Azjen, 1991; Fishbein & Azjen, 1975; Thomson & Solms,1998) e visam mensurar as atitudes dos indivíduos quanto as práticas de segurança da informação. Ademais, sua escala é do tipo Likert 10 pontos.

Para sua validação foi realizada validação semântica e por juízes da mesma forma como no instrumento de práticas, sendo que alguns de seus itens foram excluídos ou alterados. O conteúdo dos itens descreve, principalmente, as crenças positivas ou negativas dos indivíduos acerca da segurança da informação, como por exemplo: As práticas de segurança da informação requerem muito do meu esforço mental; são fáceis de ser utilizadas, são extremamente importantes para o meu trabalho.

4.8 Comportamento de Segurança da Informação

A construção dos itens desse instrumento foi realizada com base em checklists utilizados em auditorias da área de segurança da informação. Nesse sentido, foram elaborados 26 itens e associados à escala do tipo likert 10 pontos (0= Nunca ; 10 =Sempre), com o intuito de verificar a frequência com que os indivíduos apresentam tais comportamentos em seu ambiente de trabalho.

Sua validação foi semântica e por juízes e alguns de seus itens foram alterados ou excluídos. O conteúdo dos itens descreve a percepção dos indivíduos quanto às ações que adotam com relação à segurança da informação em seu ambiente de trabalho, como por exemplo: escolho senhas de acordo com as normas de segurança, altero minhas senhas em intervalos regulares e utilizo uma senha diferente para cada serviço.

4.9 Procedimento de análise de dados

Para a realização da coleta de dados, o questionário foi disponibilizado no site LimeService e o link ficou disponível na Intranet da empresa pela universidade corporativa e pela equipe de comunicação da empresa. Cabe ressaltar que não existiam campos de identificação do respondente com o intuito de preservar o anonimato dos mesmos.

O link foi disponibilizado para os respondentes por 15 dias e foi colocado um banner na intranet com informações motivacionais para conseguir o maior número possível de participantes.

A aplicação ocorreu uma única vez nos entre agosto e setembro de 2011.

4.10 Tratamento e Análise dos dados

Após a coleta de dados, exportou-se uma planilha para o software SPSS 17.0 para realização das análises estatísticas. O primeiro procedimento seguido foi a limpeza do banco de dados para assegurar a qualidade das análises. Nesse sentido, o banco de dados da pesquisa foi submetido a análises descritivas e exploratórias a fim de verificar a presença de casos extremos e de casos omissos, a distribuição das variáveis e o tamanho da amostra.

Para o tratamento dos dados omissos, analisou-se a porcentagem de respostas por casos. Os casos que apresentaram menos de 50% do instrumento respondido foram excluídos, totalizando 249 casos. Observou-se que houve um padrão nos dados omissos: surgiam a partir da terceira escala. Cabe ressaltar que o questionário foi configurado de forma que os participantes só poderiam passar para os itens da próxima escala, caso tivessem respondido todos os itens da escala anterior. Nesse sentido, acredita-se que o número elevado de dados omissos se deva, principalmente, a forma de configuração do questionário e o número elevado de itens.

Para verificar a presença de outliers univariados – valores extremos de uma variável que podem distorcer as estatísticas, as variáveis foram transformadas em escore Z e eliminados os escores entre 2,5 e 4,00, critério adotado por Hair et al. (2009). Posteriormente, foram identificados os casos extremos multivariados por meio da distância Mahalanobis ($\alpha = 0,001$) cujo valor é igual a 43,98, o que resultou na exclusão de 5 casos.

Com isso, a validação/revalidação dos instrumentos foi feita com um banco de 423 casos, o que atende ao critério de Pasquali (2005), com um mínimo de 10 casos para cada variável.

Posteriormente, foram analisadas a normalidade e distribuição dos dados e o índice de fatorabilidade da matriz fatorial (KMO). Na análise do índice KMO, foi adotada a classificação de Kaiser (1974) que varia de 0,50 (inaceitável) a 0,90 (maravilhoso).

Foram, também, aplicadas a Análise dos Componentes Principais – Principal Componentes Analysis (PCA) e,para extração dos fatores, a análise Fatorial dos Eixos principais – Principal Axis Factoring (PAF), juntamente com o método de rotação Promax. Cabe

ressaltar que se adotou como critério para extração dos fatores a variância explicada e os autovalores superior a 2, além da análise do gráfico Scree plot (Anexo II) e análise paralela. Após a extração dos fatores, utilizou-se o coeficiente alfa de *Cronbach* para medir a consistência interna do instrumento. Ademais, para a análise de mediação, adotou-se as orientações de Baron e Kenny (1986).

5 RESULTADOS

Nesta seção serão descritos os procedimentos de análise dados, bem como os resultados obtidos. Para tanto, os procedimentos de análise exploratória, validação e revalidação das medidas serão apresentados primeiro e em seguida os procedimentos para a realização das regressões múltiplas e teste do modelo de mediação.

5.1 Práticas organizacionais de segurança da informação

Para validação da escala Práticas Organizacionais de Segurança da Informação (POSI), realizou-se análise fatorial. A matriz de correlação demonstrou-se fatorável haja vista que mais de 50% dos coeficientes da matriz foram superiores a 0,30. Além disso, o valor do KMO foi 0,95, resultado classificado como maravilhoso, conforme classificação de Kaiser (1974), confirmando a fatorabilidade da matriz.

Os valores de comunalidade também foram considerados ao se avaliar a variância comum entre a variável sendo analisada e as demais. Como não houve casos extremos, não foram detectados problemas com as comunalidades.

A análise dos Componentes Principais foi utilizada para realização de uma estimativa inicial do número de fatores. Tal método visa obter combinações lineares não correlacionadas. Pela análise da variância explicada obteve-se cinco fatores (valores < 3%); já pela análise dos autovalores e análise paralela obteve-se até dois fatores. Na análise do gráfico *Scree Plot* (Anexo II), por sua vez, foram identificados dois fatores. Ao final, foram considerados, nesta escala, 2 fatores (alfa de Cronbach = 0,91 e 0,90). O total da variância explicada foi de 55,58%. As cargas das variáveis em cada fator da matriz de Práticas Organizacionais de Segurança da informação (POSI), são apresentadas na Tabela 2.

Tabela 2. Matriz do instrumento POSI

Nº do Item	Descrição	Fator	
		1	2
1	Existe política ou diretrizes formais de segurança da informação na organização.		0,99
3	Existem regras de classificação da informação.		0,714
5	Existem controles de acesso às informações importantes.		0,704
15	É utilizado gerenciamento formal de criação e alteração de senhas para acesso aos sistemas de informação da organização.		0,694
12	São adotadas regras para o uso de correio eletrônico.		0,623
16	São adotadas diretrizes para orientar usuários na escolha e manutenção segura de senhas.		0,575
8	Os funcionários são orientados a adotar práticas de segurança da informação		0,542
2	A política de segurança da informação é comunicada para todos os funcionários.		0,504
13	São adotados procedimentos de autorização formal para a disponibilização pública das informações organizacionais.		0,495
6	Existem contratos formais que determinam as responsabilidades dos funcionários pela segurança da informação.		0,358
10	Os prestadores de serviços recebem treinamento sobre as políticas e procedimentos organizacionais de segurança da informação.	0,998	-0,306
14	Os funcionários receberam um documento contendo claramente os controles de acesso aos sistemas de informação da organização.	0,85	
9	Os funcionários recebem treinamento sobre as políticas e procedimentos organizacionais de segurança da informação.	0,822	
4	Os funcionários conhecem as regras de classificação da informação.	0,734	
18	São providos recursos para que os funcionários zelem pela segurança da informação.	0,665	
11	Os funcionários recebem atualizações regulares sobre as políticas e procedimentos organizacionais de segurança da informação.	0,648	
17	Existe auditoria para avaliar práticas de segurança da informação.	0,582	
7	Os funcionários são submetidos a acordos de confidencialidade na divulgação de informações.	0,486	

No instrumento POSI, cuja estrutura é composta por 18 itens, o item complexo 6 foi eliminado, por apresentar carga fatorial compartilhada nos dois fatores, com diferença inferior a 0,10, conforme critério adotado por Pasquali (2005). O item 17 foi, também, eliminado por não apresentar coerência teórica com o fator 1. Além disso, sua exclusão não altera significativamente o índice de confiabilidade.

O conteúdo dos 9 itens do fator 1 refletem os procedimentos e regras adotadas pela organização em sua rotina, portanto, tal fator foi denominado Práticas de Segurança

relacionadas à Rotina Organizacional – POSI - RO. Seu índice de confiabilidade é igual a 0,90 e a média da correlação item-total é de 0,73 e a variância explicada é de 30,2%.

Tabela 3. Detalhamento dos itens relacionados à escala de Práticas de Segurança relacionadas à rotina organizacional (POSI–RO)

Nº do Item	Descrição	Carga
1	Existe política ou diretrizes formais de segurança da informação na organização.	0,99
3	Existem regras de classificação da informação.	0,714
5	Existem controles de acesso às informações importantes.	0,704
15	É utilizado gerenciamento formal de criação e alteração de senhas para acesso aos sistemas de informação da organização.	0,694
12	São adotadas regras para o uso de correio eletrônico.	0,623
16	São adotadas diretrizes para orientar usuários na escolha e manutenção segura de senhas.	0,575
8	Os funcionários são orientados a adotar práticas de segurança da informação	0,542
2	A política de segurança da informação é comunicada para todos os funcionários.	0,504
13	São adotados procedimentos de autorização formal para a disponibilização pública das informações organizacionais.	0,495
Número de itens: 9		
Alpha (α): 0,90		

Com relação ao segundo fator, denominado Práticas de Segurança relacionadas aos Indivíduos – POSI - RI, este é composto por 7, itens que tratam das ações de segurança adotadas pela organização que são voltadas diretamente para os indivíduos. As cargas fatoriais variam de 0,99 a 0,48, alfa de *Cronbach* é de 0,91 e a variância explicada é de 25,38%.

Tabela 4. Detalhamento dos itens de Práticas de Segurança relacionadas aos indivíduos (POSI–RI)

Nº do Item	Descrição	Carga
10	Os prestadores de serviços recebem treinamento sobre as políticas e procedimentos organizacionais de segurança da informação.	0,998
14	Os funcionários receberam um documento contendo claramente os controles de acesso aos sistemas de informação da organização.	0,85
9	Os funcionários recebem treinamento sobre as políticas e procedimentos organizacionais de segurança da informação.	0,822
4	Os funcionários conhecem as regras de classificação da informação.	0,734
18	São providos recursos para que os funcionários zelem pela segurança da informação.	0,665
11	Os funcionários recebem atualizações regulares sobre as políticas e procedimentos organizacionais de segurança da informação.	0,648
7	Os funcionários são submetidos a acordos de confidencialidade na divulgação de informações.	0,486

Número de itens: 7

Alpha (α): 0,91

5.1.1 Atitudes frente às práticas de segurança da informação

Na escala de atitudes composta por 16 itens, obteve-se um KMO de 0,88, classificado como meritório, o que mostra a fatorabilidade da matriz. Com relação à matriz de comunalidade, não houve números extremos (0-1), o que não indica problemas. Pela variância explicada obteve-se 9 fatores. Na análise dos autovalores e análise paralela houve a indicação de até três fatores. No entanto, como um fator apresentou apenas uma variável, optou-se por excluir tal fator e retirar o item, já que este reduzia significativamente o Alfa de *Cronbach* quando incluído nos outros dois fatores.

Portanto, a escala de atitudes resultou em dois fatores (alfa de *Cronbach* = 0,88 e 0,81). Tais fatores explicam 51,35% da variância das atitudes perante as práticas de segurança da informação. Todos os itens foram mantidos na análise, já que todas as cargas eram superiores a 0,30 e não houve itens complexos com diferenças inferiores a 0,10.

Tabela 5. Matriz do instrumento ASI

Nº do Item	Descrição	Fator	
		1	2
12	As práticas de segurança da informação são invasivas.	0,777	
7	As práticas de segurança da informação criam mais problemas para os funcionários do que os auxiliam em seu dia-a-dia profissional.	0,738	
13	As práticas de segurança da informação restringem minha criatividade.	0,732	
15	As práticas de segurança da informação limitam minha atuação na organização.	0,686	
16	As práticas de segurança da informação fazem com que eu me sinta vigiado.	0,673	
5	As práticas de segurança da informação fazem me sentir confuso.	0,673	
10	As práticas de segurança geram desconfiança entre os funcionários da organização	0,642	
11	As práticas de segurança são cansativas.	0,641	
9	As práticas de segurança geram dúvidas quanto a sua adoção.	0,537	
1	As práticas de segurança requerem muito do meu esforço mental.	0,448	
6	As práticas de segurança são de responsabilidade do pessoal da Tecnologia da Informação.	0,373	
3	As práticas de segurança são extremamente importantes para o meu trabalho.		0,859
4	As práticas de segurança são do meu interesse.		0,802
8	As práticas de segurança contribuem para que os funcionários desta organização exerçam suas atribuições com qualidade.		0,742
14	As práticas de segurança geram tranquilidade.		0,608
2	As práticas de segurança são fáceis de ser utilizadas.		0,524

No instrumento ASI (16 itens) foram extraídos 2 fatores. O primeiro é composto por 11 itens, cargas fatoriais entre 0,78 e 0,37, índice de confiabilidade de 0,88, e a média da correlação item-total é de r=0,58 e a variância explicada pelo fator é de 9,55%. O fator foi denominado Atitudes Negativas em relação às práticas de segurança da informação (ANSI), já o conteúdo dos itens apresenta claramente as atitudes contrárias às práticas adotadas pela organização.

Tabela 6. Detalhamento dos itens relacionados à ANSI

Nº do Item	Descrição	Fator 1
12	As práticas de segurança da informação são invasivas.	0,777
7	As práticas de segurança da informação criam mais problemas para os funcionários do que os auxiliam em seu dia-a-dia profissional.	0,738
13	As práticas de segurança da informação restringem minha criatividade.	0,732
15	As práticas de segurança da informação limitam minha atuação na organização.	0,686
16	As práticas de segurança da informação fazem com que eu me sinta vigiado.	0,673
5	As práticas de segurança da informação fazem me sentir confuso.	0,673
10	As práticas de segurança geram desconfiança entre os funcionários da organização	0,642
11	As práticas de segurança são cansativas.	0,641
9	As práticas de segurança geram dúvidas quanto a sua adoção.	0,537
1	As práticas de segurança requerem muito do meu esforço mental.	0,448
6	As práticas de segurança são de responsabilidade do pessoal da Tecnologia da Informação.	0,373
Número de itens: 11		
Alpha (α): 0,87		

Já o fator 2 englobou 5 itens, cujo alfa de *Cronbach* é de 0,81. As cargas fatoriais (variação entre 0,85 e 0,56) e a média da correlação item-total (r=0,61) foram satisfatórias, e a variância explicada foi de 41,8%. Devido ao conteúdo a que se referem os itens, o fator foi denominado Atitudes Positivas em relação às Práticas de Segurança (APSI).

Tabela 7. Detalhamento dos itens relacionados à APSI

Nº do Item	Descrição	Carga
3	As práticas de segurança são extremamente importantes para o meu trabalho.	0,859
4	As práticas de segurança são do meu interesse.	0,802
8	As práticas de segurança contribuem para que os funcionários desta organização exerçam suas atribuições com qualidade.	0,742
14	As práticas de segurança geram tranquilidade.	0,608
2	As práticas de segurança são fáceis de ser utilizadas.	0,524
Número de itens: 5		
Alpha (α): 0,81		

5.1.2 Revalidação da escala de Percepção de mudança

Na revalidação da escala de Percepção de Mudança, aqui denominada Percepção de Mudança atribuída a Segurança da Informação (PMO), comprovou-se a fatorabilidade da matriz por meio do KMO, cujo índice foi meritório (0,87); no entanto, inferior ao encontrado por Pichi (2010), que foi de 0,94. Na análise da variância explicada, o instrumento apresentou 7 fatores e na análise dos autovalores também foram encontrados 7 fatores. Porém, esta solução não era condizente com a teoria base deste trabalho. Portanto, adotou-se o mesmo critério de Pichi (2010), considerando o autovalor superior a 2,0, o que resultou em um total de 2 fatores. Afinal, conforme Pasquali (2005), não se deve reter um fator apenas por parâmetros matemáticos, pois este deve possuir relevância no contexto científico. A estrutura bifatorial do instrumento explicou 23 % da variância de Percepção de Mudança Organizacional aplicada a Segurança da Informação.

Dos 33 itens do instrumento, dois foram excluídos por não apresentarem carga fatorial em nenhum dos fatores (24 e 33). Os itens 3, 4, 5, 6, 9, 23 e 27 foram excluídos do seu respectivo fator por não estarem relacionados ao conteúdo dos demais itens do fator em que se encontravam e por reduzirem o alfa quando adicionados no outro fator.

Tabela 8. Matriz de PMO

Nº do Item	Descrição	Fator 1	Fator 2
15	Contribuiram para que hoje a organização seja outra.	0,771	
24	Foram muito abrangentes.	0,691	
19	Fizeram com que as pessoas mudassem seus comportamentos.	0,661	
25	Alteraram o direcionamento da organização.	0,645	
31	Modificaram os valores da organização.	0,642	
17	Foram planejadas e direcionadas para os objetivos da organização.	0,641	
30	Já fazem parte do cotidiano da empresa.	0,639	
23	Estão sempre acontecendo nesta organização.	0,628	
22	Alteraram a cultura da organização.	0,627	
21	Alteraram as orientações tradicionais da organização.	0,61	
28	Alteraram a visão da organização.	0,604	
6	Foram acontecendo gradualmente.	0,533	
5	Foram necessárias para a sobrevivência da organização.	0,528	
29	Ocorreram devido às necessidades do dia-a-dia.	0,512	
18	Modificaram radicalmente o modo como as coisas eram feitas na organização.	0,508	
20	Aconteceram ao mesmo tempo em todos os setores da organização.	0,435	
27	Estavam relacionadas à implantação de novas tecnologias.	0,431	
3	Alteraram os procedimentos administrativos.	0,385	
12	Ocorreram porque era preciso mudar	0,383	
1	Afetaram toda a organização.	0,376	
5	Geraram pequenos ajustes no funcionamento da organização.	0,363	
4	Alteraram a forma de se trabalhar.	0,344	
16	Ocorreram pouco a pouco.	0,332	
14	Afetaram a empresa de cima para baixo.		
8	Foram superficiais.		0,67
26	Atingiram apenas certos grupos de empregados.		0,662
13	Ocorreram mesmo sem a participação da Alta Direção.		0,628
2	Afetaram apenas algumas áreas.		0,595
33	Ocorreram sem necessidade de planejamento.		0,574
9	Aconteceram de forma repentina.		0,562
10	Surgiram por iniciativa dos próprios empregados.		0,454
11	Ocorreram lentamente.		0,325
32	Modificaram pouco a dinâmica da organização		

Nesse sentido, o primeiro fator denominado Percepção de Mudança Organizacional Radical, resultou em 15 itens e alfa de *Cronbach* meritório (α = 0,89), com variância explicada de 12,8%.

Tabela 9. Detalhamento dos itens da escala Percepção de mudança organizacional radical

Nº do Item	Descrição	Carga
15	Contribuiram para que hoje a organização seja outra.	0,771
24	Foram muito abrangentes.	0,691
19	Fizeram com que as pessoas mudassem seus comportamentos.	0,661
25	Alteraram o direcionamento da organização.	0,645
31	Modificaram os valores da organização.	0,642
17	Foram planejadas e direcionadas para os objetivos da organização.	0,641
30	Já fazem parte do cotidiano da empresa.	0,639
22	Alteraram a cultura da organização.	0,627
21	Alteraram as orientações tradicionais da organização.	0,61
28	Alteraram a visão da organização.	0,604
5	Foram necessárias para a sobrevivência da organização.	0,528
18	Modificaram radicalmente o modo como as coisas eram feitas na organização.	0,508
20	Aconteceram ao mesmo tempo em todos os setores da organização.	0,435
12	Ocorreram porque era preciso mudar	0,383
1	Afetaram toda a organização.	0,376

Número de itens: 15

Alpha (α): 0,89

Já o segundo fator, Percepção de Mudança Organizacional Incrementa, l com 7 itens, apresentou um alfa de *Cronbach* de 0,80 (meritório) e variância explicada de 10,2%.

Tabela 10. Detalhamento dos itens da escala Percepção de mudança organizacional incremental

Nº do Item	Descrição	Carga
8	Foram superficiais.	0,67
26	Atingiram apenas certos grupos de empregados.	0,662
13	Ocorreram mesmo sem a participação da Alta Direção.	0,628
2	Afetaram apenas algumas áreas.	0,595
33	Ocorreram sem necessidade de planejamento.	0,574
10	Surgiram por iniciativa dos próprios empregados.	0,454
11	Ocorreram lentamente.	0,325
Número de Itens: 7		
Alpha (α): 0,80		

5.1.3 Comportamento de Segurança da Informação

Na validação da escala de Comportamentos de Segurança da Informação (CTSI), o KMO= 0,87 aponta para a sua fatorabilidade. Para a extração dos fatores, foram utilizadas a análise da variância, análise dos autovalores e análise do gráfico *Scree pot*.(Anexo II). A análise dos autovalores e análise paralela indicaram até 7 fatores. No entanto, como alguns fatores apresentaram alfa de Cronbach considerados inaceitáveis, optou-se pela adoção do critério de autovalores superior a 2,0, resultando em uma estrutura unifatorial (alfa de Cronbach= 0,88).

A Tabela 11 mostra a matriz do instrumento Comportamento de Segurança da Informação, com as cargas das variáveis do fator.

Tabela 11. Matriz do instrumento CTSI

Nº do Item	Descrição	Fator 1
3	Utilizo uma senha diferente para cada serviço.	0,369
4	Utilizo um bom programa antivírus.	0,608
5	Configuro o antivírus para verificar os arquivos obtidos pela Internet, HDs externos e unidades removíveis.	0,794
6	Desabilito no meu e-mail a auto-execução de arquivos anexados às mensagens.	0,608
7	Caso seja necessário abrir arquivos, certifico-me que foram verificados pelo programa antivírus.	0,707
8	Utilizo na divulgação de documentos, formatos menos suscetíveis à propagação de vírus, tais como RTF ou PDF.	0,552
9	Mantenho o sistema operacional e demais softwares do meu computador sempre atualizados.	0,629
10	Em meu computador, possuo firewall pessoal.	0,645
11	Utilizo pelo menos uma ferramenta anti-spyware.	0,752
12	Faço o download de programas diretamente do site do fabricante.	0,521
13	Certifico-me da procedência do site ao realizar transações via Web.	0,515
14	Estabeleço senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do meu computador.	0,591
15	Faço cópias dos dados do meu computador regularmente.	0,644
16	Armazeno as cópias dos dados do meu computador em local seguro.	0,625
17	Fico atento a e-mails ou telefonemas solicitando informações da organização.	0,346
18	Sempre que tenho dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entro em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.	0,36
20	Criptografo todos os dados sensíveis, principalmente se estiverem armazenados em notebook.	0,455

Dos 26 itens, 4 foram eliminados por não apresentarem carga fatorial suficiente para permanecerem no fator. O item nº 25 foi excluído por não apresentar carga fatorial no fator. E o item complexo nº 17 foi excluído por possuir carga no fator cuja diferença é inferior a 0,10. Já os itens 2 e 18 foram excluídos por não terem base teórica para permanecer no fator. Os itens 1, 21, 22 e 23 foram agrupados, a priori, em um segundo fator. No entanto, como o alfa de *Cronbach* desse fator não era satisfatório, optou-se por excluí-lo juntamente com os itens (que quando acrescentados no fator 1 reduziam significativamente o alfa de *Cronbach*).

O fator encontrado foi denominado Comportamentos de Segurança da Informação voltados para o computador de trabalho (CTSI-CT). As cargas fatoriais dos itens de CTSI - CT variaram entre 0,794 e 0,360, com Alfa de *Cronbach* de 0,889 e variância explicada de 18%. Os itens, suas respectivas cargas, bem como o Alfa estão dispostos na Tabela 12.

Tabela 12. Detalhamento dos itens relacionados à CTSI voltado para o computador

Nº do Item	Descrição	Carga
20	Criptografo todos os dados sensíveis, principalmente se estiverem armazenados em notebook.	0,455
16	Armazeno as cópias dos dados do meu computador em local seguro.	0,625
15	Faço cópias dos dados do meu computador regularmente.	0,644
14	Estabeleço senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do meu computador.	0,591
13	Certifico-me da procedência do site ao realizar transações via Web.	0,515
12	Faço o download de programas diretamente do site do fabricante.	0,521
11	Utilizo pelo menos uma ferramenta anti-spyware.	0,752
10	Em meu computador, possuo firewall pessoal.	0,645
9	Mantenho o sistema operacional e demais softwares do meu computador sempre atualizados.	0,629
8	Utilizo na divulgação de documentos, formatos menos suscetíveis à propagação de vírus, tais como RTF ou PDF.	0,552
7	Caso seja necessário abrir arquivos, certifico-me que foram verificados pelo programa antivírus.	0,707
6	Desabilito no meu e-mail a auto-execução de arquivos anexados às mensagens.	0,608
5	Configuro o antivírus para verificar os arquivos obtidos pela Internet, HDs externos e unidades removíveis.	0,794
4	Utilizo um bom programa antivírus.	0,608
3	Utilizo uma senha diferente para cada serviço.	0,369

Número de itens: 15

Alpha (α)*:* 0,889

No tópico seguinte, serão apresentadas as análises descritivas dos dados.

5.1.4 Análises descritivas

Nesta seção, é descrito o comportamento das variáveis de pesquisa. As variáveis analisadas foram: Práticas Organizacionais de Segurança da Informação voltadas para a rotina da organização (POSI – RO), Práticas Organizacionais de Segurança da Informação voltadas para os indivíduos (POSI–RI), Atitudes Negativas com relação às Práticas Segurança da Informação (ANSI), Atitudes Positivas com relação às Práticas de Segurança da Informação (APSI), Percepção de Mudança Organizacional Radical atribuída a Segurança (PMOR), Percepção de Mudança Organizacional Incremental atribuída a Segurança (PMOI) e

Comportamento de Segurança da Informação voltado para o computador de trabalho (CTSI – CT) .

A média aritmética, o desvio padrão e os coeficientes de variação das variáveis estão dispostos na Tabela 13.

Tabela 13. Estatísticas descritivas

Variável do modelo	Média	Desvio Padrão	Variância	Coeficiente de variação
POSI - RO	5,99	2,24	5.04	0,37
POSI - RI	8,14	1,69	2.89	0,2
ANSI	3,99	1,87	3.52	0,46
APSI	7,88	1,77	3.14	0,22
PMOR	6,67	1,51	2.29	0,22
PMOI	3,76	1,64	2.71	0,43
CTSI-CT	6,8	1,97	3.91	0,28

Depreende-se dos resultados que os respondentes percebem mais a existência de práticas organizacionais de segurança voltadas para os indivíduos (POSI – RI m = 8,14) do que àquelas voltadas para a rotina da organização (POSI – RO, m = 6,00). Ademais, as atitudes com relação à segurança apresentadas por eles são, em sua maioria, positivas (APSI, m= 8,00).

Com relação à Percepção de Mudança Organizacional, foram relatados maiores graus de Mudança Radical (PMOR, m = 6,67). Quanto ao Comportamento de Segurança da Informação, foi mais bem avaliado o voltado para o ambiente de trabalho (m = 8,38), sendo que o relacionado ao computador de trabalho apresentou maior grau de dispersão de opiniões (dp = 2,00).

5.1.5 Análise dos modelos

Para análise dos modelos, foram verificados os pressupostos de normalidade da distribuição de respostas, linearidade entre as variáveis, casos de multicolinearidade e homoscedastiidade. Para tanto, adotou-se os seguintes critérios: teste de assimetria (relacionado à similaridade das metades da distribuição) e curtose (achatamento da distribuição).

A assimetria de todas as variáveis oscilou entre -, 954 a, 486. Já as estimativas da curtose ficaram dentro dos limites de -,111 a ,684. Todas as variáveis apresentaram valores inferiores a 1, ou seja, problema de normalidade (assimetria e curtose) não acentuado e 50% das variáveis apresentaram distribuição mais achatada que a normal (curtose negativa). Nesse sentido, consoante os critérios de Tabachnick e Fidel (2001), acredita-se que os desvios de normalidade encontrados não são impeditivos da aplicação da análise multivariada. Ademais, 17 casos que apresentavam omissões em mais de 50% do instrumento ou escala foram excluídos com o intuito de evitar distorções nas análises.

A Tabela 14 apresenta as correlações bivariadas entre a variável Comportamento de Segurança da Informação em relação ao computador de trabalho – variável critério – e as seis variáveis antecedentes do modelo. A matriz revela que a variável APSI apresenta a mais forte correlação com a variável critério (0,37). No entanto, as variáveis antecedentes apresentaram maior correlação entre si mesmas do que com a variável critério, o que pode gerar baixo poder preditivo dos escores da regressão múltipla.

Tabela 14. Correlações bivariadas entre as variáveis.

Correlações							
	CTSI- CT	ANSI	APSI	POSI-RO	POSI- RI	PMOR	PMOI
CTSI - CT	1						
ANSI	-0,108	1					
APSI	0,372	-0,385	1				
POSI - RO	0,353	-0,123	0,485	1			
POSI - RI	0,324	-0,227	0,524	0,783	1		
PMOR	0,263	-0,028	0,528	0,489	0,477	1	
PMOI	-0,038	0,498	-0,172	-0,139	-0,28	-0,024	1

Para verificar o poder preditivo da variável Práticas Organizacionais de Segurança da Informação, realizou-se regressões lineares padrão tendo como variáveis critério os fatores de ASI e CTSI.

No modelo 1, a relação entre os fatores de Práticas de Segurança da Informação e Percepção de Mudança Organizacional foi testada. Dessa forma, o efeito de ambos os fatores de Práticas Organizacionais de Segurança da Informação voltadas para o indivíduo e voltadas para a organização sobre a percepção de mudança organizacional radical mostraram-se significativos ($p<0,001$). Portanto, o modelo 1 se confirmou e explicou, aproximadamente, 26% da variância de Percepção de Mudança Organizacional Radical ($R^2 = 0,26$ e $p <0,001$). Ao avaliar o valor de Beta (coeficiente de regressão padronizado), o fator Práticas Organizacionais de Segurança da Informação voltadas para a rotina organizacional apresentou maior efeito positivo ($\beta = 0,30$, $p<0,001$) sobre Percepção de Mudança Organizacional Radical, demonstrando seu papel preditor sobre a variável.

O Modelo 2 , por sua vez, visa investigar a relação dos dois fatores de POSI e PMO Incremental. Neste caso, o modelo explicou apenas 9% da variância de Percepção de Mudança Organizacional Incremental ($R^2 = 0,09$, $p<0,001$). Além disso, tanto o fator POSI – RO quanto POSI - RI apresentaram baixa correlação com a variável critério ($\rho= -0,14$ e $\rho= -0,28$). Na análise do valor de Beta, o fator Práticas Organizacionais de Segurança da Informação voltadas para a rotina organizacional, apresentou efeito positivo ($\beta = 0,15$, $p<0,001$), bem como no modelo 1, mostrando que quanto maior o valor de POSI-RO, maior o valor de percepção de mudança organizacional incremental.

Pode-se dizer, portanto, que as práticas voltadas para a rotina da organização, tais como, “Existem regras de classificação da informação” ou “São adotadas regras para o uso de correio eletrônico”, geram mudanças mais superficiais, afetando apenas algumas áreas da organização e, muitas vezes, ocorrem mesmo se a participação da alta direção.

No Modelo 3, foi analisada a relação entre Atitudes Negativas perante as práticas de Segurança da Informação – ANSI e os fatores de POSI. As variáveis de POSI apresentaram pouca contribuição, explicando juntas apenas 5% da variância da variável antecedente (R^2 = 0,05 e p<0,001). Neste caso, este modelo é refutado. Os resultados indicam que o efeito de POSI – RO sobre ANSI é de β = 0,14 p<0,001, e o de POSI – RI é de β = -0,33,p<0,001, ou seja, quanto maior for o valor de práticas organizacionais voltadas para a rotina organizacional maior será o valor de ANSI, e quanto maior o valor de práticas voltadas para o indivíduo menor será o valor de ANSI.

O Modelo 4 testa a relação entre Atitudes Positivas perante à Segurança da Informação – APSI e os fatores de POSI. Nesse sentido, as variáveis de POSI apresentaram uma contribuição significativa, explicando 28% da variância da variável antecedente (R^2 = 0,28 e p<0,001). Os resultados indicam que o efeito de POSI – RO sobre APSI é de β = 0,15 p<0,001 e de POSI – RI é de β = 0,38, p<0,001. Destarte, pode-se inferir que quanto maior a adoção de práticas organizacionais de segurança da informação mais os indivíduos apresentam atitudes positivas quanto ao tema, mostrando o poder preditivo da variável POSI sobre APSI.

No modelo 5, foi testada a relação entre comportamentos de segurança da informação voltados para o computador de trabalho e POSI. Este modelo explica 13% da variância da variável antecedente (R^2 = 0,13 e p<0,001). Na análise do Beta, pode-se observar que a POSI – RO apresentou maior poder preditivo (β = 0,26, p<0,001), ou seja, quanto maior é a adoção de práticas organizacionais de segurança da informação voltadas para a rotina organizacional mais os indivíduos adotam comportamentos de segurança da informação voltados para seus computadores de trabalho.

Por fim, o modelo 6 testou a relação entre comportamentos de segurança da informação voltados para o ambiente de trabalho e POSI. Nesse contexto, este modelo explicou cerca de 10% da variância da variável antecedente (R^2 = 0,10 e p<0,001).

A Tabela 15 apresenta os principais dados dos 5 modelos e suas versões, apresentados anteriormente.

Tabela 15. Compilação dos dados dos modelos preliminares – Variável antecedente POSI.

	Modelo 1		Modelo 2		Modelo 3		Modelo 4		Modelo 5	
Variável Critério	PMOR		PMOI		ANSI		APSI		CTSI - CT	
Variável Antecedente	Beta	R² do modelo	Beta	R² do modelo	Beta	R² do modelo	Beta	R² do modelo	Beta	R² do modelo
POSI - RO	0,3**		0,204**		0,139**		0,198**		0,267**	
POSI - RI	0,242**	0,262	,-44	0,095	-0,335	0,059	0,367**	0,288	0,109**	0,129

** significância p< 0,0001

Para verificar o poder preditivo da variável percepção de mudança organizacional atribuída à segurança da informação, realizou-se regressões lineares padrão tendo como variáveis critério os fatores de ASI e CTSI.

No modelo 1, a relação entre os fatores de percepção de mudança organizacional e atitudes negativas perante as práticas de segurança da informação foi testada. A partir das análises, pode-se verificar que o modelo 1 explica, aproximadamente, 25% da variância de Atitudes Negativas perante as práticas de Segurança da Informação(R^2 = 0,25 e p <0,001). Ao avaliar o valor de Beta, o fator Percepção de Mudança Organizacional Radical apresentou grande efeito positivo (β = 0,50, p<0,001) sobre Atitudes Negativas perante as práticas de Segurança da Informação. Pode-se, portanto, inferir, que quanto mais os indivíduos percebem a mudança organizacional como sendo incremental, mais negativa é a atitude com relação à segurança da informação por eles apresentada.

No Modelo 2, visa-se investigar a relação dos dois fatores de PMO e Atitudes Positivas perante as práticas de Segurança da Informação. Os dois fatores juntos explicam 30% da variância de Atitudes Positivas perante a Segurança da Informação (R^2 = 0,30, p<0,001). Na análise do valor de Beta, o fator Percepção de Mudança Organizacional Radical, apresentou maior efeito positivo (β = 0, 61, p<0,001). Nesse caso, quanto maior a percepção de mudança organizacional radical, mais positiva é a atitude dos indivíduos quanto à segurança.

O Modelo 3 apresentou a relação entre Comportamentos de Segurança da Informação voltadas para o Computador de Trabalho e os fatores de PMO. As variáveis de PMO

apresentaram pouca contribuição para o modelo, já que explicam juntas, apenas 7% da variância da variável antecedente (R^2 = 0,07 e p<0,001). Os resultados indicam que o efeito de PMOR sobre CTSI- CT é de β = 0,26, p<0,001, e o de PMOI é de β = -0,03, p<0,001, indicando que a direção da relação PMOR → CTSI-CT é direta, já a direção da relação PMOI→ CTSI-CT é inversa. Diante disso, é possível afirmar que diante de mudanças radicais, ou seja, que são caracterizadas por serem abrangentes, por modificarem os valores da organização, por alterarem a cultura e a visão desta, dentre outras características, os indivíduos tendem a adotar mais comportamentos de segurança do que quando as mudanças são do tipo incremental.

O Modelo 4 testa a relação entre Comportamentos de Segurança da Informação voltadas para o Ambiente de Trabalho e os fatores de PMO. Nesse sentido, as variáveis de PMO apresentaram, também, pouca contribuição, explicando 7% da variância da variável antecedente (R^2 = 0,07 e p<0,001). Pode-se perceber que quanto maior a percepção de mudança incremental menos os indivíduos percebem os comportamentos de segurança.

Na Tabela 16, encontram-se dispostos os principais dados dos 3 modelos e suas versões, conforme apresentado anteriormente.

Tabela 16. Compilação dos dados dos modelos preliminares – Variável antecedente PMO.

	Modelo 1		Modelo 2		Modelo 3	
Variável Critério	ANSI		APSI		CTSI-CT	
Variável Antecedente	Beta	R² do modelo	Beta	R² do modelo	Beta	R² do modelo
PMOR	,-017		0,524**		0,262**	
PMOI	0,498**	0,249	-0,16	0,304	-0,033	0,07

** significância p< 0,0001

Após analisar o papel preditor de Práticas Organizacionais de Segurança da Informação e Percepção de Mudança Organizacional, a segunda parte desta seção verifica se a relação de POSI e PMO com o comportamento dos indivíduos é mediada pelos pelas atitudes por eles apresentadas.

A mediação é um conceito que implica suposição de relacionamentos causais entre as variáveis envolvidas. Nesse sentido, uma variável mediadora é aquela que, ao estar presente na equação de regressão, diminui a magnitude do relacionamento entre a variável antecedente

e a critério. Para testar o efeito mediador, utilizou-se o método de Baron e Kenny (1986). Consoante esse método, são necessários quatro passos, alcançados por meio de três equações de regressão, para estabelecer se uma variável é mediadora de uma relação entre a variável antecedente e a critério:

a) Mostrar que há uma relação significativa entre a variável mediadora e a critério;
b) Mostrar que a variável antecedente está relacionada com a mediadora;
c) Mostrar se a força da relação entre a variável antecedente e a critério é significativamente reduzida quando a mediadora for adicionada ao modelo.

Ao analisar se os modelos de mediação que seriam testados atendiam a todas as condições, foram encontradas algumas dificuldades: a variável mediadora Atitudes Negativas perante as práticas de Segurança da Informação apresentou fraca relação com ambos os fatores da variável critério (R^2 = 0,06 e R2 = 0,06) e com as variáveis antecedentes. Ademais, a variável antecedente PMO Incremental apresentou fraca relação com o fator da variável critério CTSI (R^2 = 0,07). Por isso, a variável Atitudes Negativas frente a Segurança da Informação neste estudo não pôde ser considerada mediadora da relação entre POSI e PMO atribuída a segurança da informação em nenhuma de suas escalas. A variável antecedente PMO Incremental também não foi considerada devido ao seu baixo poder preditivo com relação às outras variáveis do modelo.

5.1.6 Modelo de Mediação com CTSI – CT como variável critério

Para teste do modelo de mediação, primeiramente, analisou-se a influência da variável antecedente – Práticas Organizacionais de Segurança da Informação voltadas para a rotina da organização – sobre a variável critério – Comportamentos de Segurança da informação voltadas para o computador de trabalho.

Posteriormente, fez-se a análise de regressão incluindo as variáveis antecedentes sobre a variável mediadora – atitudes positivas perante a segurança da informação. As duas primeiras equações foram repetidas utilizando-se a variável PMO – Radical como antecedente. Por fim, realizou-se a análise incluindo todas as variáveis, como antecedentes as práticas organizacionais de segurança da informação, a percepção de mudança organizacional radical

e as atitudes positivas perante a segurança, e como variável critério o comportamento de segurança da informação voltado para o computador de trabalho.

Teste da 1ª Equação

Primeiramente, buscou-se verificar se as variações na variável antecedente – POSI – RO e RI – explicavam uma porção significativamente diferente de zero da variável critério CTSI – CT (Figura 6).

A relação entre as variáveis já havia sido testada nos modelos apresentados anteriormente. A condição foi satisfeita com a variável POSI como antecedente.

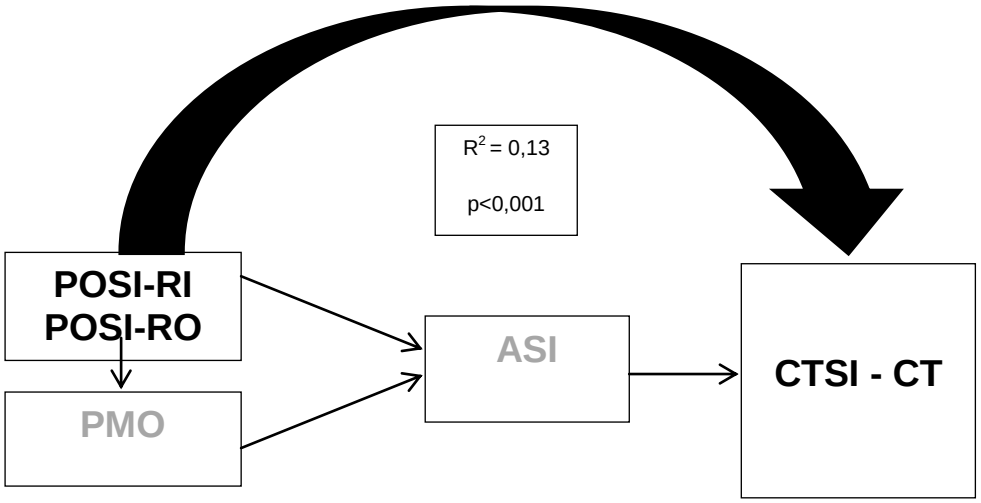


Figura 6. Teste da 1ª equação (CTSI – CTI como variável critério do modelo de mediação).

Teste da 2ª equação

A segunda equação teve o intuito de verificar se as variações na variável antecedente POSI explicavam uma porção significativamente diferente de zero da variável mediadora Atitudes Positivas perante a Segurança da Informação (Figura 7). Tal condição foi satisfeita, já que Práticas Organizacionais de Segurança da Informação explica aproximadamente 28% de Atitudes Positivas perante a Segurança da Informação (p<0,001).

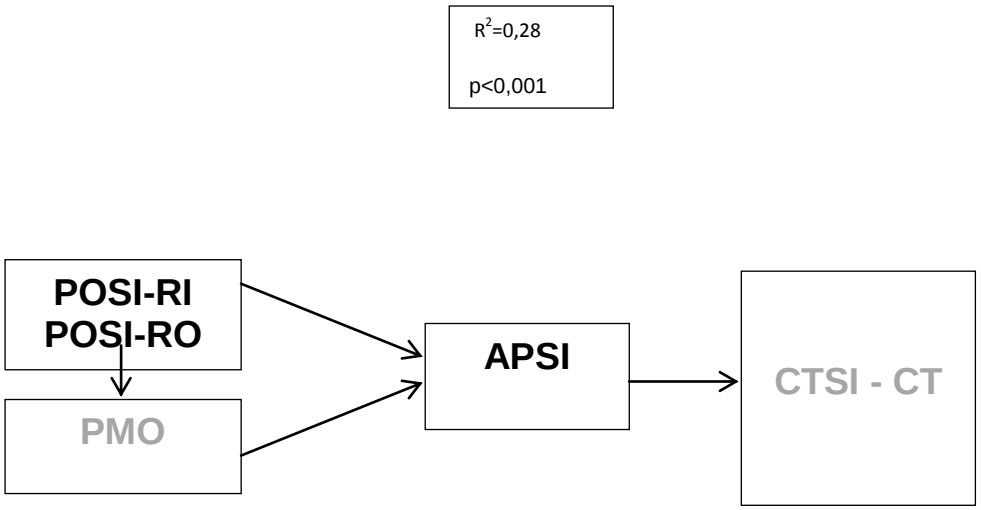


Figura 7. Teste da 2ª equação (ASI como variável critério do modelo de mediação).

Posteriormente, as duas primeiras equações foram repetidas tendo, no entanto, a variável Percepção de Mudança Organizacional Radical atribuída a Segurança da Informação como variável antecedente e a variável CTSI – CT como critério.

Teste da 1ª Equação

Nesta etapa, verificou-se se as variações a variável antecedente – PMOR explicou uma porção significativamente diferente de zero da variável critério CTSI – CT (Figura 8). Assim, a condição foi satisfeita com a variável PMOR como antecedente (R2 = 0,70, p<0,001).

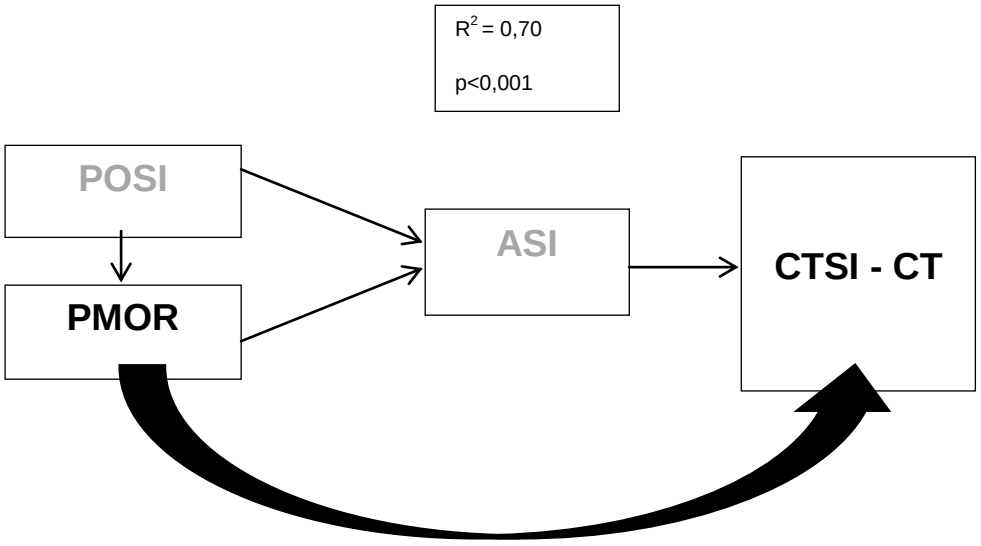


Figura 8. Teste da 1ª equação (CTSI – CT como variável critério do modelo de mediação).

Teste da 2ª equação

A segunda regressão verificou se as variações na variável antecedente PMOR explicavam uma porção significativamente diferente de zero da variável mediadora Atitudes Positivas perante a Segurança da Informação (Figura 9). A condição foi satisfeita, pois Percepção de Mudança Organizacional Radical atribuída a Segurança da Informação explicou, aproximadamente, 28% de Atitudes Positivas perante a Segurança da Informação (p<0,001).

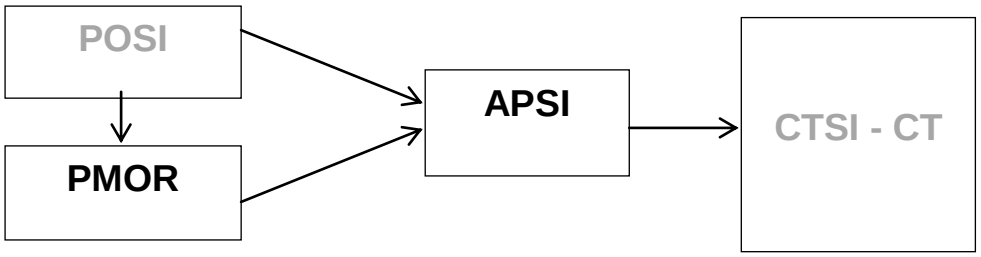


Figura 9. Teste da 2ª equação (APSI como variável critério do modelo de mediação).

Teste da 3ª Equação

A 3ª equação testa se a variável mediadora APSI explica uma porção significativamente diferente de zero da variável critério CTSI- CT, conforme ilustra a figura 10.

A condição foi satisfeita, já que a variável mediadora Atitudes Positivas perante as práticas de Segurança da Informação explicou aproximadamente 18% da variável critério CTSI – CT (p< 0,001).

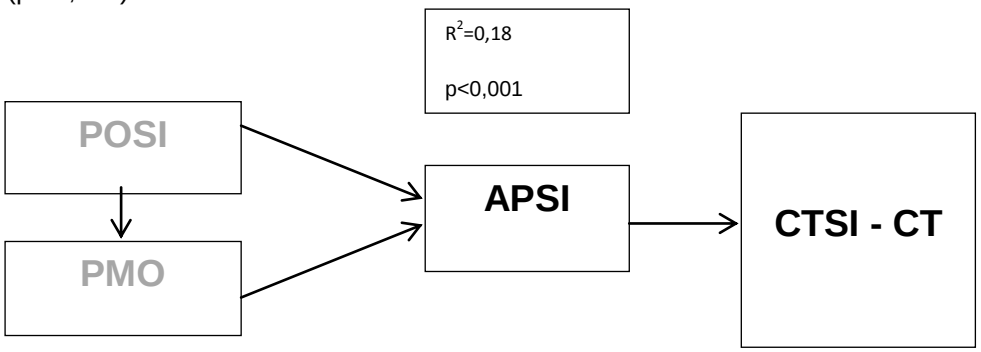


Figura 10. Teste da 3ª equação (CTSI- CT como variável critério do modelo de mediação).

A Figura 11 apresenta o resultado das 3 equações.

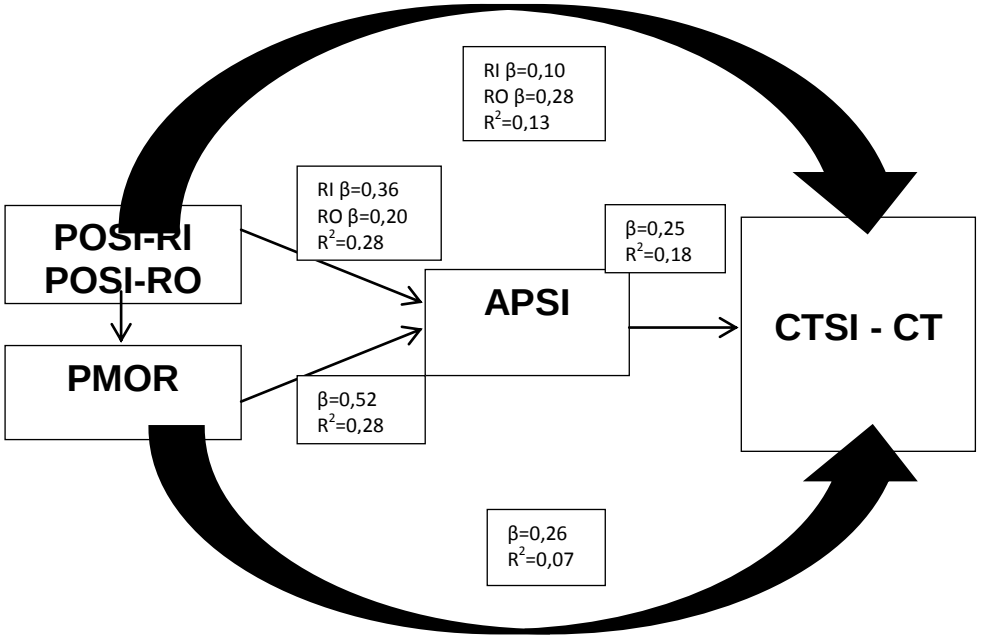


Figura 11. Resultado das 3ª equações

Posteriormente, a variável mediadora foi introduzida no modelo com o intuito de confirmar a mediação. Dessa forma, deve haver redução dos coeficientes de B e Beta das variáveis antecedentes (POSI e PMOR) quando comparados com o modelo composto apenas pela variável antecedente e critério, conforme Baron e Kenny (1986). Cabe ressaltar, entretanto, que a mediação se confirma mais pelo valor de beta.

Tabela 17. Detalhamento dos resultados (CTSI – CT como variável critério do modelo de mediação).

	Coeficientes de regressão			Sig. Estatística		Correlações			Estatísticas de Colinearidade	
Variáveis do modelo	B	Erro Padrão	Beta	*t*	Sig.	Ordem zero	Parciais	Semi-parciais	Tolerância	VIF
APSI	0,286	0,063	0,26	4,512	0	0,375	0,219	0,203	0,624	1,604
POSI -RO	0,185	0,073	0,21	2,847	0,005	0,263	0,14	0,128	0,369	2,708
POSI - RI	0,012	0,065	0,01	0,135	0,893	0,353	0,007	0,006	0,36	2,779
PMOR	0,025	0,087	0,02	0,348	0,728	0,318	0,017	0,016	0,646	1,549
R^2= 0,179										

Variável Critério: Comportamento de Segurança da Informação voltado para o computador de trabalho

Pôde-se constatar que houve baixo declínio do Beta da relação entre POSI-RO e CTSI-CT de 0,26 na primeira equação, para 0,21 com a inserção da variável mediadora no modelo. O declínio foi maior com a variável POSI-RI que foi de 0,10 para 0,010. Com a variável PMOR houve, também, um grande declínio de 0,26 para 0,02. A partir dos resultados, depreende-se que Atitudes Positivas perante a Segurança da Informação parecem mediar a relação entre os dois fatores de POSI, PMOR e CTSI- CT.

A seguir será apresentada a discussão dos resultados à luz da teoria apresentada nos capítulos 2, 3 e 4.

5.2 Discussão

A segurança da informação não se restringe apenas à segurança computacional, de redes, sistemas ou segurança física, pois seu sucesso depende, principalmente, das pessoas envolvidas (Dias, 2001). Nesse sentido, o intuito da presente pesquisa foi abordar a segurança sob a ótica dos indivíduos, buscando entender de que forma as intervenções no nível organizacional, como a adoção de práticas de segurança e mudança organizacional, influenciam no nível individual (atitudes e comportamentos).

Além disso, a variável mudança organizacional foi inserida no escopo da pesquisa, já que segundo Vieira (2009), a adoção de práticas de segurança gera mudanças na estrutura da organização, nos comportamentos de seus funcionários e até mesmo na cultura organizacional. Nesse sentido, foi analisado se as intervenções no nível organizacional

desencadearam mudanças comportamentais, já que segundo Neiva (2004) uma intervenção efetiva deve ter como primeira consequência a alteração do comportamento no trabalho.

Neste capítulo serão apresentados os resultados à luz da teoria, abordando os seguintes tópicos: medidas, dados descritivos, modelos preliminares, modelos de mediação, limitações da pesquisa e considerações finais.

5.2.1 Medidas

Na validação da medida Práticas Organizacionais de Segurança da Informação obteve-se uma estrutura bifatorial e a correlação entre os fatores foi alta (r =, 78). Tal correlação demonstra que há forte correlação entre os fatores Práticas Organizacionais de Segurança da Informação voltadas para a rotina da organização e voltadas para os indivíduos. Além disso, o alfa de *Cronbach* de ambos os fatores foi bem expressivo (α = 0,91 e α = 0,90), indicando, portanto, um grau elevado de consistência interna do instrumento. Embora os dois fatores possam ser considerados parte integrante um do outro, devido à alta correlação em ambos, a diferenciação entre os dois se faz necessária.

As práticas classificadas como voltadas para a rotina da organização afetam diretamente o dia-a-dia da organização e até mesmo sua cultura e estruturação, como, por exemplo, ao se adotar regras de classificação da informação e controles de acesso a informações importantes. Já as práticas classificadas como voltadas para os indivíduos atingem diretamente os funcionários, tal como, a prática de prover recursos para que os funcionários zelem pela segurança da informação, ou mesmo, o treinamento dos funcionários.

Outrossim, os sujeitos podem perceber de forma distinta os dois fatores, como ocorreu neste estudo, cuja percepção de práticas organizacionais de segurança da informação voltadas para os indivíduos foi maior do que a percepção das práticas voltadas para a rotina da organização (POSI – RI m = 8,14, dp= 2,24; POSI – RO m= 5,99, dp = 1,69).

Quanto à validação da escala de atitudes em Segurança da Informação, esta também apresentou estrutura formada por dois fatores, claramente distintos um do outro. Tal fato é devido não apenas ao conteúdo dos itens, como também, a correlação negativa e de baixa magnitude apresentada entre os fatores (r = - 385). Ademais, os índices estatísticos apontam

para a qualidade psicométrica da medida. A média das correlações item-fator também é boa (APSI r= 0,58; ANSI r=0,61). Tal estrutura corrobora com os achados na literatura (Smith et al.,2000 ; Dambrot et al.;1985).

A revalidação da medida de percepção de mudança organizacional apontou para uma estrutura de dois fatores, conforme os estudos de Pichi (2010) e Domingos (2009). No entanto, houve uma redução do alfa de *Cronbach*, de 0,88 para 0,80 de PMO-Incremental e de 0,96 para 0,89 de PMO- Radical; quando comparado com os dados de Pichi (2010); o que pode ser devido à diferença no número de itens de cada fator. Quanto à composição dos fatores, obteve-se estrutura similar à encontrada por Pichi (2010), já que os itens 3, 4, 5, 6, 9, 23, 27 e 33 foram excluídos em ambas as pesquisas. Os itens que compõem cada fator também foram semelhantes, salvo alguns itens que foram mantidos nas escalas desta pesquisa. Ao se comparar o resultado aqui encontrado com a teoria (classificação de mudança radical e incremental de Domingos, 2009; Pichi,2010), nota-se uma convergência entre os princípios teóricos definidos como mudança organizacional radical e incremental e as dimensões empiricamente testadas.

Por fim, na validação da escala de comportamento de segurança da informação foi encontrada, primeiramente, uma estrutura bifatorial cujos fatores apresentaram correlação moderada (r=0,41). Os fatores foram denominados Comportamentos de Segurança da Informação voltados para o computador e voltados para o ambiente de trabalho. No entanto, como o segundo fator apresentou baixa consistência interna, optou-se por excluí-lo, o que resultou em uma estrutura unifatorial.

As escalas de Práticas Organizacionais, Atitudes e Comportamento relacionados à Segurança da Informação apresentam uma novidade com relação a outros estudos. A literatura, principalmente em português, utiliza como forma de mensuração das práticas, atitudes e comportamentos em segurança, *checklists* ou pesquisas cuja abordagem é predominantemente qualitativa. Portanto, os instrumentos aqui construídos e validados parecem ser adequados e fidedignos para mensuração dessas variáveis e podem servir como base para os estudos vindouros.

No entanto, aponta-se para a necessidade de aplicar tais instrumentos em outros contextos, tendo em vista a realidade de cada organização. Alguns itens talvez necessitem ser ajustados ou excluídos, como por exemplo, nem todas as organizações permitem que os seus funcionários instalem programas em suas máquinas, portanto os itens da escala de comportamento que se referem à instalação de software devem ser excluídos.

O instrumento de Percepção de Mudança Organizacional também necessita ser reaplicado, a fim de se verificar a estabilidade da estrutura fatorial encontrada neste estudo e nos achados de Domingos (2009) e Pichi(2010).

5.2.2 Resultados Descritivos

Depreende-se dos resultados que as pessoas percebem mais as práticas organizacionais voltadas para os indivíduos (m= 8,14, dp= 1,69) do que as voltadas para a rotina organizacional (m= 5,99, dp= 2,24). A prática mais percebida pelos respondentes foi a existência de política ou diretrizes formais de Segurança da Informação, o que indica que provavelmente essa prática tem sido bem divulgada. Cabe ressaltar que constitui um dos fatores críticos de sucesso para a Segurança da Informação, segundo a norma ABNT ISO/IEC 27002, a correta divulgação da política e das normas de segurança a todos os diretores, funcionários e outras partes.

Outra prática apontada por grande parte dos respondentes foi à relacionada ao treinamento sobre as políticas e procedimentos organizacionais de segurança, o que indica que a organização fornece treinamentos de Segurança da Informação para seus funcionários. As práticas relacionadas à existência de regras de classificação da informação e controles de acesso foram, também, apontadas pelos respondentes. Já as práticas relacionadas a procedimentos de autorização formal para a disponibilização pública das informações e existência de acordo de confidencialidade na divulgação de informações da organização foram menos percebidas.

Com relação às atitudes dos respondentes quanto a segurança, estes apresentaram mais atitudes positivas (m= 7,88, dp= 1,77), o que pode apontar certo nível de desejabilidade social na escala de atitudes, conforme alerta Azjen (1991).Além disso,a maioria acredita que as

práticas de segurança são de extrema importância para o seu trabalho e apresenta interesse com relação a elas. No entanto, grande parte dos respondentes acreditam que as práticas são invasivas e que criam mais problemas para os funcionários do que os auxiliam em seu dia a dia profissional. Um dado interessante é que poucos acreditam que as práticas de segurança sejam de responsabilidade apenas da área de Tecnologia da Informação, o que indica que os respondentes reconhecem seu papel no contexto da segurança levando-os a adotarem mais as práticas organizacionais.

A percepção de mudança organizacional incremental obteve pior resultado por parte dos respondentes (m= 3,76, dp = 1,64), indicando que as mudanças ocasionadas pelas práticas organizacionais de segurança tendem a ser mais radicais. Ou seja, tais mudanças são capazes de alterar a cultura da Empresa, sua visão, o comportamento dos indivíduos e a forma como as coisas são feitas. É possível afirmar, portanto, que as práticas de segurança da informação provocaram mudanças na organização, corroborando com os achados de Vieira (2009). Nesse sentido, é importante que as organizações ao adotarem um programa de Segurança da Informação, realizem gestão de mudanças. Tal gestão pode ser feita por meio de criação de comitê, que seria responsável pela divulgação das mudanças e conscientização de sua importância para a organização.

Ainda com relação à mudança organizacional, os respondentes perceberam que as mudanças ocasionadas pelas práticas de segurança contribuíram para que a organização seja outra. Além disso, perceberam que houve mudança de comportamento dos indivíduos, corroborando com os estudos que apontam para a existência de ligação entre comportamentos individuais e mudanças organizacionais (Neiva, 2004). Os respondentes perceberam, também, que as práticas já fazem parte do cotidiano da empresa e que alteraram sua cultura e orientações tradicionais. No entanto, a coleta de dados foi realizada alguns anos após as primeiras intervenções na organização, o que pode ter afetado os resultados.

Com relação ao Comportamento de Segurança da Informação, os comportamentos mais adotados pelos respondentes foram os relacionados a ferramentas de segurança, como antivírus, *antispyware* e *firewal*l. Os respondentes apresentaram, também, comportamentos relacionados a backup de dados e atualização de softwares. Já o comportamento menos

adotado foi o relacionado à utilização de uma senha diferente para cada serviço, o que pode ser devido à dificuldade em se memorizar várias senhas.

5.2.3 Relação entre as variáveis e modelos preliminares

A literatura da área de segurança da informação tem enfatizado a importância de se adotar ações de segurança voltadas para os indivíduos nas organizações, levando em consideração fatores organizacionais e culturais, principalmente, ao se tratar de atitudes e comportamentos de segurança. (Albrechtsen, 2007; Vieira, 2009). Portanto, esse estudo traz as variáveis Práticas Organizacionais de Segurança da Informação e Percepção de Mudança Organizacional atribuída à Segurança da Informação como variáveis do ambiente e avalia seu impacto no nível individual, analisando, também, a relação atitude-comportamento e a capacidade mediadora do construto atitude, conforme os estudos de Azjen (1991) e Fishbein e Azjen (1975).

Práticas Organizacionais de Segurança da Informação apresentou baixa contribuição na predição de Atitudes Negativas de Segurança (R^2=0,06), mas apresentou forte poder preditivo ao se tratar de atitudes positivas (R^2=0,28). Com relação ao comportamento, mostrou contribuição moderada ao predizer comportamentos voltados para o computador de trabalho (R2=0,13).

Quanto à Percepção de Mudança Organizacional, a variável Práticas Organizacionais mostrou-se forte preditora de mudança radical (R^2 = 0,26). No entanto, pouco contribui com a predição de mudanças incrementais; o que sugere que adoção de práticas organizacionais de segurança tende a gerar mudanças de maior escopo e abrangência, capazes de atingir componentes essenciais da organização, como o comportamento dos indivíduos e cultura da organização. Tal fato corrobora com os achados de Vieira (2009), que verificou o impacto da segurança da informação na cultura da organização pesquisada.

Ao mensurar o poder preditivo da variável Percepção de Mudança Organizacional, pôde-se perceber o seu forte poder preditivo com relação aos dois fatores de atitudes, explicando cerca de 30% da variância das variáveis. No entanto, a variável explicou apenas 7% da variância do comportamento. Isso indica que a curto prazo, as atitudes dos indivíduos perante

a segurança da informação tendem a ser afetadas pelas mudanças, notadamente àquelas de grande escopo. No entanto, em longo prazo tais atitudes podem alterar o comportamento apresentado por eles, consoante Zimbardo e Leippe (1991).

A organização pesquisada pode ser caracterizada como tendo práticas voltadas para Segurança da Informação. Os resultados encontrados levam a crer que tais práticas geraram mudanças de natureza radical na organização. Além disso, as atitudes dos indivíduos quanto à segurança, são em sua maioria, positivas. Cabe ressaltar que na literatura foram encontrados poucos relatos de pesquisa que tenham investigado a relação entre a percepção de mudança organizacional e o comportamento dos indivíduos.

5.2.4 Modelos de mediação

A partir dos resultados, pôde-se confirmar o modelo de mediação entre a relação Práticas Organizacionais de Segurança da Informação voltadas para o ambiente de trabalho e para a rotina da organização, Percepção de Mudança Organizacional Radical e Comportamentos de Segurança da Informação voltados para o computador de trabalho, sendo mediadas (Baron & Kenny, 1986) pelas atitudes que os indivíduos possuem sobre Segurança da Informação.

A mediação mostra que uma parte moderada dos efeitos das práticas e a percepção de mudança se deve à influência das atitudes positivas perante a segurança da informação. Isso leva a crer que outras variáveis podem também influenciar o comportamento, tais como a cultura organizacional, os valores dos indivíduos, ou mesmo as intenções, conforme a relação atitude-comportamento de Fishbein e Ajzen (1975). Cabe ressaltar que as variáveis individuais, como idade e tempo de serviço, podem ter influenciado nos resultados, já que a maior parte dos respondentes tinha entre 21 a 30 anos de serviço e de 46 a 55 anos de idade.

Por fim, o modelo de pesquisa corrobora com a análise correlacional de Bentler e Speckart (1981) que demonstra que atitudes têm prioridade causal sobre comportamentos. As mediações importantes do modelo foram POSI-RI e PMOR mediadas pelas atitudes positivas, que no modelo desse estudo, apresentou maior poder de mediação.

5.2.5 Limitações e considerações para futuras pesquisas

As organizações têm investido, em maior parte, nas práticas organizacionais voltadas para as rotinas organizacionais (controle de acesso, adoção de política de segurança, dentre outras). No entanto, essa pesquisa buscou mostrar o importante efeito das práticas voltadas para os indivíduos (treinamentos e conscientização) e da mudança organizacional delas decorrentes nas atitudes e comportamentos que os indivíduos apresentam diante da segurança. Além disso, buscou-se adotar um método diferente das pesquisas sobre segurança da informação, ao se utilizar a análise de mediação e regressão múltipla.

Com relação às escalas construídas, aponta-se para a necessidade de uma revalidação em contextos diferentes a fim de se testar a estabilidade da estrutura proposta nesta pesquisa.

Pode-se dizer que os objetivos foram alcançados e que os resultados encontrados podem contribuir na construção do conhecimento científico na área de segurança da informação. Ademais, pode servir como base para diagnóstico da situação atual da organização com relação à segurança da informação, bem como, para criação de programas de conscientização, treinamentos e educação.

Cabe, no entanto, ressaltar algumas limitações deste estudo:

- Escopo reduzido, já que a aplicação foi realizada em apenas uma organização, devido, principalmente, à preocupação das organizações em expor suas vulnerabilidades de segurança.
- Utilização de uma medida adaptada para a realidade da organização participante. Portanto, recomenda-se cautela nas generalizações dos resultados.
- Utilização de escalas perceptuais e limitação a autoavaliações dos próprios participantes. Recomenda-se a utilização de índices duros para relacioná-los com os resultados de percepção.

Para pesquisas futuras, sugere-se:

- Desenvolvimento de outros itens para a escala de Comportamento.
- Inclusão da variável cultura como antecedente em modelos de regressão cuja variável critério seja o comportamento;
- Revalidações das escalas utilizadas nesta pesquisa para confirmação da estrutura fatorial;

- Reformulação das escalas de Percepção de Mudança Incremental e Atitudes Negativas de Segurança da Informação.

6 Considerações Finais

Os indivíduos exercem um papel fundamental no contexto da segurança da informação. Portanto, para que os programas de segurança adotados pelas organizações obtenham sucesso é preciso investir também no *fator humano* e não apenas nos recursos tecnológicos.

Essa pesquisa teve o objetivo de investigar o comportamento dos indivíduos com relação à segurança da informação e alguns fatores que o influenciam – práticas organizacionais, mudança organizacional e atitudes. Para tanto, propôs-se a seguinte pergunta de pesquisa: as práticas organizacionais de segurança da informação e a percepção de mudanças atribuídas a essas práticas influenciam as atitudes e a adoção de comportamentos de segurança da informação nas organizações?

De fato, as Práticas Organizacionais de Segurança e a Percepção de Mudança Organizacional mostraram exercer influência sobre as atitudes e os comportamentos dos indivíduos. Ressalta-se que as práticas e mudanças organizacionais apresentaram grande influência sobre as Atitudes Positivas dos indivíduos. Além disso, os indivíduos perceberam mudança radical como resultado da adoção de práticas adotadas pela organização; e ambas as variáveis apresentaram influência, embora moderada, no comportamento, mostrando-se significativos estatisticamente na predição de comportamento frente à segurança.

A relação atitude-comportamento, embora tenha tido efeito de predição modesto nessa pesquisa, pode gerar mudanças nos comportamentos dos indivíduos, o que enfatiza a importância do construto para os estudos relacionados com comportamento, conforme apontado por Azjen (1991) e Fishbein e Azjen (1975).

Cabe ressaltar que outras variáveis podem igualmente exercer influência sobre o comportamento em Segurança da Informação e precisam ser levadas em consideração no momento da elaboração de programas de segurança nas organizações. Destacam-se a cultura organizacional, o clima organizacional, valores, impacto de treinamento e variáveis individuais, como idade, tempo de serviço e setor.

Diante dos resultados dessa pesquisa, recomenda-se que as organizações não tratem a Segurança da Informação como um assunto restrito apenas para a equipe de tecnologia da informação. Por ser um tema multidisciplinar, é importante que outras áreas estejam envolvidas

na elaboração dos programas de segurança, notadamente, a área de gestão de pessoas que pode contribuir para a capacitação dos indivíduos quanto a esse aspecto.

Além disso, o trabalho a ser desenvolvido com os indivíduos deve ser continuo, não bastando apenas ações de conscientização e treinamentos esporádicos. É preciso que as práticas organizacionais ao serem implantadas, sejam comunicadas a todos os funcionários e que todos recebam orientações sobre como adotá-las da forma correta. As mudanças organizacionais decorrentes das práticas – como uso de controle de acesso biométrico- devem, também, ser comunicadas a todos. Recomenda-se, também, que as práticas e procedimentos sejam adequados à realidade e à rotina da organização.

Por fim, recomenda-se que mais estudos em Segurança da Informação com foco nos indivíduos sejam realizados, por se tratar de um assunto de capital importância no contexto da Sociedade da Informação na qual vivemos.

REFERÊNCIAS BIBLIOGRÁFICAS

Albrechtsen,E.& Hovden,J.(2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computer&Security,29(2010), 432-445.

ABNT NBR ISO/IEC 27002:2007 –Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação.

Albrechtsen, E. (2007). A qualitative study of user´s view on information security.Computer&Security,26, 276-289.

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 179–211.

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. British Journal of Social Psychology, 40, 471–499.

Bentler, P.M.& Speckart,G.(1981). Attitudes cause behaviors. A structural equation analysis. American Psychological Association,40(2),226-238.

Caminha,J.,Leal,R.T.,Marques,R.O.P.C.(2006) Implantação da Gestão da Segurança das Informações em um Instituto de Pesquisa Tecnológica. Fundação Centro de Análise, Pesquisa e Inovação Tecnológica (FUCAPI).

Cavalcante, S.M. (2003). Segurança da Informação no correio eletrônico baseada na ISO/IEC 17799:Um estudo de caso em uma instituição de ensino superior, com foco no treinamento. Dissertação de Mestrado, Departamento de Engenheiro, Universidade Federal do Rio Grande do Norte.

Dias, C. (2001) Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro, RJ: Axcel books.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

Furnell,S.&Thomson,K.L (2009). Recognising the varying user acceptance of IT security. Computer Fraud & Security,5-10.

Glassman, L.R.& Albarracín, D. (2006) Forming attitudes that predict behavior : A meta-analysis of attitude-behavior relation. Psychological Bulletin, 32 (5),778-822.

Gouveia, V., Veloso F.,et al.(2002)Atitudes frente à avaliação psicológica para condutores: perspectivas de técnicos, estudantes de psicologia e usuários. Psicol. cienc. prof. [online]., vol.22, n.2 , pp. 50-59 .

Hair,J.F.,Anderson,R.L.,Tatham,R.L.&Black,W.C.(2005).Análise Multivariada de dados (5a ed.).Porto Alegre:Bookman.

Hamblin, A.C.(1978). Avaliação e controle do treinamento. São Paulo:McGraw-Hill do Brasil.

Leach, J. (2003). Improving user security behaviour. Computer&Security,22(8), 685-692.

Lima, S. M. V., & Bressan, C. J. (2003). Mudança Organizacional: uma introdução, Em S. M. V, Lima (Org.) Mudança Organizacional. Teoria e Gestão (pp. 17-63). Rio de Janeiro: Editora FGV.

Lorens, E.L.(2007) Aspectos normativos da Segurança da informação: um modelo de cadeia de regulamentação. Dissertação de mestrado. Departamento de Ciência da Informação. Universidade de Brasília.

Neiva, E.R.,Paz,M.G.T.(2007) Percepção de mudança organizacional: um estudo em uma organização pública. Revista de administração contemporânea , 11(1),36-46.

Neiva, E.R., Mauro,T.G.S. (2011) Atitude e Mudança de Atitudes .Em: Psicologia Social. Principais temas e Vertentes. Artmed, Porto Alegre – RS, 171-203.

Neiva, E. R. (2004). Percepção da Mudança Organizacional: O papel das atitudes e das características organizacionais. Tese de Doutorado, Brasília: Universidade de Brasília.

Passos, J. L. (2005). Síndrome de Dédalo: Dilemas Éticos e Jurídicos doProfissional de Segurança da Informação. São Paulo: Instituto de Pesquisas Energéticas e nucleares.

Pasquali, L. (2005). Análise Fatorial para pesquisadores. Brasília – LabPAM.

Quintella, H.L.M.M, Mello,M.L.L.(2007). A qualidade percebida em sistema de segurança da informação. Revista Gestão da Produção, Operações e Sistemas.3(2),11-24.

Robbins,S.P.(2005) Valores, atitudes e satisfação com o trabalho. In:_____. Comportamento organizacional. Trad. Reynaldo Marcondes. 11. ed. São Paulo: Pearson Prentice Hall,. cap. 3.

Silva, M. H. L.,Costa, V.A.S.F.(2009). O fator humano como pilar da Segurança da Informação : Uma proposta alternativa [Artigo].Em: IX Jornada de Ensino Pesquisa e Extensão (JEPEX) da UFRPE. Recife-PE.

Silva, J.R.G & Vergara,S.C.(2002).Sentimentos, subjetividades e supostas resistências à mudança Organizacional. RAE, 43(3),1-12.

Siqueira, M.M.(2002). Medidas do comportamento organizacional. Estudos de Psicologia, 7, 11-18.

Smith, B., Caputi, P., Rawstorne, P. (2000) Differentiating computter, experience and atitudes toward computers: na empirical investigation. Computer in Human Behavior, 16 (1), 59-81.

Santos,S.R.(2001). Análise das atitudes de enfermeiros e estudantes de enfermagem na Paraíba-BR quanto à utilização de computador. Revista Latino-Americana de Enfermagem,9(6), 56-61.

Stanton,J.M.,Stam,K.R, Mastrangelo, P., Jolton, J.(2005) Analysis of end user security behaviors. Computer&Security,24, 124-133.

Thomson, M. & Solms,R.(1998). Information security awareness: educating your users effectively.Information Management & Computer Security,6,167-173.

Tabachnick,B.G. & Fidell,L.S. (2001).Using multivariate statistics.New York:Harper-Collins College Publishers.

Vroom,C.&Solms,R.(2004). Towards information security behavioural compliance. Computer&Security,23 ,191-198.

Vieira, P.S (2009).Cultura de Segurança da informação: Um processo de mudança organizacional na Petrobrás. Dissertação de Mestrado. EBAPE, FGV.

Whitman, E.M. & Mattord, J.H.(2011) Principles of Information Security. Boston: Course Technology Cengage Learning.

Wood Jr, T.(1992). Mudança organizacional: Uma abordagem preliminar. Revista de Administração de Empresas,32(3), 74-87.

Zafra, D., Pitcher, S.,Tressler, J.Ippolito, J.(1998) Information Technology Security Training Requirements: A role and Performance based model. Gaithersburg:NIST.

Zimbardo, P. G.,& Leippe, M. (1991). The psychology of attitude change and social influence (3rd ed.). New York: McGraw- Hill.

ANEXO I

Questionário

PESQUISA ACADÊMICA: SEGURANÇA DA INFORMAÇÃO

Participe desta pesquisa, apoiada pela X, que visa avaliar a sua percepção em relação às práticas de segurança da informação adotadas em sua organização. Este estudo faz parte da dissertação de mestrado sob a orientação da Profa. Dra. Elaine Neiva, do Departamento de Psicologia Social e do Trabalho da Universidade de Brasília (Unb).

OBSERVAÇÕES:

O tempo estimado de preenchimento é de 20 minutos.
Os campos com asterisco * são obrigatórios sendo os demais opcionais.
Os dados coletados são considerados sigilosos e estarão disponíveis apenas para o grupo de pesquisadores que farão a análise.
Dúvidas podem ser enviadas para o correio talitafas@uab.unb.br.

Obrigada por reservar um pouco de seu tempo para participar dessa pesquisa.
Sua participação é muito importante.

Talita Freire Arantes
Mestranda em Psicologia Social e do Trabalho (UNB)
Gestora de Tecnologia da Informação (UNB)

Práticas organizacionais de Segurança da Informação

Neste momento serão listadas várias práticas de segurança da informação que podem ser adotadas em sua organização. Por isso, para informar se as práticas listadas refletem ou não o que você percebe na sua organização, marque **apenas** um número de 0 (zero) a 10 (dez) ao lado de cada item, de acordo com a seguinte escala:

DISCORDO TOTALMENTE 1 2 3 4 5 6 7 8 9 10 CONCORDO TOTALMENTE

1

NA ORGANIZAÇÃO NA QUAL TRABALHO... *

Por favor, escolha a resposta adequada para cada item:

	1	2	3	4	5	6	7	8	9	10
Existe política ou diretrizes formais de segurança da informação na organização.	○	○	○	○	○	○	○	○	○	○
A política de segurança da informação é comunicada para todos os funcionários.	○	○	○	○	○	○	○	○	○	○
Existem regras de classificação da informação.	○	○	○	○	○	○	○	○	○	○

	1	2	3	4	5	6	7	8	9	10
Os funcionários conhecem as regras de classificação da informação.	○	○	○	○	○	○	○	○	○	○
Existem controles de acesso às informações importantes.	○	○	○	○	○	○	○	○	○	○
Existem contratos formais que determinam as responsabilidades dos funcionários pela segurança da informação.	○	○	○	○	○	○	○	○	○	○
Os funcionários são submetidos a acordos de confidencialidade na divulgação de informações.	○	○	○	○	○	○	○	○	○	○
Os funcionários são orientados a adotar práticas de segurança da informação.	○	○	○	○	○	○	○	○	○	○
Os funcionários recebem treinamento sobre as políticas e procedimentos organizacionais de segurança da informação.	○	○	○	○	○	○	○	○	○	○
Os prestadores de serviços recebem treinamento sobre as políticas e procedimentos organizacionais de segurança da informação.	○	○	○	○	○	○	○	○	○	○
Os funcionários recebem atualizações regulares sobre as políticas e procedimentos organizacionais de segurança da informação.	○	○	○	○	○	○	○	○	○	○
São adotadas regras para o uso de correio eletrônico.	○	○	○	○	○	○	○	○	○	○
São adotados	○	○	○	○	○	○	○	○	○	○

	1	2	3	4	5	6	7	8	9	10
procedimentos de autorização formal para a disponibilização pública das informações organizacionais.										
Os funcionários receberam um documento contendo claramente os controles de acesso aos sistemas de informação da organização.	○	○	○	○	○	○	○	○	○	○
É utilizado gerenciamento formal de criação e alteração de senhas para acesso aos sistemas de informação da organização.	○	○	○	○	○	○	○	○	○	○
São adotadas diretrizes para orientar usuários na escolha e manutenção segura de senhas.	○	○	○	○	○	○	○	○	○	○
Existe auditoria para avaliar práticas de segurança da informação.	○	○	○	○	○	○	○	○	○	○
São providos recursos para que os funcionários zelem pela segurança da informação.	○	○	○	○	○	○	○	○	○	○

ATITUDES FACE AS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Para a próxima etapa, indique o que você pensa e sente a respeito de práticas de segurança da informação adotadas em sua organização. Sua tarefa é indicar se você concorda ou não com as frases a seguir, marcando apenas um número de 0 (zero) a 10 (dez), de acordo com a seguinte escala:

DISCORDO TOTALMENTE 1 2 3 4 5 6 7 8 9 10 CONCORDO TOTALMENTE

2

AS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO...

*

Por favor, escolha a resposta adequada para cada item:

	1	2	3	4	5	6	7	8	9	10
Requerem muito do meu esforço mental.	○	○	○	○	○	○	○	○	○	○
São fáceis de ser utilizadas.	○	○	○	○	○	○	○	○	○	○
São extremamente importantes para o meu trabalho.	○	○	○	○	○	○	○	○	○	○
São do meu interesse.	○	○	○	○	○	○	○	○	○	○
Fazem me sentir confuso.	○	○	○	○	○	○	○	○	○	○
São de responsabilidade do pessoal da Tecnologia da Informação.	○	○	○	○	○	○	○	○	○	○
Criam mais problemas para os funcionários do que os auxiliam em seu dia-a-dia profissional.	○	○	○	○	○	○	○	○	○	○
Contribuem para que os funcionários desta organização exerçam suas atribuições com qualidade.	○	○	○	○	○	○	○	○	○	○
Geram dúvidas quanto a sua adoção.	○	○	○	○	○	○	○	○	○	○
Geram desconfiança entre os funcionários da organização	○	○	○	○	○	○	○	○	○	○
São cansativas.	○	○	○	○	○	○	○	○	○	○
São invasivas.	○	○	○	○	○	○	○	○	○	○
Restringem minha criatividade.	○	○	○	○	○	○	○	○	○	○
Geram tranquilidade.	○	○	○	○	○	○	○	○	○	○
Limitam minha atuação na organização.	○	○	○	○	○	○	○	○	○	○
Fazem com que eu me sinta vigiado.	○	○	○	○	○	○	○	○	○	○

MUDANÇAS ORGANIZACIONAIS DECORRENTES DA ADOÇÃO DE PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Pense na sua organização. Considere o período em que ela passou a adotar práticas de segurança da informação. Você acha que sua organização mudou nesse período? Para indicar se ela mudou e em que aspectos, responda às frases seguintes ; marcando apenas um número de 0(zero) a 10 (dez), de acordo com a seguinte escala:

DISCORDO TOTALMENTE 1 2 3 4 5 6 7 8 9 10 CONCORDO TOTALMENTE

3

A ADOÇÃO DE PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO CONTRIBUI PARA GERAR MUDANÇAS QUE... *

Por favor, escolha a resposta adequada para cada item:

	1	2	3	4	5	6	7	8	9	10
afetaram toda a organização.	○	○	○	○	○	○	○	○	○	○
afetaram apenas algumas áreas.	○	○	○	○	○	○	○	○	○	○
alteraram os procedimentos administrativos.	○	○	○	○	○	○	○	○	○	○
alteraram a forma de se trabalhar.	○	○	○	○	○	○	○	○	○	○
foram necessárias para a sobrevivência da organização.	○	○	○	○	○	○	○	○	○	○
foram acontecendo gradualmente.	○	○	○	○	○	○	○	○	○	○
geraram pequenos ajustes no funcionamento da organização.	○	○	○	○	○	○	○	○	○	○
foram superficiais.	○	○	○	○	○	○	○	○	○	○
aconteceram de forma repentina.	○	○	○	○	○	○	○	○	○	○
surgiram por iniciativa dos próprios empregados.	○	○	○	○	○	○	○	○	○	○
ocorreram lentamente.	○	○	○	○	○	○	○	○	○	○

	1	2	3	4	5	6	7	8	9	10
ocorreram porque era preciso mudar.	○	○	○	○	○	○	○	○	○	○
ocorreram mesmo sem a participação da Alta Direção.	○	○	○	○	○	○	○	○	○	○
afetaram a empresa de cima para baixo.	○	○	○	○	○	○	○	○	○	○
contribuíram para que hoje a organização seja outra.	○	○	○	○	○	○	○	○	○	○
ocorreram pouco a pouco.	○	○	○	○	○	○	○	○	○	○
foram planejadas e direcionadas para os objetivos da organização.	○	○	○	○	○	○	○	○	○	○
modificaram radicalmente o modo como as coisas eram feitas na organização.	○	○	○	○	○	○	○	○	○	○
fizeram com que as pessoas mudassem seus comportamentos.	○	○	○	○	○	○	○	○	○	○
aconteceram ao mesmo tempo em todos os setores da organização.	○	○	○	○	○	○	○	○	○	○
alteraram as orientações tradicionais da organização.	○	○	○	○	○	○	○	○	○	○
alteraram a cultura da organização.	○	○	○	○	○	○	○	○	○	○
estão sempre acontecendo nesta organização.	○	○	○	○	○	○	○	○	○	○
foram muito abrangentes.	○	○	○	○	○	○	○	○	○	○
alteraram o direcionamento da organização.	○	○	○	○	○	○	○	○	○	○
atingiram apenas certos	○	○	○	○	○	○	○	○	○	○

	1	2	3	4	5	6	7	8	9	10
grupos de empregados.										
estavam relacionadas à implantação de novas tecnologias.	○	○	○	○	○	○	○	○	○	○
alteraram a visão da organização.	○	○	○	○	○	○	○	○	○	○
ocorreram devido às necessidades do dia-a-dia.	○	○	○	○	○	○	○	○	○	○
já fazem parte do cotidiano da empresa.	○	○	○	○	○	○	○	○	○	○
modificaram os valores da organização.	○	○	○	○	○	○	○	○	○	○
modificaram pouco a dinâmica da organização.	○	○	○	○	○	○	○	○	○	○
ocorreram sem necessidade de planejamento.	○	○	○	○	○	○	○	○	○	○

COMPORTAMENTOS DE SEGURANÇA DA INFORMAÇÃO

A seguir estão listados alguns comportamentos de segurança da informação. Indique com que frequência você adota tais comportamentos, de acordo com a seguinte escala:

NUNCA 1 2 3 4 5 6 7 8 9 10 SEMPRE

4

NO MEU TRABALHO, EU...

*

Por favor, escolha a resposta adequada para cada item:

	1	2	3	4	5	6	7	8	9	10
Escolho senhas de acordo com as normas de segurança.	○	○	○	○	○	○	○	○	○	○
Altero minhas senhas em intervalos regulares.	○	○	○	○	○	○	○	○	○	○

	1	2	3	4	5	6	7	8	9	10
Utilizo uma senha diferente para cada serviço.	○	○	○	○	○	○	○	○	○	○
Utilizo um bom programa antivírus.	○	○	○	○	○	○	○	○	○	○
Configuro o antivírus para verificar os arquivos obtidos pela Internet, HDs externos e unidades removíveis.	○	○	○	○	○	○	○	○	○	○
Desabilito no meu e-mail a auto-execução de arquivos anexados às mensagens.	○	○	○	○	○	○	○	○	○	○
Caso seja necessário abrir arquivos, certifico-me que foram verificados pelo programa antivírus.	○	○	○	○	○	○	○	○	○	○
Utilizo na divulgação de documentos, formatos menos suscetíveis à propagação de vírus, tais como RTF ou PDF.	○	○	○	○	○	○	○	○	○	○
Mantenho o sistema operacional e demais softwares do meu computador sempre atualizados.	○	○	○	○	○	○	○	○	○	○
Em meu computador, possuo firewall pessoal.	○	○	○	○	○	○	○	○	○	○
Utilizo pelo menos uma ferramenta anti-spyware.	○	○	○	○	○	○	○	○	○	○
Faço o download de programas diretamente do site do fabricante.	○	○	○	○	○	○	○	○	○	○
Certifico-me da procedência do site ao realizar transações via Web.	○	○	○	○	○	○	○	○	○	○

	1	2	3	4	5	6	7	8	9	10
Estabeleço senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do meu computador.	○	○	○	○	○	○	○	○	○	○
Faço cópias dos dados do meu computador regularmente.	○	○	○	○	○	○	○	○	○	○
Armazeno as cópias dos dados do meu computador em local seguro.	○	○	○	○	○	○	○	○	○	○
Fico atento a e-mails ou telefonemas solicitando informações da organização.	○	○	○	○	○	○	○	○	○	○
Sempre que tenho dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entro em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.	○	○	○	○	○	○	○	○	○	○
Disponibilizo dados sensíveis da organização em blogs e sites de relacionamento.	○	○	○	○	○	○	○	○	○	○
Criptografo todos os dados sensíveis, principalmente se estiverem armazenados em notebook.	○	○	○	○	○	○	○	○	○	○
Faço logoff no meu computador ao deixar minha mesa do trabalho.	○	○	○	○	○	○	○	○	○	○
Mantenho sempre minha mesa limpa.	○	○	○	○	○	○	○	○	○	○
Descarto dados importantes de forma segura.	○	○	○	○	○	○	○	○	○	○

	1	2	3	4	5	6	7	8	9	10
Eventualmente, encaminho arquivos com conteúdo do trabalho para meu e-mail pessoal.	○	○	○	○	○	○	○	○	○	○
Acesso sites de lojas virtuais, internet banking, redes sociais, blogs, e outros, no computador do meu trabalho.	○	○	○	○	○	○	○	○	○	○
Utilizo computadores desconhecidos para acessar informações do meu trabalho.	○	○	○	○	○	○	○	○	○	○

Dados demográficos

SEXO

Favor escolher apenas uma das opções a seguir:

○ Feminino ○Masculino

IDADE

Favor escolher apenas uma das opções a seguir:

- ○18 a 25 anos
- ○26 a 35 anos
- ○36 a 45 anos
- ○46 a 55 anos
- ○56 anos ou mais

TEMPO DE EMPRESA

Favor escolher apenas uma das opções a seguir:

- ○Menos de 1 (um) ano
- ○1(um) a 5(cinco) anos
- ○6(seis) a 10(dez) anos
- ○11(onze) 20 (vinte) anos

- ○21 (vinte e um) a 30 (trinta) anos
- ○31(trinta e um) ou mais

ESCOLARIDADE

Favor escolher apenas uma das opções a seguir:

- ○Fundamental
- ○Médio
- ○Superior
- ○Especialização
- ○Mestrado
- ○Doutorado

TIPO DE FUNÇÃO

Favor escolher apenas uma das opções a seguir:

- ○Diretoria
- ○Assessoramento
- ○Área de negócio
- ○Área de desenvolvimento de sistemas
- ○Área de infra-estrutura tecnológica
- ○Área de gestão

REGIÃO

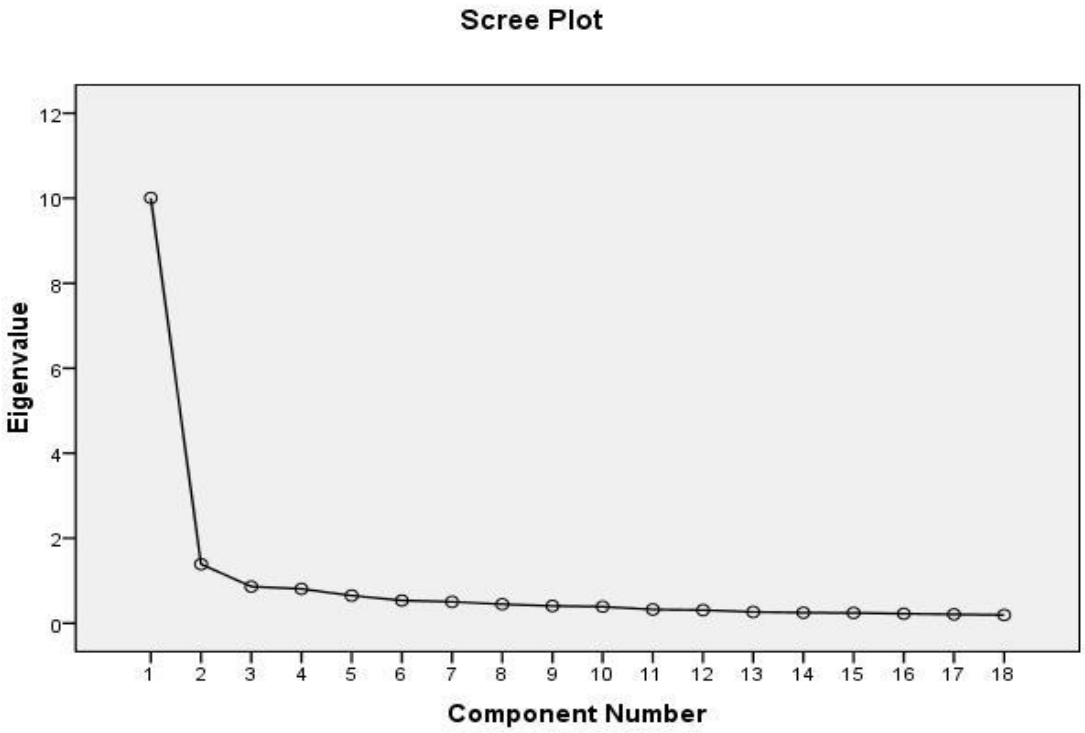
Favor escolher apenas uma das opções a seguir:

- ○Centro-Oeste
- ○Norte
- ○Nordeste
- ○Sul
- ○Sudeste

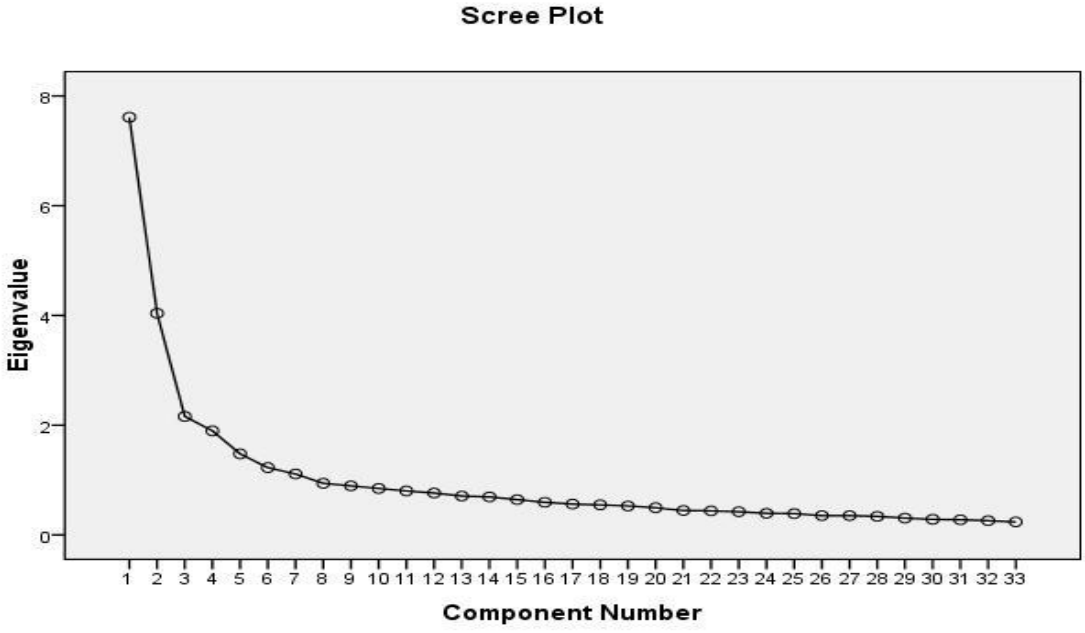
ANEXO II

Gráficos Scree Ploot

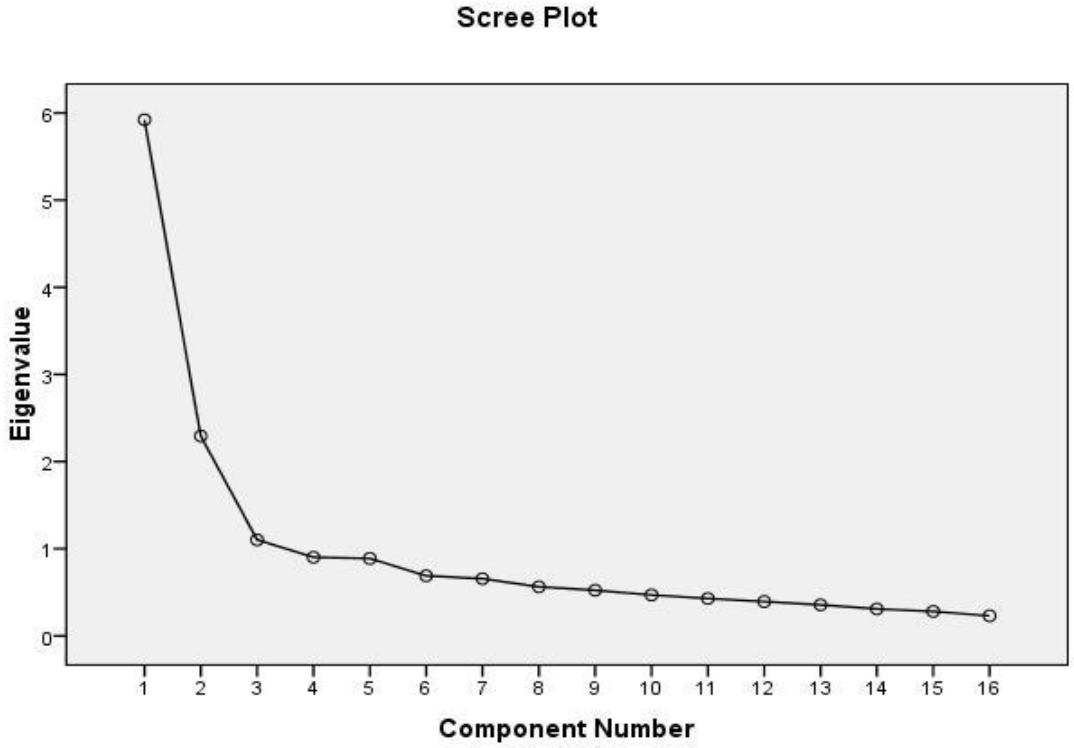
1. **Gráfico *Scree Plot* do Instrumento Práticas Organizacionais de segurança da Informação**



2. **Gráfico *Scree Plot* do Instrumento Percepção de Mudança Organizacional atribuída**



3. **Gráfico *Scree Plot* do Instrumento Atitudes frente às Práticas de Segurança da Informação**



4. Gráfico *Scree Plot* do Instrumento de Comportamento de Segurança da Informação