UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
INSTITUTO DE CIÊNCIAS ECONÔMICAS, ADMINISTRATIVAS E CONTÁBEIS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO – PPGA/FURG

CONFORMIDADE COM AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: A INFLUÊNCIA DA CULTURA DE SEGURANÇA DA INFORMAÇÃO E DO JEITINHO BRASILEIRO

Jonas Rafael Silveira

Rio Grande
2020

Jonas Rafael Silveira

CONFORMIDADE COM AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: A INFLUÊNCIA DA CULTURA DE SEGURANÇA DA INFORMAÇÃO E DO JEITINHO BRASILEIRO

Dissertação apresentada ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande, como requisito parcial à obtenção do título de Mestre em Administração.
Área de Concentração: Gestão Organizacional
Linha de Pesquisa: Tecnologias Gerenciais
Orientador: Prof. Dr. Guilherme Lerch Lunardi

Rio Grande, 2020

Por fim, permita que eu fale, não as minhas cicatrizes
Achar que essas mazelas me definem é o pior dos crimes
É dar o troféu pro nosso algoz e fazer nóis sumir.

(Oliveira)

DEDICATÓRIA

Dedico este trabalho a todos que acreditam no papel da ciência para a construção de uma sociedade mais justa.

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer à Universidade Federal do Rio Grande (FURG), pela oportunidade de estudar em uma universidade pública, gratuita e da qualidade, mas acima de tudo, uma universidade acolhedora, que educa além de conteúdos programáticos, transformando as pessoas para melhor.

Em segundo, agradeço a minha família, especialmente minha mãe Teresinha, mulher negra, batalhadora, que criou cinco filhos sozinha e sempre teve todo amor do mundo para dar. Uma heroína. E as minhas irmãs, que mesmo à distância, sempre me acompanharam nessa jornada.

Em terceiro lugar, ao Marcos, que foi a melhor pessoa que poderia ter ao meu lado durante o mestrado.

Agradeço também ao Prof. Dr. Lucas Cerqueira, que desde a graduação me apoiou, reconhecendo meus esforços e minha capacidade. Ao meu orientador Prof. Dr. Guilherme Lunardi, com quem aprendi muito desde a graduação, ao Prof. Décio Dolci, que me orientou durante a graduação e me ajudou a compreender diferentes aspectos da Tecnologia da Informação, sempre muito paciente. Aos demais professores, que contribuíram com o meu desenvolvimento dentro da academia, cada um ao seu modo e tempo, essa conquista também é de vocês.

Agradeço aos meus amigos, sempre presentes. E à Coordenação de Aperfeiçoamento do Ensino Superior (CAPES), pela oportunidade de ser bolsista demanda social, e permitir assim que pudesse concluir o mestrado.

RESUMO

Estudiosos do mundo inteiro buscam, através de suas pesquisas, compreender o que leva os indivíduos a cumprirem com as Políticas de Segurança da Informação (PSI) presentes nas organizações em que trabalham. Uma dessas correntes define que a cultura é um dos fatores que pode influenciar os funcionários a terem boas práticas relacionadas à segurança da informação. Entretanto, a maioria das pesquisas foca apenas em aspectos da cultura organizacional, desconsiderando outras culturas que formam o indivíduo, como a nacional. No Brasil, país conhecido por ter uma cultura própria e com características específicas, como o formalismo, a hierarquização e o pessoalismo, compreender a relação entre seus aspectos culturais e o cumprimento das PSIs pode trazer novos *insights* sobre a gestão da segurança da informação nas organizações brasileiras. Este estudo teve como objetivo analisar como os aspectos organizacionais relacionados à cultura de segurança da informação, em conjunto com o jeitinho brasileiro, influenciam na conformidade com as Políticas de Segurança da Informação presentes em diferentes organizações brasileiras. Para atingir esse objetivo, aplicou-se uma *survey* com 196 funcionários de diferentes organizações, cujos dados foram analisados através da modelagem de equações estruturais, baseada na técnica dos mínimos quadrados parciais. Os resultados indicam que o cumprimento das PSIs é influenciado positivamente pelo comportamento planejado dos indivíduos (seja pela atitude, normas subjetivas e controle percebido), sendo este precedido pela consciência de segurança da informação e pelo suporte organizacional de segurança da informação. O jeitinho brasileiro relacionado à segurança da informação influencia negativamente o cumprimento das PSIs, sendo necessário que as organizações construam uma cultura de segurança da informação forte e consistente para diminuir as falhas de segurança relacionadas ao jeitinho.

Palavras-chave: Segurança da Informação, Política de Segurança da Informação, Cultura, Cultura Organizacional, Cultura Nacional, Jeitinho Brasileiro.

ABSTRACT

Scholars from around the world seek through their research to understand what leads individuals to comply with those Information Security Policies (ISP) present in the organizations in which they work. One mainstream defines that culture is one of the factors that can influence employees to have good practices related to information security. However, most studies focus only on organizational culture aspects, disregarding other cultures that form the individual, such as the national one. In Brazil, a country known for having its own culture and specific characteristics such as formalism, hierarchy, and personalism, understanding the relationship between its national culture and the fulfillment of ISPs can bring new insights about information security management in Brazilian organizations. This study aimed to analyze how the organizational aspects related to the culture of information security, together with the "Brazilian little way", influence compliance with Information Security Policies in different Brazilian organizations. In order to achieve this goal, a survey was applied to 196 employees from different organizations, in which data was analyzed through structural equation modeling, based on the partial least squares technique. The results indicate that the compliance with ISPs is positively influenced by the person's planned behavior (either by the attitude, subjective norms, and perceived control), which is preceded by the information security awareness and organizational information security support.

The "Brazilian little way" related to information security negatively influences the compliance of the ISPs, making it necessary for organizations to build a strong and consistent information security culture to reduce security flaws related to it.

Keywords: Information Security, Information Security Policy, Culture, Organizational Culture, National Culture, The Brazilian Way.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O uso efetivo de Sistemas de Informação (SI) tem se mostrado essencial para o sucesso de qualquer organização, devido ao atual cenário de negócios ser altamente globalizado e orientado digitalmente (CRAM; D'ARCY; PROUDFOOT, 2019). Gestores utilizam a informação para apoiar sua tomada de decisão, de modo que as organizações onde atuam alcancem seus objetivos e melhorem seu desempenho, devendo tanto a informação quanto a Tecnologia da Informação (TI) ter proteção adequada (GALEGALE; FONTES; GALEGALE, 2017). Esse contexto tem exigido a realização de ações vinculadas a um cenário global, mesmo que as ações organizacionais estejam limitadas a um contexto local (MUZZIO, 2010). Assim, a globalização ressalta a necessidade de entender o gerenciamento das organizações que abrangem diferentes nações e culturas (STRAUB et al., 2002).

Nessa comunidade global, habilitada pela Internet e outras tecnologias digitais, os usuários de computador têm enfrentado níveis cada vez mais altos de riscos de segurança, especialmente porque em muitos casos não estão totalmente cientes das ameaças, além de suas organizações não apresentarem sistemas bem protegidos. Nesse sentido, várias quebras de segurança, de elevada proporção, têm sido relatadas ultimamente. Em maio de 2017, por exemplo, um ataque em escala global afetou mais de 200 empresas em 153 países, incluindo o Brasil. Um mês depois, o vírus Petya - ainda mais perigoso e sofisticado - impactou grandes empresas em diversos países, com perdas que chegaram a US$ 300 milhões para as companhias afetadas, segundo dados do relatório *The Global Risks Report* 2018 (MARTINS, 2017).

Complementarmente, em sua 20ª pesquisa global, realizada entre junho e setembro de 2017, com 1200 diretores e executivos da área de segurança da informação de todo o mundo, a consultoria Ernest & Young revelou alguns dados interessantes, destacando que somente 4% das organizações estavam confiantes de ter considerado totalmente as implicações de segurança da informação na estratégia atual; apontou, ainda, que entre 2013 e 2017, a vulnerabilidade que mais aumentou, segundo os pesquisados, são os empregados descuidados e sem conhecimento, passando de 53 para 60%, e para muitas organizações o ponto fraco mais óbvio virá de um empregado descuidado ou que não siga as diretrizes de segurança da informação.

Assim, tecnologias que protegem computadores e sistemas contra vírus, acessos não autorizados, interrupções, *spywares* e outras ameaças se tornaram importantes na sociedade

altamente interconectada (DINEV et al., 2009), considerando-se que medidas associadas à proteção tecnológica e à ocorrência de problemas de segurança da informação possuam uma relação negativa pelo fato de que uma sofisticação das medidas de proteção implementadas pelas organizações aumente a probabilidade de identificação dos potenciais problemas ligados a uma quebra de segurança (CORTEZ; KUBOTA, 2013). Mesmo assim, a proteção de redes de computadores, suas comunicações ou dados de trânsito não dependem mais da implementação única de controles técnicos sólidos, dependendo também de outros requisitos de segurança, como conformidade, legislação, cultura ou meio ambiente, pois a dimensão humana relacionada à Segurança da Informação não pode ser resolvida apenas por aspectos tecnológicos (NEL; DREVIN, 2019).

A segurança da informação se tornou um requisito essencial para fazer negócios, exigindo a presença de diferentes normativas, como as estabelecidas pela própria ISO27001 – que corresponde à norma internacional responsável pelo gerenciamento das Políticas de Segurança da Informação (PSI) (CRAM; D'ARCY; PROUDFOOT, 2019; ONWUBIKO; LENAGHAN, 2009). Por esses motivos, compreender como diferentes aspectos influenciam a conformidade dos usuários com as PSIs em suas organizações se torna um tema de pesquisa relevante. E como fatores organizacionais, alguns pesquisadores da área de SI apontam a cultura organizacional como um aspecto influenciador no comportamento do indivíduo relacionado à conformidade com as normas de Segurança da Informação, em relação à estrutura organizacional, seus colegas, chefias, e na própria relação com a tecnologia (THOMSON; VON SOLMS, 2006).

Assim, analisar como tais aspectos podem influenciar os indivíduos no seu comportamento relacionado à segurança da informação, considerando também aspectos da cultura brasileira, pode trazer resultados que sejam mais alinhados à realidade dos indivíduos nas organizações brasileiras ou organizações situadas no Brasil, pois esta é rica, influenciada pela sua colonização, independência e formação da república, sendo derivada de diferentes países com diferentes culturas (HOFSTEDE et al., 2010; MUZZIO, 2010), o que a diferencia de outros países. Portanto, desenvolver um estudo que busque analisar como alguns valores da cultura brasileira influenciam na conformidade com as normativas organizacionais que tratam da segurança de dados, torna-se um importante tema a ser pesquisado, pois à medida que a informação passa a ser cada vez mais relevante para as organizações, o perigo relacionado ao mau gerenciamento dessas informações também cresce.

A cultura brasileira, mais especificamente, tem sido pesquisada principalmente na área de Estudos Organizacionais, que destaca algumas das características presentes nas organizações brasileiras, como a hierarquização, o personalismo e o formalismo (CHU; WOOD, 2008). Além destes, o "jeitinho brasileiro" é considerado como uma das características mais comuns nas relações organizacionais presentes neste país (MUZZIO, 2010), tendo como principal característica o contorno de regras para se alcançar um objetivo. Mesmo que alguns pesquisadores o defendam pela criatividade desenvolvida para alcançar um objetivo organizacional (CHO; WOOD JR, 2008), utilizar o jeitinho também pode trazer problemas, como a violação de leis, o sentimento de desigualdade e até mesmo a corrupção (BARROSO, 2017). De qualquer maneira, no momento em que um funcionário se utiliza do jeitinho para alcançar algum objetivo, deixando de cumprir normativas, ele vai contra o que a organização determina oficialmente.

Assim, a partir do exposto acima, define-se como questão de pesquisa norteadora dessa dissertação a seguinte pergunta: *Como aspectos culturais organizacionais relacionados à segurança da informação, em conjunto com aspectos específicos da cultura organizacional brasileira, influenciam a conformidade dos funcionários com as Políticas de Segurança da Informação em organizações brasileiras?* A partir do problema de pesquisa identificado, pretende-se nesta dissertação de Mestrado analisar como os aspectos organizacionais relacionados à cultura de segurança da informação e a cultura organizacional brasileira influenciam na conformidade com as Políticas de Segurança da Informação em diferentes organizações brasileiras.

1.1 OBJETIVOS

Nesta seção são apresentados o objetivo geral e os objetivos específicos propostos nesta dissertação.

1.1.1 Objetivo Geral

Tem-se como objetivo geral neste trabalho analisar como os aspectos culturais organizacionais relacionados à segurança da informação no Brasil e a cultura organizacional brasileira influenciam na conformidade com as Políticas de Segurança da Informação por funcionários de diferentes organizações brasileiras.

1.1.2 Objetivos Específicos

Para atingir o objetivo geral proposto no trabalho, definem-se como objetivos específicos os seguintes:

(1) Adaptar e validar a escala de "Jeitinho Brasileiro" para a área de Segurança da Informação;
(2) Desenvolver um modelo causal que relacione os aspectos da cultura organizacional brasileira, como o jeitinho, relacionados à segurança da informação, à conformidade com as PSIs e à ocorrência de falhas de segurança; e
(3) Identificar diferentes características organizacionais e individuais associadas à conformidade com as PSIs.

1.2 JUSTIFICATIVA

O tema dessa pesquisa insere-se no campo da Administração e de Sistemas de Informação, mais especificamente na área de Gestão da Tecnologia da Informação e Segurança da Informação. A importância da elaboração e execução dessa pesquisa ocorre pela necessidade de compreender melhor o comportamento dos indivíduos quando o assunto é a conformidade com as PSIs presentes nas organizações.

De acordo com a pesquisa ISO de 2014, existiam 23.972 organizações certificadas no mundo com a ISO 27001. No Brasil, o número de organizações certificadas nesse período era apenas 86, com uma grande variedade em termos de setores e características (GALEGALE; FONTES; GALEGALE, 2017). Já de acordo com a "*survey* ISO 2018" (ISO, 2018), existiam 31.910 empresas certificadas no mundo com a ISO IEC 27001:2013, o que corresponde a um aumento de 33% no número de empresas certificadas, quando comparado à ISO *survey* de 2014. O Brasil passou a 110 empresas certificadas, sendo que dessas, 56 são empresas de Tecnologia da Informação, correspondendo a 61,4% do total, enquanto 44 correspondiam a empresas de outros setores. Já a China, que se tornou a nação com o maior número de certificações, possui 1.024 empresas de Tecnologia da Informação certificadas, sendo as demais 6.571 empresas, presentes em outros setores, o que corresponde a quase 90% das empresas chinesas certificadas. Esses números revelam a disparidade na proporcionalidade de certificações, pois no Brasil o foco para a certificação parece ser de empresas de TI, enquanto que na China, a certificação ocorre em empresas dos mais diversos setores da economia.

Essas diferenças demonstram a necessidade de se abordar a temática da Segurança da Informação no Brasil. Isso porque algumas pesquisas apontam que o Brasil se tornou um alvo para *hackers*, como a realizada pela consultoria Symantec, divulgada em seu Relatório de Ameaças à Segurança na Internet em 2017, estando o Brasil como um dos países que mais sofre com *spams*, ocupando a terceira posição, além de demonstrar uma nova modalidade de ataque: contra a cadeia de suprimentos das empresas (SYMANTEC, 2018). Recentemente, a Lei nº 13.709, de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet (BRASIL, 2018), torna as empresas responsáveis pelos dados de seus clientes, e prevê medidas caso problemas de Segurança da Informação ocorram e prejudiquem os cidadãos. Esse novo cenário, onde a Segurança da Informação passa a ter um papel de maior destaque entre as organizações brasileiras, leva à necessidade de estudos que possam auxiliar os gestores a tomarem decisões que auxiliem na proteção de suas informações e ativos de TI. No ambiente organizacional é necessário considerar não apenas os aspectos tecnológicos e técnicos, mas também os aspectos humanos. Marciano e Lima Marques (2006) já destacavam a importância de discussão aprofundada dos preceitos subjacentes às PSIs adotadas no Brasil – que em sua maioria, do lado estatal, são voltadas ao próprio aparato do Estado, e do lado corporativo, uma discussão adequada da realidade nacional ante o fenômeno da sociedade da informação e dos modelos que a sociedade brasileira pretendia adotar diante desta realidade. Além disso, os mesmos pesquisadores já destacavam que não se conhece qualquer solução meramente tecnológica para problemas sociais, sendo a segurança da informação necessitada de uma visão igualmente embasada em conceitos sociais, além dos tecnológicos, para sua correta cobertura (MARCIANO; LIMA-MARQUES, 2006).

Mesmo assim, as pesquisas relacionadas à Segurança da Informação no Brasil ainda são limitadas, existindo a necessidade de se aprofundar no tema a partir da utilização de teorias sociais (ALBUQUERQUE JUNIOR; SANTOS, 2014; 2013), como a Teoria Institucional, usada por Albuquerque Junior e Santos (2017). Alguns autores já vêm indicando a necessidade de um maior aprofundamento na relação entre as PSIs e a ação dos usuários nos estudos realizados no Brasil (FERREIRA; DOLCI; TONDOLO, 2016), e a necessidade de trabalhos que busquem comprovações estatísticas, relacionadas ao tema Segurança da Informação, também considerados escassos no país (GALEGALE; FONTES; GALEGALE, 2017). Quando se considera os aspectos culturais nacionais nos estudos sobre segurança da informação no Brasil, a necessidade de aprofundamento é ainda maior, já que não existem

estudos nacionais que façam essa relação. Cram, D'arcy e Proudfoot (2019) recomendam que estudos sobre PSIs que considerem aspectos culturais podem trazer melhores explicações se considerarem as culturas nacionais específicas, como por exemplo, a cultura organizacional brasileira.

Nesse sentido, espera-se com este trabalho auxiliar a comunidade científica, gestores de TI e de organizações, a compreender como diferentes aspectos constituintes da cultura do indivíduo, como a cultura organizacional e nacional (GALLIVAN; SRITE, 2005), influenciam a conformidade com as PSIs, auxiliando no enfrentamento das ameaças e na diminuição das vulnerabilidades de Segurança da Informação presentes nas organizações.

1.3 ORGANIZAÇÃO DA DISSERTAÇÃO

Esta dissertação está organizada em seis capítulos. O primeiro contextualiza o estudo realizado, definindo ainda a sua questão de pesquisa, seus objetivos e a justificativa para a sua realização. O segundo capítulo aborda a revisão da literatura sobre o tema investigado. O terceiro capítulo destina-se ao desenvolvimento do modelo de pesquisa proposto neste estudo, destacando-se diferentes processos identificados na literatura como potenciais influenciadores da conformidade com as PSIs. O quarto capítulo apresenta a metodologia utilizada no estudo, cabendo ao quinto a apresentação dos resultados obtidos; enquanto no sexto, e último capítulo, apresentam-se as considerações finais.

A seguir, expõe-se o referencial teórico que dá suporte ao desenvolvimento da presente pesquisa.

2 REFERENCIAL TEÓRICO

Este capítulo dedica-se ao desenvolvimento do referencial teórico utilizado como base para a construção desta dissertação. Primeiramente, expõem-se conceitos sobre Cultura Organizacional, para em seguida definirem-se os conceitos relacionados à Cultura Organizacional Brasileira, com ênfase no aspecto do "jeitinho brasileiro". Mais a frente, apresentam-se os conceitos relacionados à Cultura na área de TI e, mais especificamente, à Cultura de Segurança da Informação, para logo após abordar os conceitos e práticas relacionadas às Políticas de Segurança da Informação utilizadas pelas organizações, publicadas internacionalmente e no Brasil. Por fim, destaca-se a Teoria do Comportamento Planejado, a qual é utilizada como teoria de base neste estudo, e sua aplicação nos estudos sobre a conformidade com as Políticas de Segurança da Informação.

2.1 CULTURA ORGANIZACIONAL

A discussão em torno da cultura organizacional segue uma base de conceitos fornecida pela Antropologia Cultural, em que existem diversas correntes teóricas, que privilegiam aspectos diferentes de um mesmo fenômeno (MUZZIO, 2010; FREITAS, 1991), sendo, portanto, o conceito de "Cultura" considerado espinhoso. Além da Antropologia, a cultura também é estudada na área da Psicologia, avançando até a gestão de negócios transcultural. Muitos pesquisadores têm usado mais de uma definição de cultura, dependendo da época em que sua definição havia sido formulada e do assunto a que se referia (STRAUB et al., 2002).

Na área de Estudos Organizacionais, o tema Cultura foi desenvolvido a partir da década de 1970, com a denominação de cultura organizacional ou cultura corporativa. A partir desse momento, houve uma proliferação de trabalhos com distintas abordagens teóricas e metodológicas, gerando múltiplos conceitos que, em algumas situações, complementavam-se e, em outras, excluíam-se mutuamente (BARALE; SANTOS, 2017). A grande variedade de estudiosos que trabalha nessa área produziu numerosas definições de cultura, que vão do simples ao complexo, incorporam e estendem as definições anteriores e até mesmo as contradizem (BARALE; SANTOS, 2017; LEIDNER; KAYWORTH, 2006; STRAUB et al., 2002).

Freitas (1991) coloca que uma das argumentações mais encontradas para o interesse de estudar a cultura na área de Administração relaciona-se ao declínio da produtividade norte-

americana e ao ganho de competitividade dos japoneses. Por muitos anos, várias organizações contrataram serviços de consultoria para aplicar as técnicas responsáveis pelo sucesso japonês. Esse tipo de transposição levava em consideração as principais diferenças entre a sociedade japonesa e a ocidental, onde o Japão aparecia como mais homogêneo, com visão holística e ênfase no coletivo. Ao mesmo tempo, a autora destaca que outra motivação para o crescimento pelo interesse na área deve-se ao fato de que a cultura organizacional surgiu como um contra-ataque aos problemas de desintegração da sociedade, como uma solução atraente, enfatizando ideias comuns, formas de pensar, valores, padrões e maneiras de trabalhar, fornecendo a resposta a essas tendências de desagregação social pela quebra dos padrões culturais, reproduzindo uma ordem particular, via consenso e solidariedade entre os membros da organização.

Quanto às diferentes abordagens relacionadas à cultura, Straub et al. (2002) dividem as suas definições em três grupos, sendo o primeiro representado pela visão mais comum sobre cultura, que é acerca das Definições Baseadas em Valores Compartilhados. Em resumo, essa categorização sugere que esta consiste em formas padronizadas de pensar que são compartilhadas entre as pessoas de uma sociedade; e esses padrões são baseados em valores que influenciam as cognições, atitudes e comportamentos dos indivíduos. Além disso, há uma distinção entre valores centrais e periféricos. A cultura é principalmente uma manifestação de valores fundamentais.

Já a segunda abordagem, representada pelas Definições Baseadas na Resolução de Problemas, coloca que em vez de tentar definir a cultura na perspectiva de sua composição (como na abordagem anterior), esta analisa os resultados da cultura e o que ela pode realizar. Straub et al. (2002) enfocam nessa abordagem a solução de problemas e como isso define um grupo específico de pessoas. Por fim, o terceiro grupo é formado por definições generalizadas e distinções abrangentes, que tendem a ser mais abstratas e, em alguns casos, esotéricas ou espirituais.

Como um dos principais autores da cultura por definição de valores, Hofstede (1980a) traz em seu trabalho a importância das diferenças entre as culturas nacionais na constituição das organizações e, principalmente, dos próprios estudos organizacionais. Mas antes, para falar de cultura organizacional, o autor propõe suas definições para a formação da cultura. Para Hofstede (1980a, p. 24), cultura pode ser definida como “a programação coletiva da mente humana que distingue os membros de um grupo humano dos de outro. A cultura, nesse sentido, é um sistema de valores coletivamente mantido”. Essa cultura possui subculturas,

sendo que o grau de integração cultural varia de uma sociedade para outra e pode ser especialmente baixo para algumas das nações mais novas.

A maioria das subculturas dentro de uma nação, no entanto, ainda compartilha traços comuns que tornam seus membros reconhecíveis pelos estrangeiros como pertencentes à sua sociedade. No centro está um sistema de normas sociais, consistindo dos sistemas de valores compartilhados pela maioria da população. Essas normas sociais levaram ao desenvolvimento e manutenção de padrões de instituições sociais com uma estrutura e modo de funcionamento particular, que incluem família, sistemas educacionais, política e legislação. As instituições, uma vez que se tornaram fatos, reforçam as normas sociais e as condições ecológicas que reforçam esses padrões institucionais. As instituições podem ser alteradas, mas isso não afeta necessariamente as normas sociais. Quando essas normas permanecem inalteradas, a influência persistente de um sistema de valores majoritário molda pacientemente as novas instituições, até que sua estrutura e funcionamento sejam novamente adaptados às normas da sociedade. Hofstede (1980a) acredita que as normas mudam raramente pela adoção direta de valores externos, mas sim por uma mudança nas condições ecológicas: tecnológica, econômica e higiênica. Em geral, as mudanças nas normas serão graduais, a menos que as influências externas sejam particularmente violentas.

Em seu trabalho mais conhecido, em que propôs um grande banco de dados de pesquisas sobre valores e sentimentos, relacionados de populações equiparadas de funcionários da corporação IBM em mais de 50 países ao redor do mundo, com 116.000 funcionários, Hofstede identificou empiricamente quatro “dimensões das culturas nacionais”: *Distância de Poder*, *Evitação de Incerteza*, *Individualismo versus Coletivismo* e *Masculinidade versus Feminilidade* (HOFSTEDE, 1980b). Em um estágio posterior, uma quinta dimensão foi adicionada: *Longo Prazo versus Orientação de Curto Prazo*. Cada país poderia receber uma pontuação em cada dimensão, posicionando-a em relação a outros países. As pontuações dos países foram extensivamente validadas contra dados externos conceitualmente relacionados de muitas fontes diferentes (HOFSTEDE et al., 2010).

Um problema identificado em seu estudo foi que ele foi conduzido em muitos países, mas apenas com funcionários da IBM, refletindo as idiossincrasias dessa empresa. O trabalho de Hofstede também se baseia no pressuposto de que os funcionários contratados pela IBM são representantes das culturas de onde eles vêm - uma suposição duvidosa. É possível que os funcionários que foram selecionados e socializados pela IBM para seu modo de fazer negócios difiram de algum modo de seus pares. Apesar dessas críticas, o impacto de Hofstede

para a pesquisa em Administração tem sido substancial, e suas dimensões culturais formam a espinha dorsal conceitual de muitas pesquisas interculturais e de SI (GALLIVAN; SRITE, 2005).

Outro autor que é referência quando o assunto é Cultura Organizacional é Schein, que traz a importância da aprendizagem através da solução de problemas para a cultura organizacional. Em seu trabalho destacado aqui, Schein (1984, p. 3), na busca de uma definição operacional, tanto para acadêmicos como para organizações, definiu Cultura Organizacional como:

> "a estrutura de pressupostos fundamentais estabelecida, descoberta ou desenvolvida por dado grupo no processo de aprendizagem de solução de problemas de adaptação externa e integração interna que, tendo funcionado suficientemente bem para ser admitida como válida, deve, portanto, ser ensinada aos novos membros do grupo como a maneira correta de perceber, pensar e sentir aqueles problemas."

A necessidade de melhor compreensão dos aspectos relacionados à cultura levou a criação de uma estrutura com diferentes níveis para essa análise. O início seria os artefatos visíveis, compostos pela organização construída, sua tecnologia, os padrões visíveis e audíveis de comportamento, as vestimentas dos funcionários, documentos de conhecimento geral, manuais de orientação; enfim, tudo que aparentemente pode ser analisado e perceptível. Esse nível de análise é colocado como traiçoeiro, porque os dados são fáceis de obter, mas de difícil interpretação. Pode-se descrever "como" um grupo estrutura seu ambiente e "quais" os padrões de comportamento são discerníveis entre os membros, mas com frequência não se pode entender a lógica subjacente, ou seja, aquilo que está por trás.

Além dos artefatos, Schein (1984) destaca que para analisar por que os membros das organizações se comportam de tal modo, deve-se buscar os valores que regem esses comportamentos - em seu modelo, constituindo o segundo nível. O autor coloca que ao identificar esses valores, percebe-se que eles representam com boa precisão os valores esposados de uma cultura, concentrando-se no que as pessoas *dizem ser* a razão para seus comportamentos, a razão idealizada, sendo geralmente sua racionalização para o comportamento, deixando as verdadeiras razões ocultas ou inconscientes.

Por isso, para o autor, o entendimento de uma organização só é possível quando se vai mais a fundo, e se encaram os pressupostos fundamentais, que tipicamente são inconscientes, mas determinam o modo como os membros do grupo percebem, pensam e sentem. Os pressupostos são respostas aprendidas que tiveram seu início como valores esposados. Um determinado valor pode levar a um comportamento e, dependendo do resultado desse comportamento baseado em um ou mais valores, esse se transforma gradualmente em uma

preposição subjacente que explica como as coisas são, para que, na medida em que essa pressuposição se torna inquestionável dentro da organização, ela desaparece da percepção consciente, possuindo esse poder, pois não são submetidos a confrontos e combates com os valores esposados. Para Schein (1984), um pesquisador se depararia com um pressuposto quando ao tentar se discutir algum assunto, encontra resistência, ou os membros organizacionais consideram até mesmo ignorância a busca pelo entendimento dessas questões.

Esses pressupostos, de acordo com o autor, tornam-se inconscientes pela repetição bem-sucedida de processos cognitivos e emocionais. Estes são difíceis de serem quebrados, pois estão na formação dos grupos dentro das organizações, estruturados em paradigmas culturais, os quais estão bem estruturados, interpenetrados com um padrão coerente. Nesse sentido, os pressupostos fundamentais subjacentes à cultura de origem dos fundadores da organização determinarão em larga medida as formulações iniciais da missão central da organização, dos objetivos, meios, critérios e estratégias de ocasião, no sentido de que essas maneiras de fazer as coisas serão as únicas com as quais os membros do grupo estarão familiarizados. Mas na medida em que a organização desenvolve sua própria experiência de vida poderá começar a modificar os pressupostos originais.

O autor coloca que se os seres humanos têm de fato necessidade cognitiva de ordem e consistência, deve-se então admitir a tese de que todos os grupos, mais cedo ou mais tarde, terminarão por estabelecer conjuntos de pressupostos que sejam compatíveis e consistentes. A transmissão de conhecimento dos membros mais antigos para os mais novos é essencial para a definição da cultura de um grupo. Quando esse conhecimento é passado sem a percepção de que esteja ocorrendo, devido ao sucesso obtido na solução de problemas, pode-se supor que esse grupo já possua uma vivência compartilhada para ter desenvolvido uma cultura. Ao falar da robustez da cultura, Schein (1984) coloca que um grupo, para ter uma cultura forte e estabilizada, deve ter uma história longa, variada e intensa com a resolução de problemas e ser bem-sucedido. Do contrário, se um grupo teve constantes mudanças no seu quadro de membros ou que esteja reunido por tempo curto e que ainda não enfrentou qualquer dificuldade séria, será por definição portadora de uma cultura fraca, mesmo que seus membros possuam certa experiência, pois essa não se refletirá em experiências compartilhadas com o grupo.

O conteúdo da cultura e o grau com que suas soluções atendem aos problemas levantados pelo ambiente aparecem como as variáveis determinantes. Esse modo de definir cultura faz com que ela seja específica para dado grupo. Se a totalidade de uma organização

consiste de subgrupos estáveis em termos funcionais, divisionais, geográficos ou hierárquicos, então a organização terá múltiplas culturas dentro de si. A cultura total pode, então, ser muito homogênea ou heterogênea, dependendo do grau de semelhança ou de diferença das culturas dos subgrupos.

Schein (1984) coloca que os elementos culturais são definidos como soluções aprendidas de problemas, existindo dois tipos: (1) situações positivas de solução de problemas, que produzem reforço positivo ou negativo, conforme a solução tentada funciona ou não; e (2) situações de evasão de angústia, que produzem reforço positivo ou negativo conforme a solução tentada contribui ou não para se livrar de alguma angústia, sendo que para a cultura desempenhar sua função, ela deve ser percebida como correta e válida e, sendo percebida desse modo, transmitida aos novos membros da organização. O autor deixa claro que o desenvolvimento da cultura não significa que a organização terá o controle das maneiras de ser, pensar e agir dos seus empregados. À medida que o aprendizado cultural progride, mais e mais respostas das pessoas estarão envolvidas. Então, a imersão do indivíduo na cultura, de acordo com sua intensidade, influenciará os modos de pensar, ser e agir desse indivíduo.

Deste modo, entende-se que a cultura organizacional é um conceito essencial à construção das estruturas organizacionais. Percebe-se, então, que a cultura de uma sociedade ou organização será um conjunto de características que a distingue em relação a qualquer outra. Ela adota o papel de legitimadora do sistema de valores, que assim produzem normas de comportamento genericamente aceitas por todos (EGITO; MONTEIRO, 2018).

Essas diferentes definições de cultura e cultura organizacional influenciaram os estudos na área de SI, devendo ser levados em conta quando se utilizam os aspectos culturais em estudos na área (STRAUB et al., 20012; GALLIVAN; SRITE, 2005). Mas ao se estudar como os aspectos culturais se relacionam com os aspectos organizacionais, é necessário ainda trazer estudos e conceitos que abordem a visão da cultura organizacional específica das organizações brasileiras, tema dessa pesquisa, e que será abordada a seguir.

2.2 CULTURA ORGANIZACIONAL BRASILEIRA

Os estudos sobre a influência da cultura nacional na cultura organizacional foram impulsionados a partir dos anos 1980, pelo fato da repercussão dos resultados da pesquisa de Hofstede dos anos 1970, na qual o pesquisador analisou a dimensão da cultura associada à

gestão de empresas em diversos países, inclusive no Brasil (MOREIRA; ROCHA, 2018). Assim, quando se fala de cultura organizacional em geral, precisa-se compreender que o desenvolvimento de estudos sobre a cultura organizacional brasileira possui diferentes correntes.

De acordo com Muzzio (2010), duas correntes prevalecem. A primeira é a histórico-evolucionista. Inspirado no positivismo de Comte, no darwinismo social e no evolucionismo de Spencer, procurou encontrar um nexo entre as diversas sociedades humanas, baseando-se no fato de que as sociedades evoluíam do simples para o complexo, através do estabelecimento de leis do progresso, e através da relação com a raça e ambiente. A segunda trabalha com uma perspectiva dialética, a partir do levantamento de um perfil da cultura brasileira, que valoriza as condições únicas que marcam os valores do país. É uma análise posterior à primeira, que possibilita uma leitura mais adequada às nuances de um contexto de intensas transformações.

No Brasil, a primeira corrente analisa a cultura nacional sob uma ótica linear, temporal e racial, marcada por traços culturais originados nas raças formadoras do país ou na convergência dessas ao longo do tempo, que acabam por definir o "ser brasileiro". A segunda foca nos aspectos simbólicos das relações sociais, estudando suas dramatizações com ênfase nas particularidades da sociedade brasileira, ou seja, o que diferencia a sociedade brasileira das outras sociedades (MUZIO, 2010). A definição desses traços culturais precisa ser cuidadosa no sentido de não querer mostrar uma face única dos brasileiros, mas sim, perceber que alguns elementos ajudam a formar uma identidade nacional e explicam determinados comportamentos nas organizações, além da criação de regras formais e informais que influenciam as ações e as relações organizacionais (BUENO; ARANTES, 2015).

De qualquer forma, a cultura brasileira resulta do processo histórico de conquista, colonização e escravidão no país. Após os portugueses, o primeiro grupo étnico que colocou uma forte marca na cultura brasileira foi o indígena. Logo após, o período da escravidão marcou a presença dos negros trazidos da África como mão de obra. Eles acrescentaram muitas características importantes de suas culturas, como sua musicalidade e o sincretismo religioso no Brasil atual, que está profundamente enraizado nas tradições africanas. Finalmente, uma terceira onda veio da grande variedade de imigrantes trazidos e convidados da Europa (alemães, italianos, espanhóis) e da Ásia (japoneses, libaneses e sírios) que, a partir da segunda metade do século XIX, substituíram os escravos, tornando ainda mais complexas

as relações interculturais, o que influenciou a constituição da sociedade brasileira atual (HOFSTEDE et al., 2010; MOREIRA; ROCHA, 2018).

De uma forma geral, os traços relacionados à cultura nacional brasileira que mais aparecem na literatura de estudos organizacionais são:

- A Desigualdade de poder e hierarquia: em que a desigualdade de poder enraizada na cultura brasileira e na cultura organizacional brasileira advém muito do sistema hierárquico que vigorou nas relações entre senhor e escravo no Brasil colonial, e que marcou profundamente a sociedade (CHU; WOOD JR., 2008). Possui uma tendência à centralização do poder em grupos sociais com alto grau de distanciamento entre os níveis e passividade e aceitação dos grupos inferiores (BUENO; ARANTES, 2015). As organizações brasileiras geralmente possuem uma distância de poder tão grande que parecem lembrar a própria distribuição de renda no país e seu passado escravocrata (PRESTES, 1997);
- A Flexibilidade: que se traduz na capacidade de ajustes a situações diversas e à capacidade de inovação (CHU; WOOD JR., 2008), causada por uma ética de duas pontas que opera simultaneamente e que leva a comportamentos diferentes. Os brasileiros estão constantemente negociando entre dois códigos diferentes, o que exige flexibilidade (BARTEL-RADIC, 2013);
- A Plasticidade: manifestada pela assimilação fácil de práticas e costumes estrangeiros, e que revela a propensão a mirar modelos e conceitos desenvolvidos em outros contextos de gestão, em detrimento daqueles desenvolvidos localmente. Apesar da continuidade no uso de padrões internacionais de gestão, já se notava o desenvolvimento de um senso crítico e uma atenção à valorização de práticas locais (CHU; WOOD JR., 2008);
- O Personalismo: expressa a importância atribuída às pessoas e aos interesses pessoais, grupo ou comunidade. Indica o alto grau de confiança depositado na rede de amigos e familiares para resolução de problemas ou obtenção de privilégios (CHU; WOOD JR., 2008), como solicitar um favor, pedir a alguém para “quebrar um galho”, ou propor um jeitinho. Ou seja, são diferentes maneiras de expressar a pessoalidade em oposição à impessoalidade da relação Estado-indivíduo, característica da implantação do Estado Brasileiro nos moldes norte-americanos e europeus (BARLACH, 2015). A ideia de que, no Brasil, ninguém quer ser como os outros e que as relações sociais e organizacionais são reguladas não só pelo poder, mas também por relações pessoais profundas que transcendem elos organizacionais, busca aproximação e afeto nas relações (FREITAS, 1997);

- O Formalismo: que é uma escola de pensamento em lei e jurisprudência, a qual assume que a lei é um sistema de regras que pode determinar o desfecho de qualquer caso, sem referenciar-se às normas externas (EGITO; MONTEIRO, 2018). Considerado por alguns autores como a raiz do jeitinho (BERNARDO; SHIMADA; ICHIKAWA, 2015), este se traduz nas organizações por meio de comportamentos que buscam, por um lado a redução do risco, da ambiguidade e da incerteza e, por outro, o aumento da previsibilidade e do controle sobre as ações e comportamentos humanos. Essa busca se dá por meio da criação de grande quantidade de regras, normas e procedimentos que visam garantir segurança, ou seja, esse traço está presente no apego a leis e regras e pode provocar discrepâncias entre o que é escrito e o que é realizado, ou entre o que é dito e o que é de fato feito (CHU; WOOD, 2008).

Como traços esféricos da cultura organizacional brasileira, baseado em Hofstede (1980b), Chu e Wood Jr. (2008) destacam que a gestão no Brasil é levemente mais orientada a valores femininos, como o cuidado com o próximo, igualdade, bem-estar e qualidade de vida, do que masculinos, como agressividade, assertividade, resultados, performance, entre outros. Além disso, a orientação para a ação e o planejamento organizacional é reduzida, o tempo é gerido com ineficiência e a orientação predominante é para o curto prazo. De acordo com os autores, da grande distância de poder entre as pessoas derivam os traços do autoritarismo, do desconforto diante de conflitos abertos e a postura de espectador. Em seu trabalho, os autores colocam que a cultura organizacional brasileira possuía um quadro híbrido, típico de transição, no qual se percebem traços da cultura organizacional mais tradicional em conjunto com traços pós-globalização (CHU; WOOD Jr., 2008).

Atualmente, Hofstede (2019) disponibiliza em seu site *insights* sobre as culturas de diferentes países, incluindo a classificação do Brasil em suas atuais seis dimensões, as quais são pontuadas de 0 a 100. De acordo com esse modelo, o Brasil reflete uma sociedade que acredita que a hierarquia deve ser respeitada e as desigualdades entre as pessoas são aceitáveis (escore igual a 69). Também se coloca que é uma cultura coletivista, na qual nos negócios é importante construir relacionamentos confiáveis e duradouros: uma reunião geralmente começa com conversas gerais para se conhecer antes de fazer negócios, com um escore de 38. Referente à feminilidade x masculinidade, o Brasil aparece em uma posição intermediária (49). Já quanto à Evitação de Incertezas, possui um escore de 69, considerado alto, em que a burocracia, as leis e as regras são muito importantes para tornar o mundo um lugar mais seguro para se viver. Na orientação a longo prazo, possui uma pontuação intermediária (44), e sobre a Indulgência, que se refere à medida em que as pessoas tentam controlar seus desejos e

impulsos, com base na maneira como foram criadas, o Brasil possui uma pontuação de 59, o que de acordo com o modelo de Hofstede significa que os brasileiros possuem uma atitude positiva e têm uma tendência ao otimismo. Além disso, eles dão um alto grau de importância ao lazer, agem como bem entendem e gastam dinheiro como desejam (HOFSTEDE, 2019).

De todos os aspectos reconhecidos na literatura que tratam da cultura brasileira, talvez o "jeitinho brasileiro" seja o mais conhecido e controverso, possuindo as mais variadas facetas (PRESTES, 1997), sendo este discutido a seguir.

2.2.1 O "Jeitinho Brasileiro"

Como aspecto característico da cultura brasileira, é comum que o jeitinho permeie a cultura das organizações e instituições, sejam elas de caráter público ou privado (EGITO; MONTEIRO, 2018). O jeitinho constitui a identidade do brasileiro, configurando tanto como quanto ele se vê e como é visto por outros povos de outras sociedades (MOREIRA; ROCHA, 2018).

Entre os estudiosos existem correntes que se colocam de forma a condenar ou defender, conforme o contexto em que esse jeitinho ocorre. Pode ser visto como uma solução para aquilo que não tem solução, não sendo as leis, normas e a própria constituição nacional barreiras definitivas e irrevogáveis para o comportamento (BARLACH, 2015). Possui como característica a desconexão entre o que foi prescrito como correto e o que realmente ocorre no cotidiano das instituições e da sociedade de maneira geral, sendo maneira peculiar de resolver problemas, situações difíceis ou proibidas (BERNARDO; SHIMADA; ICHIKAWA, 2015).

Para Prestes (1997), o jeitinho é uma prática cordial que implica personalizar relações por meio de coisas em comum, como um time de futebol, por exemplo, sendo diferente da arrogância em apelar para um *status quo* mais alto. E diferente também da malandragem, mesmo estando próximo, pois não se caracteriza por "passar alguém pra trás". Islam (2012) coloca que o "jeitinho brasileiro", em sua concepção, é essencialmente o uso de laços personalistas para ultrapassar temporariamente as regras formais, passando notas promissórias quando está sem dinheiro ou indo para frente da fila por causa de conexões pessoais, sendo a ordem administrativa temporariamente invertida para consolidar a ordem pessoal. É uma estratégia para suavizar as formas impessoais que regem as relações pessoais.

O jeitinho é ambíguo e admite dupla leitura, pode significar uma postura conformista de convivência com o *status quo* injusto e inaceitável; e pode ser visto como uma forma de

sobreviver ao cotidiano, um recurso de resistência cultural, comportamento que visa à harmonização das regras e determinações universais da vida com as necessidades diárias do cidadão, buscando a realização de objetivos a despeito de determinações legais contrárias (CHU; WOOD JR., 2008). Uma vez que os brasileiros não veem muito sentido em certas regras, diferenciam-nas em dois grupos, as que devem ser seguidas e as que se pode contornar, utilizando-se principalmente das relações pessoais e de status (BUENO; ARANTES, 2015).

Mansur e Sobral (2011) enfatizam o poder político do jeitinho nas relações entre os indivíduos organizacionais. A postura de espectador, baixa consciência crítica e permissividade fazem com que o brasileiro aceite o jeitinho, moderando, assim, os efeitos da percepção de política dentro das organizações brasileiras, considerando-o como um instrumento de poder ou habilidade não restrita a líderes da organização, sendo percebido por todos. Para Egito e Monteiro (2018), ao problematizarem o conceito do jeitinho em relação ao contexto da Administração Pública, este não deveria nem ser usado, pois não soluciona a causa do problema que busca contornar. No caso, o formalismo não melhora os processos e funciona somente como um paliativo. Para mais adiante disso, o uso do jeitinho demonstra uma postura antagônica aos princípios da Administração Pública, a qual poderia ser configurada como corrupção, e se caracteriza pelo individualismo.

Para Hofstede et al. (2010), relacionando o jeitinho brasileiro com os aspectos culturais de suas pesquisas a partir dos resultados de suas análises, o mesmo se relaciona com aqueles processos na sociedade que, do ponto de vista ético, devem ser governados pelo nível de Evitação de Incertezas. As histórias do jeitinho descrevem características de forte e fraca Evitação de Incertezas operando simultaneamente, podendo ser interpretado como a combinação de forte Evitação de Incerteza com tendências coletivistas, o que significa que laços dentro do grupo podem ser usados para fazer as coisas, mesmo onde as regras estão no caminho (HOFSTEDE et al., 2010).

Em um dos poucos estudos empíricos sobre aspectos culturais nacionais realizados quantitativamente, Fernandes e Hanashiro (2015) desenvolveram uma pesquisa visando identificar e analisar a incidência dos traços do jeitinho e da Sociedade Relacional na gestão de uma instituição financeira nacional privada, com dois objetivos específicos, sendo o primeiro analisar se esses traços manifestavam-se de forma diferente, segundo: sexo, idade, cargo, escolaridade e tempo de empresa; e o outro, analisar a relação entre o Jeitinho e a

Sociedade Relacional. Para isso, os autores desenvolveram uma escala que mensurava esses dois traços.

O construto Jeitinho foi desenvolvido com base nos traços Formalismo e Flexibilidade, no qual se espera que o praticante do jeitinho perceba: (a) a existência de regras inadequadas à prática social; (b) a necessidade de flexibilização na aplicação das regras; (c) a necessidade de contornar regras, visando resolver problemas ou situações especiais; e (d) a necessidade de ajudar alguém ou dar andamento ao trabalho como sendo prioritária, mesmo que regras tenham que ser contornadas. Na análise dos dados, após os procedimentos estatísticos, o construto Jeitinho Brasileiro se dividiu em três fatores, sendo eles o *Contorno de regras*, que inclui também a ideia de ambiguidade (entre o Sim e o Não, o Pode e o Não Pode, sempre existe um Talvez), a *Flexibilização*, ou seja, a necessidade de ter jogo de cintura, e o terceiro fator a *Estratégia informal de resolução de problemas*, que revela um raciocínio no qual seguir regras é menos importante que resolver os problemas.

Os autores colocam como uma das contribuições de seu estudo que as escalas de Jeitinho e Sociedade Relacional podem ser aplicadas em investigações como variáveis independentes ou moderadoras, para a compreensão de fenômenos que podem sofrer influências da cultura brasileira. Ou, ainda, como variáveis dependentes, buscando-se entender quais fenômenos explicam esses dois traços. Como limitações e sugestões, os autores destacaram que as escalas desenvolvidas precisariam ser testadas em amostras mais heterogêneas, constituídas por organizações de diferentes setores e porte, estatais e públicas, origem e regiões geográficas do Brasil. Além disso, pesquisas também poderiam ser endereçadas para verificar se empresas com código de conduta ou de integridade apresentam resultados diferentes das que não possuem tais códigos. Essas sugestões serviriam como uma boa indicação para aplicação dos construtos em ambientes que apresentam um conjunto de regras relacionadas à segurança da informação, principalmente para compreender como o jeitinho influencia na conformidade dessas regras, como é proposto nesta pesquisa.

2.3 CULTURA, TECNOLOGIA DA INFORMAÇÃO E SISTEMAS DE INFORMAÇÃO

O conceito de Cultura tem sido estudado por pesquisadores de SI desde os primórdios da disciplina. As crenças e valores em relação à TI e SI, que permeiam os grupos sociais, foram examinados a partir de uma variedade de perspectivas, como a cultura nacional, étnica, organizacional e profissional (GALLIVAN; SRITE, 2005). A pesquisa cultural nacional e a

pesquisa sobre cultura organizacional surgiram como fluxos de pesquisa amplamente separados (LEIDNER; KAYWORTH, 2006) e percebendo-se a necessidade de desenvolver estudos que abordassem como os fatores culturais se relacionavam à TI, buscando a construção de teorias para a área, alguns pesquisadores se debruçaram sobre a temática.

Straub et al. (2002) foram uns dos primeiros a buscar um caminho para o relacionamento entre cultura e SI. De acordo com os autores, na pesquisa em SI, a cultura de sujeitos e entrevistados era problemática, pois era conceitualizada de uma maneira simplista. Uma das soluções encontradas para essa questão foi considerar o uso da Teoria da Identidade Social, ou *Social Identity Theory* (SIT), desenvolvida por Tajfel (1970, 1978). Straub et al. (2002) propuseram uma visão alternativa da cultura através da SIT, que sugere que cada indivíduo é influenciado por uma infinidade de culturas e subculturas, algumas étnicas, algumas nacionais e algumas organizacionais.

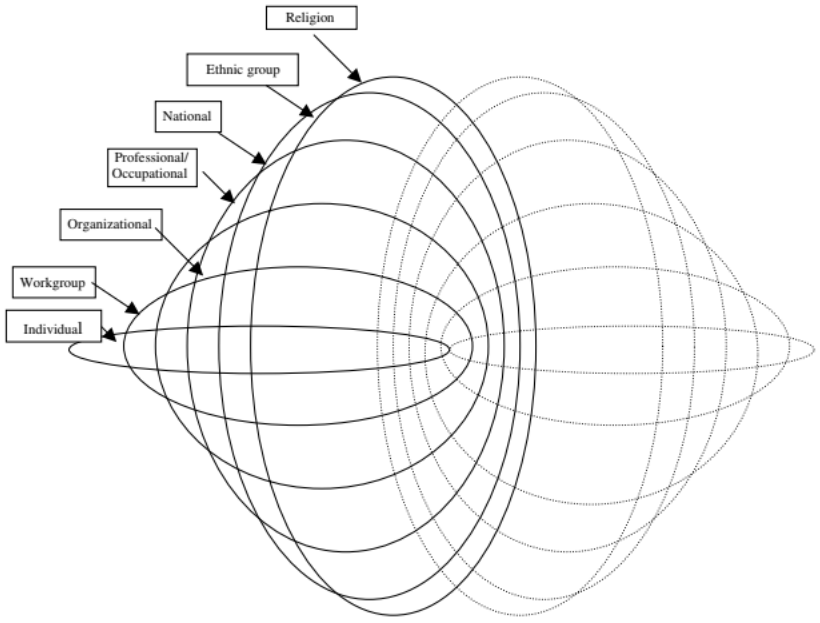
Os autores sugerem que a identidade social de um indivíduo representa a fusão de culturas entre fronteiras (nacional, organizacional, profissional, etc.), que se fundem para criar uma cultura global, sendo essa combinação única para cada indivíduo. Na SIT, os indivíduos percebem que pertencem ou não a um grupo. Se pertencem, são parte do "grupo interno"; se não, eles são parte do "grupo externo". O grupo interno torna-se uma forma proeminente de os indivíduos avaliarem a si mesmos e aos outros, se as normas do grupo são respeitadas, se essas normas são distintas das normas de outros grupos e assim por diante. Dessa maneira, o grupo interno se torna referência para crenças, atitudes, valores, normas e comportamentos. A força do sentimento de similaridade cultural depende de quantas das características os indivíduos acreditam ter em comum com os outros do grupo.

Para tornar mais compreensíveis suas colocações, Straub et al. (2002) propuseram a metáfora da "cebola" (Figura 1) para descrever essas características em camadas, onde as camadas mais próximas do núcleo da cebola seriam as mais relevantes. Assim, a imagem de uma "cebola virtual" apresenta camadas internas que ocasionalmente trocariam de lugar com as camadas externas. As camadas são permeáveis, sua espessura sinaliza a força do valor mantido pelo indivíduo. Além disso, a inter-relação entre uma camada e um comportamento específico pode variar dependendo das circunstâncias externas - criando uma cebola virtual, onde cada camada pode se mover para dentro ou para fora do núcleo.

Pela compreensão de ser impossível questionar ou investigar o inconsciente coletivo de toda uma cultura, a unidade individual de análise seria apropriada e significativa. Uma vez que os dados do nível individual fossem agregados, também seria possível afirmar que certas

características culturais pertencem ou não a certas culturas. A metáfora da "cebola virtual" supõe que a estratificação da cebola que compõe a cultura de uma pessoa não é um conjunto permanente e imutável de relacionamentos. Enquanto uma pessoa pode ser um composto cultural de apenas alguns elementos, ele ou ela atribui importância a essas subculturas de acordo com as mudanças de condições e tensões.

Figura 1 - Modelo da "cebola virtual"



Fonte: Galivan e Srite (2005)

Complementando a construção de Straub et al. (2002), Gallivan e Srite (2005) colocam que muitas vezes é assumido que a cultura organizacional é um subconjunto da cultura nacional, sendo essa visão difundida, já que a maioria das organizações opera dentro de uma determinada nação e emprega membros da mesma cultura nacional. Assim, gerentes e pesquisadores geralmente consideravam a cultura organizacional como um microcontexto que seus funcionários operam e a cultura nacional como o macro.

Após sua revisão de literatura, Gallivan e Srite (2005) sugeriram que em muitos estudos na área de TI, a cultura nacional era concebida em termos bastante simples – presume-se que as pessoas pertencem apenas a um único grupo cultural, e esses grupos são considerados estáticos, homogêneos e mutuamente exclusivos. Além disso, em muitos estudos, o significado da cultura e como as crenças, valores e normas específicas influenciam o uso da TI ou os atributos dos gerentes e funcionários de TI não eram abordados diretamente. Como uma possível solução para desenvolver uma visão mais integrada da cultura, considerar

o que as perspectivas culturais nacionais e organizacionais têm em comum seria mais adequado, pois ao se considerarem as perspectivas de cultura nacional e organizacional separadamente, o resultado seria uma perspectiva limitada sobre a contribuição da cultura para a compreensão do comportamento humano e, especificamente, das crenças e comportamentos relacionados à TI.

Para isso, retomando a construção de Straub et al. (2005), a partir da Teoria da Identidade Social (SIT), os autores postularam que há necessidade de uma abordagem mais holística para definir cultura e entender como ela modela o comportamento individual e de grupo. Uma ilustração simples é o fato de que a identidade nacional de um indivíduo (ou seja, o seu país de origem) é mais crítica na formação de suas crenças em curso sobre eventos políticos internacionais; enquanto a cultura ocupacional e culturas específicas de grupos de trabalho tendem a moldar crenças sobre TI. Através da metáfora virtual da cebola, baseada na SIT, haveria muitas oportunidades para examinar a influência de várias camadas de identidade nas crenças e comportamentos relacionados à TI de uma pessoa. Mas os autores colocam que testar o modelo proposto por Straub et al. (2002) na íntegra poderia ser problemático, dada a sua complexidade. Um caminho mais simples poderia ser examinar as interações entre apenas dois níveis de identidade social de cada vez, como por exemplo, entre a cultura nacional e a organizacional.

Leidner e Kayworth (2006) seguem um caminho diferente ao relacionar a TI com aspectos culturais. Após sua revisão da literatura, evidenciaram alguns pontos, como por exemplo, que a cultura nacional e a organizacional apareciam como correntes distintas na literatura. Outro ponto importante evidenciado é que, apesar da diversidade de pesquisas relacionando cultura e TI, ainda existiam lacunas como a própria cultura de TI, pois os estudos geralmente tratavam a cultura como sendo homogênea, sem considerar os valores competitivos entre subgrupos organizacionais, conflitos e resultados contraditórios de TI. Assim, substituindo o termo cultura por valor, já que a maioria dos trabalhos encontrados em sua revisão abordava a cultura a partir de valores, Leidener e Kayworth (2006) trazem três tipos de conflitos que poderiam emergir entre a TI e os valores de diferentes grupos:

- o conflito do sistema, o qual surge quando os valores implícitos de uma TI específica contradizem os valores mantidos pelos membros do grupo que usam ou que devem usar o sistema, sendo rotulado dessa forma porque é o conflito introduzido por um sistema específico que traz a questão da cultura à tona;

- o conflito de contribuição, o qual é definido como a contradição entre os valores dos membros do grupo e os valores de TI do grupo, sendo rotulado assim, pois no centro desse conflito está a relevância percebida, ou irrelevância, da TI para complementar os valores do grupo; e
- o conflito de visão, que é a contradição entre valores incorporados em um sistema e os valores de TI de um grupo. É denominado assim porque o grupo utilizador deve conciliar sinais mistos sobre os valores que eles associam à TI e os valores que eles percebem estar incorporados em um sistema de informações específico.

Enquanto muitas das pesquisas realizadas anteriormente sobre cultura de TI fizeram suposições sobre a influência direta da cultura nacional, organizacional ou de subunidades na gestão, desenvolvimento, adoção, uso e resultados de uso de TI, Leidener e Kayworth (2006) propõem que, no contexto da TI, é igualmente importante olhar além dos efeitos diretos da cultura em SI e considerar as maneiras pelas quais esses três conflitos culturais influenciam e são influenciados. Para isso, utilizam-se da Teoria de Bourdieu (1979) sobre valores e preferências mantidos por grupos para construir as preposições da teoria do conflito entre cultura e TI, levando em conta os três tipos de conflitos já citados. A partir da resolução desses conflitos, os autores colocam que seria possível a mudança cultural a partir da TI.

Essa abordagem possui desafios no tocante aos estudos em nível de empresa sobre a influência da cultura no uso de um sistema de informação não dever apenas examinar a cultura organizacional, mas também suas possíveis interações com valores de subcultura nacional ou organizacional e como essas interações potencialmente influenciam comportamentos. Outro desafio na pesquisa da cultura em SI é a suposição de que todos os indivíduos dentro de uma determinada unidade cultural responderão de maneira consistente com base nos valores culturais do grupo. O problema potencial dessa visão é que ela não leva em consideração a possibilidade de diferenças individuais dentro de uma unidade cultural específica levar a diferentes resultados comportamentais. Essa noção de adequação individual à cultura sugere que a pesquisa da cultura de SI pode precisar considerar a disposição individual como um fator ao estudar os impactos da cultura em determinados resultados de TI, como colocado por Straub et al. (2002).

Sendo a Segurança da Informação um dos tópicos dos estudos da área de Sistemas de Informação, espera-se que as relações entre diferentes aspectos culturais possuam influência no comportamento dos indivíduos para seguir as normas de segurança da informação, sendo abordado nos próximos tópicos como essas relações são estudadas atualmente pelos

pesquisadores de Segurança da Informação, principalmente no que tange ao comportamento dos indivíduos dentro das organizações.

2.4 CULTURA E SEGURANÇA DA INFORMAÇÃO

É importante destacar que existem diferentes concepções sobre a influência da cultura na sociedade. Como já definido por Straub et al. (2002), diferentes culturas podem influenciar o comportamento do indivíduo relacionado à TI. Nos estudos sobre Segurança da Informação, diferentes abordagens culturais são utilizadas para explicar os aspectos que influenciam principalmente o comportamento dos indivíduos relacionados à Segurança da Informação.

Utilizando conceitos da Cultura Organizacional, estudiosos da área de SI propuseram o termo Cultura de Segurança da Informação. Para Da Veiga e Eloff (2010), uma cultura de segurança da informação é definida como as atitudes, suposições, crenças, valores e conhecimentos que empregados e demais partes interessadas usam para interagir com os sistemas e procedimentos da organização em qualquer ponto no tempo. Para os autores, a interação resulta em um comportamento aceitável ou inaceitável (isto é, incidentes) evidente em artefatos e criações que se tornam parte da forma como as coisas são feitas na organização para proteger seus ativos de informação. Alhogail e Mirza (2014) definem a cultura da segurança da informação como a coleta de percepções, atitudes, valores, suposições e conhecimento que orientam a interação humana com ativos de informação em uma organização, com o objetivo de influenciar o comportamento de segurança dos funcionários para preservar a segurança da informação. Os controles de segurança têm um impacto nos processos organizacionais, na tecnologia e na maneira pela qual os usuários processam as informações.

Thomson e Von Solms (2006) desenvolveram o MISSTEV- *Model for Information Security Shared Tacit Espoused Values*. O primeiro componente do Modelo MISSTEV é o Modelo de Aprendizado por Competências Conscientes. O modelo descreve o processo e os estágios de aprendizagem de uma nova habilidade ou comportamento, e é dividido em quatro etapas, que progridem da Incompetência Inconsciente, que é a etapa em que os indivíduos não reconhecem que não possuem as habilidades e conhecimentos necessários para executar uma tarefa, até a Competência Inconsciente, que desenvolvida após o ganho da consciência da necessidade de se aprender novas atividades e o desenvolvimento das mesmas, tornaram-se tão praticadas que as pessoas não precisam mais pensar em como realizá-las. O segundo

componente do modelo é o modo de criação de conhecimento de Nonaka. O processo de Criação de Conhecimento compreende o conhecimento tácito e o conhecimento explícito, assim como as etapas de conversão de conhecimento que devem ocorrer para que um tipo de conhecimento seja traduzido para o outro.

Resultante dessas duas abordagens, Thomson e Von Solms (2006) detalham a evolução desde o desenvolvimento da Política Corporativa de Segurança da Informação até a realização da Obediência Corporativa à Segurança da Informação. A partir do conhecimento tácito, ou visão da gerência sênior sobre Segurança da Informação, diferentes etapas, que seguem com a Externalização da PSI pela alta gestão, e com treinamentos que possibilitem a internalização desse conhecimento pelos funcionários. Por meio da internalização, os funcionários devem compreender e apoiar totalmente a visão de segurança da informação da gerência sênior e, até esse ponto, as habilidades de segurança da informação devem ter se tornado tão praticadas que são de segunda natureza para os funcionários. A socialização desse conhecimento permitiria a evolução para o estágio final de Obediência da Segurança da Informação Corporativa, o que seria o sucesso da visão da alta administração para a segurança da informação implementada na organização. Fica clara a importância da alta gestão para o desenvolvimento da Cultura de segurança da Informação nas considerações dos autores – sendo um ponto essencial, instrumentalizado através das PSIs.

Da Veiga e Martins (2015) utilizaram a ISCA (*Information Security Culture Assessment*), ou avaliação da cultura de segurança da informação, através de um estudo empírico que forneceu a oportunidade de avaliar a eficácia do modelo teórico desenvolvido durante pesquisas anteriores. O impacto dos programas de conscientização e treinamento em segurança da informação medido pela ISCA é analisado para verificar se o foco nesses aspectos poderia contribuir para instalar uma cultura de segurança da informação mais forte. Nos resultados do estudo, algumas evidências foram encontradas, entre as principais: os funcionários que receberam treinamento prévio em segurança da informação responderam de forma mais positiva do que aqueles que não receberam. Isso ficou evidente na análise comparativa das quatro ocasiões de avaliação e dos testes *t*. Fica claro no trabalho a importância de a organização desenvolver a consciência em seus colaboradores, e do treinamento.

Visando estabelecer que a não conformidade dos funcionários com as PSIs pode ser abordada através do incentivo à cultura de conformidade com as PSIs, ou da *ISP compliance culture* (ISPCC), através da promoção da cultura organizacional de apoio, envolvimento do

usuário final e liderança de conformidade nas organizações, Amankwa, Loock e Kritzinger (2018) desenvolveram um modelo no qual se estabeleceu que a cultura organizacional de apoio, a liderança de segurança da informação e o envolvimento dos usuários possuem um efeito significativo na atitude de conformidade com as PSIs, e essa atitude exerce um efeito positivo na cultura de conformidade com as PSIs e com a intenção comportamental de cumpri-las. Já a intenção comportamental teria um efeito positivo na ISPCC também. Foi demonstrado que dois dos três construtos são influentes na construção de atitudes positivas em relação ao ISPCC nas organizações, sendo eles a cultura organizacional de apoio e o envolvimento dos usuários. A liderança de segurança, mesmo tendo um efeito positivo, não foi estatisticamente significante. Já a atitude obteve um efeito significativo na intenção comportamental e essa um efeito significativo na cultura de conformidade. Em sua discussão, os autores destacam a importância do cultivo da cultura de conformidade com a segurança da informação, apontando a importância de treinamentos e *workshops*, da conscientização relacionada à segurança da informação e da determinação dos papéis dos funcionários nas PSIs. Ao final, destacaram que futuros pesquisadores poderiam investigar os efeitos de outros fatores, como tipos de personalidade, motivação e sanções nas atitudes dos funcionários em relação ao estabelecimento do ISPCC para a conformidade real com as PSIs nas organizações.

Mas como colocado anteriormente, além da cultura organizacional relacionada à segurança da informação, alguns estudos abordam como as diferenças culturais nacionais interferem no comportamento de segurança da informação dos funcionários, principalmente a partir de estudos transculturais. Karjalainen et al. (2013) desenvolveram um estudo qualitativo para compreender o comportamento de segurança da informação de funcionários de diferentes países, a partir da suposição que os pressupostos culturais são aprendidos e, portanto, podem ser alterados. A partir dessa compreensão, os autores se baseiam nos paradigmas de aprendizagem: o behaviorismo, o cognitivismo e o construtivismo. A coleta de dados empíricos foi realizada em vários locais de uma empresa global. Os locais de entrevista selecionados foram Finlândia, Suíça, Emirados Árabes Unidos e China, sendo selecionados representantes de diferentes ambientes culturais com a ajuda do gerente de segurança da informação da organização. Nos resultados, os autores destacam que entre as razões independentes da cultura que explicam o comportamento de segurança dos funcionários em todos os países estão a experiência anterior de trabalho, a moral e a educação, o ambiente de trabalho, a identidade profissional, a mídia e a conformidade social. E entre as razões dependentes da cultura que explicam o comportamento dos funcionários estão as preferências

dos funcionários em relação aos meios de aprendizagem do comportamento de segurança, este variando conforme a cultura nacional. Em particular, os métodos de aprendizagem behaviorista são preferidos na China. Na Suíça, os métodos de aprendizagem construtiva e social construtiva são os preferidos. Uma das implicações práticas colocadas pelos autores é que, de acordo com as entrevistas, em cada país, o equívoco dos funcionários de que eles já conhecem o comportamento adequado de segurança de SI pode levá-los a superestimar suas habilidades de segurança e a conformidade com os procedimentos adotados pela organização. Isso cria um desafio para motivar funcionários experientes a adquirir mais habilidades em segurança de SI.

Utilizando como amostra indivíduos norte-americanos e sul-coreanos, Hovav e D'arcy (2012) buscaram explorar a eficácia transcultural das contramedidas de segurança em dissuadir o uso indevido de sistemas de informação. A partir das concepções da Teoria da Dissuasão, desenvolveram um modelo causal que considera as contramedidas processuais e técnicas como influenciadoras das sanções formais e informais e do status social, e esse influenciando a intenção do uso indevido de SI. Para auxiliar os respondentes, foram utilizados cenários hipotéticos que demonstravam o uso indevido de componentes de SI no ambiente organizacional. Como principais resultados, os autores destacaram que a certeza percebida de sansões teve uma influência mais forte na intenção de uso indevido do SI para a amostra coreana, enquanto a influência da gravidade das sanções foi mais forte para os EUA. Assim, a Teoria da Dissuasão não é culturalmente neutra. A comparação de médias também indicou que os usuários sul-coreanos perceberam os comportamentos do cenário de uso indevido de SI como menos moralmente aceitáveis do que seus equivalentes nos EUA.

Então, baseado nas diferentes abordagens utilizadas nas pesquisas citadas anteriormente, verifica-se que o desenvolvimento de uma cultura de segurança da informação requer esforços organizacionais, seja através do apoio da alta gerência, da oferta de treinamentos e suporte organizacional, de modo a influenciar a consciência de segurança dos indivíduos que impacta em uma maior conformidade com as PSIs. Além disso, considerar a influência da cultura nacional no comportamento relacionado à segurança da informação dos indivíduos pode ser um diferencial para a efetividade das normas de segurança da informação.

2.5 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Uma PSI assegura, dentre muitos fatores justificados por sua grande abrangência, que as informações estejam sempre disponíveis, íntegras e confiáveis (NASCIMENTO, 2012). Segundo Goel e Chengalur-Smith (2010), uma PSI é um documento que declara a maneira que uma organização pretende proteger seus ativos de informação de ameaças (sendo elas internas ou externas), operacionaliza a implantação da segurança e fornece orientações para condutas de funcionários e de gestão. Para Bulgurcu et al. (2010), as PSIs são declarações dos papéis e responsabilidades dos empregados para proteger as tecnologias de informação e recursos de suas organizações. Já Aurigemma e Panko (2012) destacam que uma PSI descreve as funções e responsabilidades dos funcionários, abordando questões específicas de segurança na proteção dos recursos de informações de sua organização. É uma das ferramentas vitais para garantir o uso seguro de ativos de informação e dados em um contexto organizacional. Embora a conformidade da política de segurança tenha atraído cada vez mais atenção acadêmica nos últimos anos, o tópico tem uma rica história em pesquisa de segurança de sistemas de informação, sendo amplamente reconhecido que fatores como suporte administrativo para atividades de segurança, comunicação clara com os usuários sobre políticas e sanções por não conformidade podem influenciar os funcionários a se comportarem com segurança (CRAM; D'ARCY; PROUDFOOT, 2019).

Identifica-se na literatura um interesse crescente dos pesquisadores em estudar os fatores que influenciam os comportamentos de conformidade e transgressão das políticas de segurança pelos usuários finais, principalmente com base na proteção, escolha racional e teorias gerais de dissuasão (CHENG et al., 2013). Diferentes abordagens têm sido utilizadas na tentativa de compreender o que leva o indivíduo a cumprir ou não com as normativas organizacionais, estando grande parte da pesquisa empírica contemporânea sobre a conformidade da política de segurança enraizada nas teorias do comportamento humano que abrangem as disciplinas de criminologia, psicologia e sociologia (CRAM; D'ARCY; PROUDFOOT, 2019).

Siponen e Vance (2010), a partir das concepções da Teoria da Neutralização que coloca que os indivíduos criam maneiras de tornar as normativas inoperantes, descobriram que o efeito das sanções quando os indivíduos estão operando através da neutralização são insignificantes no que tange à intenção de cumprir com as PSIs. Vance et al. (2012) foram os primeiros autores a aplicar a Teoria da Proteção a Motivação (PMT) por completo na área de

Segurança da Informação, em conjunto com o hábito, considerado na literatura um aspecto anterior ao processo cognitivo da PMT (VANCE et al., 2012). Como principais achados, identificaram que quase todos os construtos da PMT possuíam correlação com a intenção de cumprir com as políticas de segurança da informação e que o hábito de cumprir com as normativas possuía uma forte relação com o processo cognitivo da PMT. Desenvolvendo um novo modelo que combina a Teoria da Motivação a Proteção, a Teoria da Ação Racional e a Teoria da Avaliação Cognitiva, Siponen, Mahmood e Pahnila (2014), através da técnica de modelagem de equações estruturais, encontraram que a severidade percebida de possíveis ameaças à segurança da informação, a crença dos funcionários quanto à sua aplicação e aderência às políticas de segurança da informação, a vulnerabilidade percebida a possíveis ameaças à segurança, a atitude dos funcionários em cumprir as políticas de segurança da informação e as normas para o cumprimento dessas políticas tiveram um efeito significativo e positivo na intenção dos funcionários de cumprir com estas políticas. A intenção de cumpri-las também teve um impacto significativo na conformidade real com essas políticas.

Mesmo com os mais variados tipos de pesquisa e teorias que visam analisar o que leva à conformidade ou não das PSIs, alguns pontos específicos merecem mais atenção dos pesquisadores. Cram, D'arcy e Proudfoot (2019) realizaram uma meta-análise sobre os principais antecedentes da conformidade da política de segurança da informação por funcionários em diferentes contextos, encontrando alguns *insights* interessantes que colaboram com possíveis direções futuras para novos estudos. De acordo com os autores, especificamente quando se fala de estudos que consideram os aspectos culturais como influentes na intenção ou conformidade com as PSIs, a maior parte deles se baseia em aspectos organizacionais, com poucos estudos considerando aspectos de culturas nacionais. Além disso, quando se trata de estudos transculturais, a maior parte se concentra entre países da América do Norte e Sudeste Asiático. Os autores também colocam que existe a necessidade de os estudiosos considerarem antecedentes do cumprimento de PSIs específicos para determinadas culturais nacionais, como a brasileira, por exemplo.

Nesse sentido, estudos que contemplem aspectos culturais nacionais, em conjunto com aspectos organizacionais da gestão de organizações, podem auxiliar o preenchimento dessa lacuna nas pesquisas relacionadas à Segurança da Informação, como um todo, e mais especificamente a sua aplicação no Brasil.

2.5.1 Políticas de Segurança da Informação no Brasil

Dentro dos estudos sobre Políticas de Segurança da Informação no Brasil existem duas abordagens predominantes, uma foca nos aspectos organizacionais, principalmente nos processos de Segurança da Informação, enquanto a outra foca nos aspectos que influenciam a conformidade com as PSIs por funcionários nas organizações. Galegale, Fontes e Galegale (2017), em estudo realizado em diferentes organizações brasileiras, identificaram que as PSIs nas organizações pesquisadas eram consolidadas e maduras, e que em todas, as PSIs analisadas possuíam o escopo para os diferentes tipos de usuários: funcionários, estagiários, fornecedores e prestadores de serviço, denotando a abrangência da responsabilidade para com a informação da organização, envolvendo tanto pessoas internas como externas à mesma. Os autores identificaram 40 controles citados de forma recorrente em políticas, os quais também foram associados à principal referência da literatura da área, descritos e agrupados em quatro extratos de frequência: 12 controles citados por 100% das políticas, 15 por 90%, 16 por 80% e 40 por 70% (GALEGALE; FONTES; GALEGALE, 2017). Já Albuquerque Junior e Santos (2017) constataram a partir da análise de PSIs de diferentes organizações brasileiras, considerando como base teórica a Teoria Institucional, que mesmo que as organizações possuam essas Políticas bem determinadas, isso não significa que o usuário final compreenda a importância de seu papel para garantir a segurança das informações organizacionais, pois a conformidade das organizações com as diretrizes de Segurança da Informação pode sofrer influências internas e externas, o que pode levar à implantação de PSIs que sirvam apenas para cumprimento de pressões externas do que para atender as necessidades de proteção de informações na organização.

Nascimento (2012), em seu estudo realizado no Ministério do Desenvolvimento Agrário, que visava identificar o impacto de aspectos culturais e estruturais na implantação de PSIs, identificou que havia a necessidade de uma política de comunicação interna em nível de informativos e propaganda sobre a importância que a política de segurança da informação tem para o cotidiano dos funcionários e para as atividades-fim do órgão, pois a política não parecia ser bem aceita, seguida ou mesmo compreendida pelos diversos setores da organização. Além disso, apesar da força de lei que obriga as organizações públicas a terem uma PSI, nem sempre era dada a devida importância e tampouco essa política era bem aceita, seguida ou mesmo compreendida pelos diversos setores da organização (NASCIMENTO, 2012). Em seus resultados sobre as práticas utilizadas pelas instituições federais de ensino

superior (IFES) para implantação de PSIs, Rios, Filho e Rios (2017) constataram que apenas 43% das IFES possuíam a PSI institucionalizada, cenário considerado preocupante, pois é estrutural que as instituições tenham suas políticas de segurança para que o processo de proteção da informação possa ser elaborado e assegurado. Para os autores, as poucas instituições que possuem uma PSI bem implementada está relacionado à participação da alta gestão no processo de segurança da informação, sendo apontado como um fator crítico para a elaboração de uma PSI (RIOS; FILHO; RIOS, 2017).

Já na perspectiva do usuário, Damasceno, Ramos e Pereira (2016) analisaram o papel das punições, do comprometimento moral e da eficácia percebida como fatores motivadores sobre os comportamentos do indivíduo na segurança da informação. Em seus resultados, a severidade da punição apresentou maior grau de contribuição na formação de clusters, sendo os mais predispostos e os menos predispostos a seguir as PSIs, apontando que essa variável teria um efeito dissuador na conformidade com as PSIs. Isso indica que a pessoa se sentirá mais inclinada a seguir uma política ao saber que é monitorada e, por consequência, haver a possibilidade de punição em caso de comportamento abusivo (DAMASCENO; RAMOS; PEREIRA, 2016). A severidade percebida, representada pelo perigo percebido, também apresentou forte correlação com a intenção comportamental de se seguir as PSIs no trabalho de Silveira et al. (2019). Em seu estudo, baseado na pesquisa de Vance et al. (2012), o qual teve a intenção de analisar se as PSIs eram seguidas por indivíduos atuantes em empresas localizadas no estado do Rio Grande do Sul, os autores perceberam que além do resultado do perigo percebido, a vulnerabilidade percebida, que se refere à percepção do quanto se está vulnerável às ameaças disponíveis, tanto como a eficácia da resposta, que é a percepção de que as respostas disponíveis são efetivas, não produziram efeitos diretos significantes na intenção de cumprir com as PSIs, indicando que os usuários pesquisados não percebem a ameaça por completo, nem creem na eficácia da PSI de sua organização no seu enfrentamento. Um resultado interessante é que os benefícios percebidos em não cumprir com as PSIs, como por exemplo, o ganho de tempo para outras atividades, apareceu como o fator com maior correlação com a intenção comportamental de seguir as PSIs, indicando que para os respondentes da pesquisa existem benefícios em não cumprir com as normas, regras e procedimentos de Segurança da Informação estabelecidas pelas instituições onde atuam.

Em um dos poucos trabalhos no Brasil que considerou a cultura de segurança da informação, Beck e Santos (2010) observaram que a cultura organizacional existente na empresa investigada propiciava um ambiente a comportamentos seguros por parte de seus

funcionários, destacando a importância de tentar mitigar riscos e diminuir a distância existente entre os níveis hierárquicos mais elevados e os demais, expondo os funcionários a treinamentos mais incisivos e rotineiros.

Os resultados dos trabalhos descritos nessa seção confirmam que existe a necessidade de maior aprofundamento nos estudos sobre Segurança da Informação no Brasil, principalmente no que tange à relação entre as PSIs e o comportamento dos brasileiros dentro das organizações, em seu ambiente de trabalho. Assim, destaca-se a seguir a aplicação da Teoria do Comportamento Planejado em estudos relacionados à conformidade com as políticas de segurança da informação.

2.6 A TEORIA DO COMPORTAMENTO PLANEJADO (TPB) E ESTUDOS SOBRE A CONFORMIDADE COM AS PSI

A TPB se caracteriza por ser uma extensão da Teoria da Ação Racional (AJZEN; FISHBEIN, 1980), pela noção dos autores de que a percepção de controle poderia ter um impacto importante na motivação comportamental de uma pessoa. Quanto mais a conquista de um objetivo comportamental é vista como “sob controle”, maior é a intenção de a pessoa realizar um comportamento esperado (AJZEN; MADDEN, 1986). Como na teoria original da Ação Racional, um fator central na Teoria do Comportamento Planejado é a intenção do indivíduo de executar um determinado comportamento. Supõe-se que as intenções capturam os fatores motivacionais que influenciam um comportamento; são indicações de quanto as pessoas estão dispostas a tentar, ou de quanto esforço planejam fazer para realizar o comportamento. Como regra geral, quanto mais forte a intenção de se envolver em um comportamento, mais provável deve ser seu desempenho (AJZEN; MADDEN, 1986).

Como determinantes independentes da intenção de comportamento, a TPB postula a atitude, as normas subjetivas e o controle percebido. A atitude em relação ao comportamento refere-se ao grau em que uma pessoa tem uma avaliação favorável ou desfavorável do comportamento em questão. Já a norma subjetiva refere-se à pressão social percebida para executar ou não esse comportamento. O controle comportamental percebido refere-se à facilidade ou dificuldade percebida de um indivíduo executar o comportamento, supondo-se que este reflita suas experiências passadas, bem como impedimentos e obstáculos previstos. Espera-se que a importância relativa da atitude, das normas subjetivas e do controle comportamental percebido na predição da intenção varie entre comportamentos e situações

(AJZEN; MADDEN, 1986). Para um uso correto da TPB, Ajzen (1990) define que o comportamento analisado precisa ser especificado. No caso das pesquisas que analisam o comportamento relacionado com as PSIs, a TPB é uma das teorias cognitivas mais utilizadas (CRAM, D'ARCY; PROUDFOOT, 2019).

Em uma das primeiras pesquisas empíricas que utilizaram modelagem de equações estruturais para essa finalidade, baseando-se nos modelos teóricos desenvolvidos por Dinev e Hu (2007) e Hu e Dinev (2005), que levam em conta aspectos cognitivos a partir da Teoria do Comportamento Planejado e as dimensões desenvolvidos por Hofstede (1980), Dinev et al. (2009) realizaram uma pesquisa transcultural, com amostras de americanos e sul-coreanos, com o objetivo de analisar como alguns fatores influenciam a decisão dos usuários de computador em usar tecnologias de informação de proteção contra tecnologias negativas, como *spywares*. Em seus resultados, identificaram que os usuários sul-coreanos demonstravam uma relação mais forte entre as normas subjetivas e as intenções comportamentais do que suas contrapartes nos EUA. Também descobriram que, embora em ambas as culturas o conhecimento das consequências negativas do *spyware* seja suficiente para motivar os usuários a desenvolver atitudes positivas em relação às tecnologias de informação protetoras e formar a intenção de usá-las, o papel da conscientização é muito mais forte nos EUA do que na Coréia do Sul, consistente com as características de individualismo e masculinidade das duas culturas.

Bulcurcu et al. (2010), partindo da Teoria do Comportamento Planejado, postularam em seu estudo que as atitudes e as crenças normativas, em conjunto com a autoeficácia, influenciam a intenção de conformidade com as PSIs. A partir da TPB, postularam que as crenças relacionadas à conformidade com as PSIs se baseiam nas crenças sobre a avaliação geral das consequências do cumprimento ou não cumprimento, e como antecedentes das crenças, a consciência sobre a segurança da informação (CSI). Em seus resultados, evidenciou-se que a intenção de um funcionário de cumprir a PSI é significativamente influenciada por atitudes, crenças normativas e pela autoeficácia. As crenças dos resultados afetam significativamente as crenças sobre a avaliação geral das consequências e, por sua vez, afetam significativamente a atitude de um funcionário. Além disso, a CSI influenciou positivamente as crenças de atitude e resultado. Os resultados evidenciam que a CSI, em conjunto com as crenças, possui um papel crucial para que os funcionários possam ter uma atitude de conformidade com as PSIs.

Hu et al. (2012) propuseram que os efeitos da alta administração e da cultura organizacional deveriam ser levados em conta para entender completamente o comportamento de segurança dos funcionários nas organizações e para desenvolver práticas eficazes de gerenciamento de segurança das informações. Os autores estabeleceram como crenças individuais os construtos da Teoria do Comportamento Planejado, sendo eles as atitudes, as normas subjetivas e o controle percebido para a conformidade com as PSIs. Para verificar a influência dos aspectos da cultura organizacional, os autores se concentraram no papel dos valores culturais de orientação a objetivos e orientação de regras ao influenciar as crenças cognitivas individuais em relação às políticas de segurança da informação.

Como principais resultados encontrados, a percepção da participação da alta gestão não obteve um efeito significativo na atitude dos funcionários de conformidade com as PSIs. Os autores acreditam que o resultado pode ser influenciado pela distância hierárquica da alta gerência dos demais funcionários, e colocam que não se deve concluir que a participação da alta gerência não influencia diretamente as atitudes dos funcionários em relação à conformidade da política de segurança da informação, independentemente do tamanho, estrutura, cultura e estilos de liderança da organização. Por outro lado, os resultados mostraram que a cultura organizacional, especificamente a orientação de objetivos percebida e os valores de orientação de regras percebidos, tem um efeito significativo nas atitudes dos funcionários e que a participação da alta gerência influencia fortemente os valores culturais percebidos, sugerindo, então, que o impacto da alta administração na atitude dos funcionários é mediado pela cultura organizacional (HU et al., 2012).

Além disso, os resultados sugerem claramente que o efeito da cultura organizacional, talvez da cultura em geral, no comportamento individual é totalmente mediado pelos processos cognitivos internos dos indivíduos em relação a tarefas e contextos específicos. Embora a cultura forneça uma estrutura normativa para interpretação e criação de sentido e uma abordagem geral à solução de problemas para funcionários em ambientes organizacionais, a forte cultura organizacional por Segurança da Informação só não é suficiente para mudar o comportamento individual em relação a políticas ou programas específicos, como a conformidade com a segurança da informação.

É importante destacar que o uso da TPB sofreu adaptações nos estudos sobre as PSIs, sendo adaptadas às necessidades dos pesquisadores de Segurança da Informação, com diferentes utilizações, principalmente dos preditores e os construtos principais da TPB (SOMMESTAD; KARLZÉN; HALLBERG, 2019).

3 DESENVOLVIMENTO DO MODELO DE PESQUISA

Ao se levar em conta o cumprimento das normativas de Segurança da Informação pelos funcionários, faz-se necessário considerar que diferentes culturas requerem diferentes intervenções de segurança de SI, e que procedimentos descentralizados de segurança devem ser personalizados para cada país (KARJALAINEN et al., 2013). Por isso, desenvolver estudos de segurança da informação que contemplem aspectos específicos da cultura brasileira é necessário para se tentar compreender melhor o que influencia os indivíduos que atuam em organizações brasileiras a cumprir com as regras de segurança da informação, já que os valores de diferentes culturas, sendo a nacional, organizacional ou do próprio grupo de trabalho, influenciam no uso dos sistemas de informação por esses indivíduos (LEIDNER; KAYWORTH, 2006).

Para se encontrar os estudos que contemplassem a temática desejada, realizou-se uma revisão da literatura, a partir de buscas nas bases de conhecimento *Spell*, *Web of Science*, *Scopus* e Google Acadêmico. Ao buscar pesquisas que abordassem aspectos culturais, sendo eles organizacionais e nacionais, em conjunto com a segurança da informação, não foram encontrados trabalhos quantitativos utilizando modelos causais realizados no Brasil. Como o contexto que se espera medir nessa pesquisa é a conformidade com as normas de segurança da informação dentro das organizações brasileiras que os indivíduos trabalham, considera-se a cultura organizacional a qual o indivíduo está submetido como central no modelo de pesquisa. Aspectos considerados como essenciais para o desenvolvimento de uma cultura organizacional voltada para a segurança da informação, ou melhor, para a cultura de segurança da informação são considerados como influenciadores do comportamento dos indivíduos nas organizações.

Estudos já enfatizaram a importância da construção dessa cultura através da aprendizagem no ambiente organizacional (DA VEIGA; MARTINS, 2015; KARJALAINEN et al., 2013). A partir dessa constatação, realizou-se a avaliação de aspectos influenciados pela cultura organizacional que poderiam ser considerados como essenciais para uma maior conformidade com as PSIs, e que se relacionassem com a própria construção da cultura organizacional brasileira, a partir de suas características especificas, como a Hierarquia e o Formalismo, conforme destacado por Bruno e Arantes (2015) e Chu e Wood Jr. (2008). Por isso, escolheu-se para essa pesquisa a *Participação da Alta Gestão, a Cultura de Suporte Organizacional de Segurança da Informação* e a *Consciência de Segurança da Informação*

como fatores influenciados pela cultura organizacional e que influenciariam os funcionários no cumprimento das políticas de segurança da informação. Como colocado anteriormente, medir a cultura, sendo ela organizacional ou nacional, é algo que requer um aprofundamento do pesquisador que vá além de informações superficiais (SCHEIN, 1984). Por isso, nessa pesquisa, abordam-se os fatores observáveis consequentes da cultura.

Straub et al. (2002) e Gallivan e Srite (2005), a partir do uso da teoria da cebola, enfatizam que o indivíduo é formado por diferentes culturas, que possuem diferentes camadas, e que essas diferentes culturas influenciam o seu relacionamento com a TI nas organizações. Assim, considera-se que essas diferentes culturas também se relacionam quando se consideram os comportamentos dos indivíduos sobre Segurança da Informação. Por isso, considerar que tantos aspectos da cultura organizacional a que o indivíduo está submetido, como da cultura nacional, tornam-se pertinentes. Além disso, se considerarmos que os indivíduos tendem a adaptar o uso de sistemas aos seus valores, e este indivíduo é formado por diferentes culturas que possuem diferentes valores (LEIDNER; KAYWORTH, 2006), os requisitos para o cumprimento das PSIs podem sofrer influências desses diferentes níveis de valores, sendo estes valores até mesmo conflitantes.

A partir da revisão de literatura sobre cultura organizacional brasileira, o jeitinho apareceu como um dos fatores mais presentes nos estudos que consideram a cultura nacional como uma determinante de comportamentos nas organizações brasileiras. Por conta disso, considera-se nessa pesquisa o jeitinho, caracterizado como um aspecto específico da cultura nacional, como possível influenciador comportamental da conformidade com as PSIs. Complementarmente, para avaliar o comportamento desejado (no caso dessa pesquisa, o comportamento de cumprimento ou conformidade com as PSIs), optou-se pelo uso da Teoria do Comportamento Planejado (AJZEN, 1991; AJZEN; MADDEN, 1986). A seguir, discorre-se ao desenvolvimento das hipóteses do estudo, a partir de diferentes relações entre os construtos que compõem o modelo de pesquisa proposto – o qual será apresentado mais à frente.

3.1 O COMPORTAMENTO PLANEJADO E A CONFORMIDADE COM AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

No caso dessa pesquisa, o comportamento de conformidade com as PSIs é determinado pela atitude de conformidade, pelas normas subjetivas e pelo controle percebido

para tomar a ação de conformidade com as PSIs. A opção pelo uso do comportamento de conformidade ao invés da intenção comportamental ocorre por indicação de Cram, D'arcy e Proudfoot (2019), que colocam que o uso da conformidade ao invés da intenção comportamental poderia trazer resultados mais específicos ao analisar o comportamento relacionado às PSIs.

Como já definido, a atitude em relação ao comportamento refere-se ao grau em que uma pessoa tem uma avaliação favorável ou desfavorável do comportamento em questão (AJZEN; MADDEN, 1986). No caso das PSIs, a atitude com a conformidade possui um importante papel na conformidade com as políticas de segurança da informação, pois quanto mais os funcionários perceberem a sua atitude como algo benéfico, necessário e importante, maior será a sua intenção de segui-las (BULGURCU et al., 2010; AMANKWA et al., 2018). Já as normas subjetivas referem-se às pressões sociais que os indivíduos percebem para que determinado comportamento seja seguido (AJZEN; MADDEN, 1986). Em pesquisas na área de Segurança da Informação, já se constatou que a importância das normas subjetivas pode variar de acordo com diferentes culturas (DINEV et al., 2009). No Brasil, onde a pessoalidade no ambiente de trabalho ocorre através de uma confiança desenvolvida entre os pares, esta tende a substituir a impessoalidade na relação profissional, influenciando até mesmo na produtividade dos funcionários (FERNANDES; HANASHIRO, 2015). Assim, espera-se que a pressão social de pessoas consideradas importantes pelos indivíduos em seu ambiente de trabalho possua uma influência nas normas subjetivas do indivíduo. O controle percebido, por sua vez, refere-se à facilidade ou dificuldade percebida de executar um dado comportamento e supõe-se que este indivíduo leve em consideração as suas experiências passadas, bem como impedimentos e obstáculos previstos (AJZEN; MADDEN, 1986). Nessa pesquisa, espera-se que quanto maior for o controle percebido, isto é, quanto maior a capacidade que o indivíduo acredita possuir para cumprir com as PSIs, maior será a sua conformidade com o cumprimento das normas de segurança. Assim, propõem-se as seguintes hipóteses:

H1: A atitude de conformidade com as PSIs influencia positivamente o cumprimento das PSIs

H2: As normas subjetivas relacionadas à conformidade com as PSIs influenciam positivamente o cumprimento das PSIs

H3: O controle percebido da conformidade com as PSIs influencia positivamente o cumprimento das PSIs

3.2 A CONSCIÊNCIA DE SEGURANÇA DA INFORMAÇÃO (CSI)

Para compreender o papel da consciência da segurança da informação proposta neste estudo, é necessário entender o que se postulou em relação aos antecedentes da atitude, das normas subjetivas e do controle percebido. Mesmo encontrando evidências empíricas da validade do modelo TPB, os seus autores não definiram quais as crenças que poderiam influenciar o comportamento dos indivíduos. Para resolver essa questão, Ajzen (1991) desenvolveu a questão das crenças relevantes ao comportamento. De acordo com o autor, formam-se crenças sobre um objeto associando-o a certos atributos, ou seja, a outros objetos, características ou eventos. No caso de atitudes em relação a um comportamento, cada crença vincula o comportamento a um determinado resultado ou a algum outro atributo, como o custo incorrido pela realização deste comportamento. Como os atributos que passam a ser vinculados ao comportamento já são avaliados positiva ou negativamente, automaticamente e simultaneamente, adquire-se uma atitude em relação ao comportamento. Dessa maneira, um indivíduo aprende a favor de comportamentos que ele acredita ter consequências amplamente desejáveis e forma atitudes desfavoráveis em relação a comportamentos que associa a consequências principalmente indesejáveis. Especificamente, o valor subjetivo do resultado contribui para a atitude em proporção direta à força da crença, ou seja, o subjetivo.

Mesmo evidenciada a importância das crenças para o comportamento, utilizada em outros trabalhos na área de Segurança da Informação (BULCURCU et al., 2010), os autores colocam que a Teoria do Comportamento Planejado é, em princípio, aberta à inclusão de preditores adicionais, se for possível demonstrar que eles capturam uma proporção significativa da variação na intenção ou no comportamento após as variáveis principais da teoria serem levadas em consideração (SOMMESTAD; KARLZÉN; HALLBERG, 2019; AJZEN; MADDEN, 1986). Sommestad et al. (2019), em sua meta-análise de fatores preditores da TPB que influenciam o cumprimento das PSIs, identificaram quatro construtos de onze com relação estatística significativa com os construtos da TPB. Entre eles, destacaram-se a consciência sobre segurança da informação e a consciência sobre as PSIs. Os autores enfatizam que não se evidenciou validade discriminante entre os construtos, isto é, não foram encontradas diferenças estatísticas significativas entre eles, e que isso se deve a uma grande familiaridade entre os dois construtos. Assim, nesse estudo, optou-se por utilizar o construto *Information Security Awareness* (ISA) (em português, Consciência de Segurança

da Informação - CSI), proposto por Bulcurgu et al. (2010), como a consciência geral do indivíduo sobre segurança da informação.

Dessa forma, espera-se que a consciência sobre a segurança da informação, definida aqui como a extensão com que os membros da organização compreendem a importância da segurança da informação, o nível de segurança exigido pela organização e suas responsabilidades individuais de segurança (FLORES; EKSTEDT, 2016; ALNATHEER, 2015; BULGURCU et al., 2010) teriam um papel importante na atitude de conformidade com as PSIs. Programas de conscientização, por exemplo, são instrumentos importantes para promover práticas de segurança na organização, sendo a educação do usuário sobre as práticas de segurança exigidas durante o uso dos sistemas de informação um possível meio de melhorar a segurança corporativa (MONTESDIOCA; MAÇADA, 2015). Ajzen (1991) define em seu estudo que o comportamento passado é mais bem tratado, não como uma medida de hábito, mas como um reflexo de todos os fatores que determinam o comportamento de interesse. A própria construção da consciência de segurança é colocada como um fator que requer da organização a disposição de tempo e recursos.

Da Veiga e Martins (2015) demonstraram que com o passar do tempo, os funcionários que receberam treinamento prévio em segurança da informação foram mais positivos em relação à conformidade com as PSIs em comparação com os que não receberam, supondo-se, então, que os funcionários que passaram por treinamentos em segurança da informação são mais conscientes dos requisitos da política de segurança da informação aplicáveis a eles e seu entendimento de como proteger as informações, contribuindo para um nível mais alto de conformidade e promovendo uma cultura mais forte de segurança da informação. Sendo assim, considera-se nesse estudo a conscientização como um aspecto influenciador do comportamento planejado, pois quanto maior a compreensão do indivíduo sobre a importância da Segurança da Informação e das PSIs, maior a sua probabilidade de conformidade. Assim, propõem-se as seguintes hipóteses:

H4: A consciência de segurança da informação influencia positivamente a atitude de conformidade com as PSI

H5: A consciência de segurança da informação influencia positivamente as normas subjetivas de conformidade com as PSI

H6: A consciência de segurança da informação influencia positivamente o controle percebido de conformidade com as PSI

3.3 FATORES ORGANIZACIONAIS QUE INFLUENCIAM A CONFORMIDADE COM A PSI

Desde os primeiros estudos teóricos propondo diferentes modelos sobre Segurança da Informação, o apoio da alta gestão aparece com um papel chave para que a cultura de segurança da informação se desenvolva nas organizações (THOMSON; VON SOLMS, 2006). O suporte ao gerenciamento é outro fator importante no cultivo de uma cultura de segurança, apesar de não haver muita pesquisa nessa área. O apoio consistente da alta gerência é essencial para criar um ambiente de suporte, fornecendo condições necessárias para que os indivíduos ajam em conformidade com as políticas de segurança definidas pela organização. Esse suporte inclui orçamento, tecnologia e capital humano. O suporte e a liderança da alta gestão, segundo Glaspie e Karwowski (2017), são os principais contribuintes para a implementação bem-sucedida dos esforços de segurança da informação.

Assim, o estabelecimento de PSIs que sejam consideradas válidas pelos empregados parte da percepção da presença da alta gestão no processo. Hu et al. (2012) colocam que a alta gerência tem um papel fundamental na conformidade com as PSIs, influenciando os aspectos culturais da organização, mesmo que de forma indireta. Em uma cultura como a brasileira, em que as grandes diferenças entre níveis hierárquicos ainda é uma característica presente (HOFSTEDE et al., 2010), é prudente considerar que a gestão da segurança da informação ocorra se a alta gerência se fizer presente, dando o tom das ações que serão seguidas pelo restante da empresa. Assim, propõem-se as seguintes hipóteses:

H7: A participação da alta gestão influencia positivamente na cultura de suporte à segurança da informação da organização

H8: A participação da alta gestão influencia positivamente na consciência da segurança da informação na organização

O suporte que a organização oferece através de atividades como treinamentos, PSIs claras e de fácil entendimento, auxilia o desenvolvimento da cultura de segurança da informação (DA VEIGA; MARTINS, 2015). Portanto, as organizações precisam definir expectativas de que os funcionários entendam os riscos à segurança, tanto na teoria quanto na prática (expectativas comportamentais). Além disso, os funcionários precisam entender que aprender sobre segurança da informação levará a resultados positivos para eles, como indivíduos, e para a organização, como um todo. Personalizar e tornar as informações comunicadas em programas de treinamento em segurança tangíveis torna o treinamento

pessoalmente relevante e compreensível (FLORES; EKSTEDT, 2016), o que pode refletir na presença de informações mais seguras na organização (SOOMRO; SHAH; AHMED, 2016). Em empresas nas quais a cultura de segurança da organização é desenvolvida, pode-se esperar uma maior conformidade com as PSIs por parte dos funcionários (PARSONS et al., 2015). Assim, propõe-se a seguinte hipótese:

H9: A cultura de suporte à segurança da informação na organização influencia positivamente a consciência de segurança da informação

3.4 A INFLUÊNCIA DO “JEITINHO BRASILEIRO”

A importância das relações pessoais nas organizações brasileiras é um aspecto reconhecido na literatura de Estudos Organizacionais. Islam (2012) coloca que essa mistura de regulação formal e habilitação social informal permanecem centrais nas organizações brasileiras contemporâneas. Assim, pode-se considerar que as organizações brasileiras incorporam um "sistema duplo", pelo qual os resultados interpessoais podem diferir muito, dependendo do registro no qual eles estão sendo promulgados. Mesmo que a organização busque desenvolver em seus funcionários a consciência sobre a importância da segurança da informação através do desenvolvimento da cultura de segurança da informação, não se pode negar que a carga cultural que o indivíduo possui da sociedade na qual vive exerce um papel determinante nos meios de pensar e agir do mesmo (HOFSTEDE, 1980). Em outras palavras, as pessoas geralmente desconhecem sua cultura até encontrarem uma contracultura (LEIDNER; KAYWORTH, 2006).

Karlsson, Karlsson e Åström (2017) encontraram em seus resultados, ao comparar um valor único ao valor do pluralismo na conformidade com as PSIs, que o comportamento de conformidade dos funcionários pesquisados era em grande parte uma função da ocorrência de conflitos entre a segurança da informação e outros valores organizacionais. Em uma situação em que o determinado pelas PSIs entra em conflito com a eficiência e a eficácia do fluxo de trabalho, bem como com a integridade e o bem-estar pessoais dos indivíduos, é menos provável que os funcionários o cumpram (GLASPIE; KARWOWSKI, 2017).

Assim, o jeitinho, através de seus traços, já que não se pode afirmar que seja uma característica comum a todos os brasileiros (FREITAS, 1997), compreendido aqui como sua principal característica o contorno de regras para se alcançar um objetivo, visando à resolução de problemas no ambiente de trabalho, teria uma influência negativa na conformidade com as

PSIs, pois se cumprir as regras estabelecidas pela organização for considerado inadequado para o contexto de trabalho, no uso das ferramentas de TI e SI disponíveis, considerando que é mais importante solucionar problemas, suas chances de se adaptar e criar novos mecanismos que vão contra as regras definidas oficialmente pela organização serão maiores. Assim, propõe-se a seguinte hipótese:

H10: O jeitinho influencia negativamente o cumprimento das PSIs

3.5 A INFLUÊNCIA DO COMPORTAMENTO DE CONFORMIDADE COM AS PSIS NAS FALHAS DE SEGURANÇA DA INFORMAÇÃO

Apesar de o funcionário sofrer influências de diferentes aspectos no ambiente de trabalho, como o próprio jeitinho, se ele não tiver a consciência maior sobre segurança da informação e o comportamento cognitivo desejado, esse comportamento positivo de segurança individual pode limitar a incidência de falhas de segurança da informação no ambiente de trabalho. Thomson e Von Solms (2006) colocam que, no momento em que o funcionário atingisse um nível alto de maturidade sobre segurança da informação, o cumprimento das PSIs seria como uma segunda natureza para o mesmo, e que a partir da internalização do conhecimento sobre segurança da informação, haveria uma cobrança entre os pares no ambiente de trabalho.

Para Da Veiga e Elloff (2015), a existência ou não de uma cultura de segurança da informação resulta em um comportamento aceitável ou inaceitável (isto é, incidentes) evidente em artefatos e criações que se tornam parte da forma como as coisas são feitas na organização para proteger seus ativos de informação. Em ambientes em que as tarefas dos funcionários são altamente dependentes de outros funcionários, a gerência precisa enfatizar programas de conscientização e treinamento de segurança, pois esses funcionários tendem a policiar um ao outro (GLASPIE; KARWOWSKI, 2017; IFINEDO, 2012). Por isso, define-se que quanto mais os funcionários cumprirem com as normas de segurança da informação no seu ambiente de trabalho, se criaria uma auto regulação entre os pares, que consequentemente diminuiria as falhas relacionadas ao jeitinho, pois se a conformidade com as PSIs for considerada como importante pelo indivíduo, a chance de comportamentos inadequados em seu ambiente de trabalho ocorrer serão diminuídos, mesmo que sejam vistos como adequados para solucionar problemas (GLASPIE; KARWOWSKI, 2017). Assim, propõe-se a seguinte hipótese:

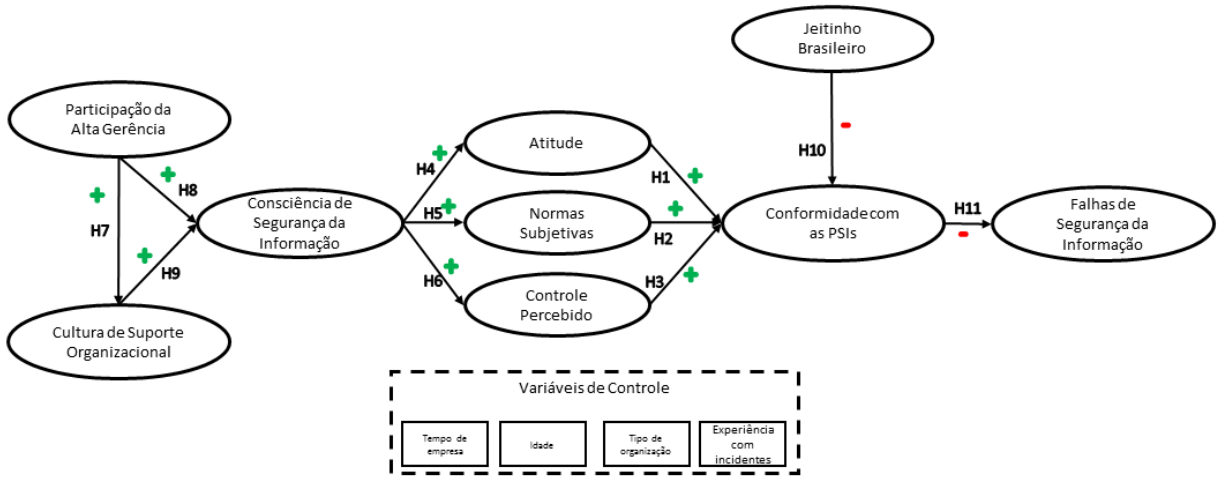
H11: A conformidade com as PSIs influencia negativamente a incidência de situações de quebra de PSIs no ambiente de trabalho

3.6 VARIÁVEIS DE CONTROLE

Incorporou-se ao modelo de pesquisa algumas variáveis de controle, como a idade, o tempo de serviço na organização, o tipo de organização e a experiência prévia com incidentes de segurança da informação, variáveis estas identificadas em estudos prévios como fatores que podem influenciar aspectos do comportamento relacionado à segurança da informação (MCCORMAC et al., 2017; ÖĞÜTÇÜ; TESTIK; CHOUSEINOGLOU, 2016).

O modelo proposto está representado na Figura 2. Assim, referentes aos aspectos da cultura organizacional, espera-se que a participação da alta gerência influencie a cultura de suporte em segurança da informação da organização, e que estes dois fatores organizacionais ocasionem uma maior consciência sobre segurança da informação na organização. Esta, por sua vez, influencia positivamente a atitude de conformidade, a importância da opinião de pessoas importantes através das normas subjetivas e a capacidade percebida de cumprir as PSIs, representado pelo controle percebido. Esses fatores da TPB possuem influência sobre a conformidade com as PSIs. Referente a aspectos da cultura nacional, o jeitinho relacionado à segurança da informação acaba por influenciar negativamente a conformidade com as normas. Complementarmente, espera-se que exista uma associação negativa entre o cumprimento das PSIs e as quebras de PSIs relacionadas ao jeitinho pelos funcionários pesquisados.

Figura 2 - Modelo conceitual da pesquisa



Fonte: Autoria própria

4 METODOLOGIA

Nesta seção apresenta-se o enquadramento da pesquisa, bem como os diferentes passos metodológicos seguidos no estudo, compreendendo o desenvolvimento do instrumento de pesquisa, a etapa de pré-teste e refinamento do instrumento realizado anterior ao trabalho de campo, a coleta de dados e a preparação da base de dados para posterior análise.

4.1 TIPO DE PESQUISA

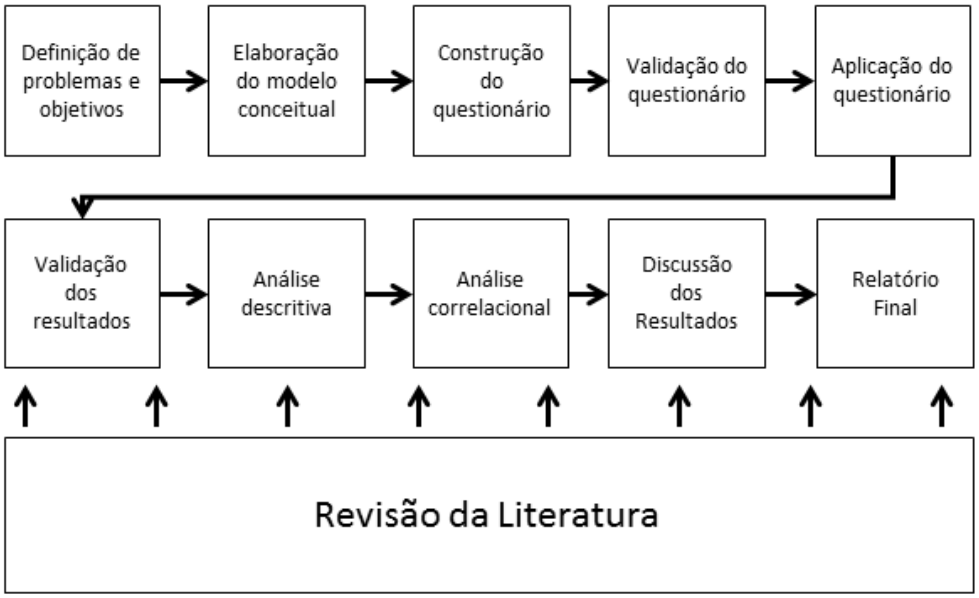
Essa pesquisa pode ser classificada como uma pesquisa de caráter exploratório, pois visa analisar um problema de pesquisa pouco estudado, especificamente no Brasil, que é a relação da conformidade com as PSIs e diferentes aspectos culturais. Também é de caráter descritivo e correlacional, pois visa especificar as propriedades e as características de um conjunto de indivíduos e organizações, além de analisar o grau de associação entre diferentes variáveis, medindo cada uma delas e analisando os vínculos existentes entre as mesmas (SAMPIERI; COLLADO; LUCIO, 2013).

De modo a se atingir os objetivos propostos neste estudo, realizou-se uma pesquisa *survey*. Este tipo de pesquisa busca produzir descrições quantitativas de aspectos específicos da população pesquisada, em que a utilização de instrumentos compostos por questões estruturadas e pré-definidas apresenta-se como a sua principal forma de coleta de dados (PINSONNEAULT; KRAEMER, 1993). Quanto ao corte da pesquisa, esta utilizou a investigação científica transversal. Uma pesquisa transversal pode ser realizada a partir da análise de um fenômeno de interesse do pesquisado, mensurando cada variável apenas uma vez, em um dado momento. Esse tipo de estudo ainda se mostra mais fácil, barato e rápido, quando comparado aos estudos de tipo longitudinal (SAMPIERI; COLLADO; LUCIO, 2013).

A Figura 3 descreve, resumidamente, o desenho metodológico da pesquisa, a qual inicia pela realização da revisão da literatura, e que acompanha todas as demais etapas do estudo, pois mesmo que se tenha realizado uma revisão específica sobre cultura e PSI, foi necessário revisar outros trabalhos científicos durante a sua execução. Com o problema de pesquisa e objetivos definidos, elaborou-se o modelo conceitual da pesquisa, juntamente com a definição das hipóteses propostas. Em seguida, desenvolveu-se o instrumento de coleta de dados – baseado em um questionário estruturado – que foi aplicado junto à amostra definida no estudo. Antes da sua aplicação, o questionário elaborado passou por duas etapas de pré-

teste, de modo a identificar possíveis fragilidades que poderiam comprometer a continuidade e a qualidade do estudo. Os resultados da aplicação do questionário foram analisados através de estatísticas descritivas e por meio da modelagem de equações estruturais, testando, assim, o modelo conceitual proposto e suas hipóteses. Após os resultados obtidos, realizou-se a discussão dos mesmos, considerando os aspectos teóricos desenvolvidos durante este trabalho e, por fim, finalizou-se este relatório com as considerações finais.

Figura 3 - Desenho de Pesquisa



Fonte: Autoria Própria

4.2 DESENVOLVIMENTO DO QUESTIONÁRIO

O questionário elaborado foi estruturado em quatro blocos. O primeiro bloco apresentava uma breve explicação sobre a pesquisa, convidando o funcionário a participar da mesma. Em seguida, duas questões eram apresentadas para identificar (1) se a empresa na qual o respondente trabalha possui normas relacionadas à segurança da informação e (2) se a empresa informa claramente essas normas aos seus funcionários. Foi utilizada uma escala Likert de 5 pontos, que variava (1) “De Maneira Nenhuma” até (5) “Muitíssimo”. No mesmo bloco, seguiram algumas questões para caracterização da amostra, em que o respondente deveria responder diferentes perguntas sociodemográficas referentes a si próprio (como idade, gênero, escolaridade, tempo de empresa, cargo, experiência com incidentes de segurança da

informação) e a organização na qual trabalha (se pública ou privada, o setor e ramo de atuação e porte).

O segundo bloco apresentava quatro questões contendo cenários hipotéticos retratando possíveis situações de falhas de segurança da informação relacionadas com o jeitinho, seguindo a definição utilizada nesse estudo. Os cenários foram retirados do estudo de Silveira et al. (2019), os quais foram adaptados para o contexto dessa pesquisa. Assim, para a criação, desenvolvimento e definição dos cenários utilizados na pesquisa, seguiram-se os seguintes preceitos:

(i) o cenário deveria descrever a função de um funcionário qualquer em uma empresa;

(ii) o cenário deveria retratar uma tarefa que precisasse ser realizada, mas era impossibilitada por falta de recursos;

(iii) a tarefa deveria afetar não somente o funcionário em si, mas seus colegas e o andamento do trabalho;

(iv) definia-se no cenário que a Política de Segurança da Informação proibia a prática específica; e

(v) o funcionário estaria quebrando a política para executar o trabalho necessário.

Esses preceitos foram definidos, pois corresponderiam aos aspectos do jeitinho, associados ao cumprimento ou não das PSIs, conforme estabelecido no referencial teórico. O Quadro 1 destaca cada cenário utilizado. Diferentemente da forma como os cenários são utilizados em outras pesquisas, em que apenas um cenário é apresentado por questionário, e os mesmos são randomizados, os cenários foram utilizados para avaliar na visão dos respondentes a propensão dessas quatro práticas não recomendadas ocorrerem em seu ambiente de trabalho, testando a relação direta entre a conformidade com as PSIs e as falhas de segurança da informação, juntamente com a variável jeitinho. Duas questões operacionalizadas por uma escala Likert de 7 pontos foram utilizadas em conjunto com os cenários, a primeira perguntava “Qual a probabilidade dessa prática ocorrer em seu ambiente de trabalho?”, utilizada para formar o construto Falhas de Segurança da Informação, e a segunda “Como você considera a realidade desse cenário?”, que foi utilizada para avaliar o realismo dos cenários propostos.

Quadro 1 - Cenários hipotéticos

Cenário Proposto	Descrição do Cenário
Uso de aplicativos piratas	Paulo trabalha editando documentos importantes para sua empresa. Ele precisa editar um documento que será utilizado por seus colegas, mas a versão do seu aplicativo está muito antiga, o que está dificultando seu trabalho. A Política de Segurança da Informação proíbe o uso de aplicativos não instalados pela TI da empresa, mas Paulo consegue uma versão mais atual do aplicativo, instala no seu computador e termina a edição dos documentos.
Uso de sites não confiáveis	Flávia necessita gerar um arquivo pdf construído a partir de outros documentos, sendo estes sigilosos para sua empresa, de modo que seus colegas possam consultar essas informações rapidamente. Como a empresa não possui o software para executar essa função, Flávia usa uma aplicação online gratuita para juntar os arquivos em um arquivo único. A política de segurança da informação proíbe o uso de sites desconhecidos para atividades da empresa, mas Carla consegue gerar o arquivo único, e repassa aos seus colegas.
Uso de mídias portáteis	Rodrigo tem acesso a importantes informações da empresa em que trabalha. A empresa solicita a ele que analise algumas dessas informações com urgência, e informe aos seus colegas a conclusão da análise. Rodrigo resolve levar alguns documentos importantes em um pendrive. A política de segurança proíbe o usuário de usar informações organizacionais fora do ambiente de trabalho, mas usando os documentos do pendrive, Rodrigo consegue terminar seu trabalho durante a viagem, e repassa aos seus colegas as conclusões da análise.
Compartilhamento de senhas	Cláudia possui acesso ao computador da empresa através de uma senha de uso pessoal. Ela está no meio de uma viagem de negócios, e seus colegas precisam de um arquivo em seu computador para finalizar um relatório. A política de segurança da empresa proíbe o compartilhamento de senhas de uso pessoal, mas Cláudia compartilha a sua senha com seus colegas, que conseguem o arquivo e finalizam o trabalho.

Fonte: Autoria Própria

O terceiro bloco do instrumento apresentava 32 questões fechadas, relacionadas ao modelo proposto no estudo. A sua operacionalização também ocorreu através de uma escala Likert de 7 pontos. A escolha por essa escala se deu por acreditar-se que as situações apresentadas no instrumento seriam facilmente compreendidas pelos participantes do estudo. De acordo com Dalmoro e Vieira (2013), escalas utilizando mais pontos geralmente são indicadas quando os entrevistados dominam o assunto objeto de estudo. As questões utilizadas foram, sempre que possível, retiradas de trabalhos previamente validados sobre o tema; enquanto que nas questões referentes à Teoria do Comportamento Planejado, buscou-se um alinhamento com as considerações de Ajzen (2002).

O quarto e, último bloco, apresentava 12 questões, abordando diferentes aspectos associados ao jeitinho. O Quadro 2 apresenta os construtos utilizados na pesquisa e suas fontes. O Anexo 1 contém as questões inseridas no questionário proposto.

Quadro 2 - Construtos e suas definições

Construto	Definição	Fonte
Participação da Alta Gerência	A importância da segurança da informação para a alta gestão que se reflete em mecanismos favoráveis à segurança da informação na organização	HU et al (2012); THOMSON; VON SOLMS (2006)
Cultura Organizacional de Suporte de Segurança da Informação	O suporte que a organização oferece através de atividades como treinamentos, PSIs claras e de fácil entendimento.	DA VEIGA; MARTINS (2015).
Consciência de Segurança da Informação	A extensão em que os membros da organização compreendem a importância da segurança da informação, o nível de segurança exigido pela organização e suas responsabilidades individuais de segurança e agem em conformidade.	FLORES; EKSTEDT (2016); ALNATHEER, (2015); BULGURCU et al., (2010)
Normas Subjetivas	Pressões sociais que os indivíduos percebem para que determinado comportamento seja seguido	BULGURCU et al., (2010); AJZEN; MADDEN (1986)
Atitude	Grau em que uma pessoa tem uma avaliação favorável ou desfavorável do comportamento em questão	AMANKWA et al., (2018); BULGURCU et al., (2010); AJZEN; MADDEN (1986)
Controle Percebido	Facilidade ou dificuldade percebida de executar o comportamento	HU et al.; (2012); AJZEN; MADDEN (1986)
Conformidade com as Políticas de Segurança da Informação	O comportamental de seguir as normas de segurança da informação estabelecidas pela organização	BULGURCU et al, (2010); CRAM et al., (2019
Jeitinho Brasileiro	O contorno de regras para se alcançar um objetivo específico, no caso a resolução de problemas através da flexibilização das normas.	FERNANDES; HANASHIRO (2015)

Fonte: Autoria Própria

4.3 PRÉ-TESTE E REFINAMENTO DO INSTRUMENTO

Para obter um questionário que retrate as intenções da pesquisa, e que ao mesmo tempo seja de fácil compreensão para os respondentes, alguns ajustes foram realizados antes da sua aplicação. Uma primeira análise do questionário foi realizada por um grupo de especialistas da área de TI, familiarizados com o tema de Segurança da Informação. Foram contatados cinco especialistas, sendo três professores de pós-graduação familiarizados com a temática, um profissional de TI de uma universidade pública e um funcionário de um setor de TI de uma empresa privada. Após alguns apontamentos e sugestões levantadas pelos especialistas, o questionário sofreu modificações, tanto na sua estrutura como no enunciado das questões.

Após essa etapa, realizou-se um pré-teste com estudantes de graduação de uma instituição pública, todos funcionários de empresas públicas ou privadas – identificados pelo autor da pesquisa como indivíduos com perfis semelhantes ao almejado no estudo. A seleção dos participantes se deu pelo próprio pesquisador, o qual contatou pessoalmente cada

participante. Para participar do pré-teste, o candidato deveria trabalhar em uma empresa que possuísse normas de segurança da informação estabelecidas, e ser informado claramente sobre essas normas. Foram obtidos 20 questionários preenchidos corretamente. Verificaram-se as contribuições de cada respondente, sendo algumas sugestões de alteração em relação ao enunciado de certas questões e à estrutura do questionário. Após essa etapa, pequenos ajustes foram realizados e o questionário foi considerado apto para aplicação. O questionário utilizado no pré-teste está disponível no Anexo 2.

4.4 COLETA DE DADOS

A amostra do estudo pode ser classificada como não probabilística, por conveniência, sendo utilizada a estratégia de bola de neve para coletar os dados da pesquisa. Como perfil de respondente para compor a amostra, foram buscados indivíduos que trabalhassem em empresas que possuíssem PSIs, em maior ou menor grau. A etapa de coleta de dados ocorreu a partir da aplicação do instrumento desenvolvido na plataforma QuestionPro (Anexo 3), a qual é paga, e oferece uma gama maior de recursos de personalização do questionário e análise prévia de dados. A coleta dos dados ocorreu entre 11 de dezembro de 2019 a 28 de janeiro de 2020, via redes sociais, sendo o Facebook e o LinkedIn as plataformas utilizadas.

Foi compartilhado o link da pesquisa a diferentes grupos do Facebook, principalmente relacionados às áreas de Administração, Ciências Contábeis e também de Universidades. No LinkedIn, o link foi compartilhado no perfil do pesquisador e de outros membros do Grupo de Pesquisa ao qual o autor está vinculado. Nos dois casos, o link do questionário era acompanhado de um texto sucinto que explicava brevemente a pesquisa (Anexo 4). Nesse texto era solicitado que o participante respondesse a um questionário e, se possível, compartilhasse o link da pesquisa com a sua rede de contatos. Vale destacar que também se buscou contatar empresas que pudessem participar da pesquisa, focando-se nas instaladas na cidade de Rio Grande/RS e região, não se obtendo autorização ou interesse das mesmas em participar.

4.5 PREPARAÇÃO DA BASE DE DADOS

Após o fim da coleta dos dados, iniciou-se a preparação da base de dados utilizada para a etapa de análise. O questionário teve ao total 1795 acessos. Desses, 457 indivíduos

iniciaram o preenchimento do questionário, sendo 200 os que finalizaram o seu preenchimento. Não foram identificados respondentes repetidos, de acordo com os dados fornecidos no relatório do QuestionPro, uma vez que essa plataforma identifica o IP de cada respondente. Após a verificação dos questionários preenchidos por meio do software Excel, prosseguiu-se à etapa de purificação dos dados através do software estatístico SPSS v. 20.0. Primeiramente, foi analisada a frequência das respostas de todas as questões, para verificar se alguma possuía muitas respostas em branco ou com pouca variação nos pontos da escala utilizada. Nessa etapa não foram encontrados problemas.

Após, realizou-se a transposição da Matriz, onde se invertem os respondentes com as variáveis. Assim, realiza-se a análise de frequência referente às respostas de cada participante, verificando a sua dispersão e o número de respostas em branco, o que permite identificar possíveis *outliers*. Quatro respondentes foram eliminados, um por excesso de respostas em branco e os demais por utilizarem apenas um ponto da escala Likert para responder todas as questões do questionário. Ao final, foram consideradas válidas as respostas de 196 respondentes.

Para estimar se o tamanho final da amostra seria suficiente para utilizar o software SmartPLS, utilizou-se o software GPower, considerando como parâmetro o construto que possui o maior número de preditores (RINGLE.; DA SILVA; BIDO, 2014). No caso dessa pesquisa, o construto Conformidade com as Políticas de Segurança da Informação (CPS) foi o maior, possuindo quatro questões. Utilizou-se essa análise a priori para verificar se a amostra alcançada atendia os valores sugeridos pela literatura. Considerando o tamanho do efeito médio do f^2 (0,15), em uma margem de confiança de 95%, obteve-se como valor mínimo de casos uma amostra de pelo menos 129 respondentes. Esse resultado sugere que a amostra total do estudo é adequada para a etapa de análise dos resultados, os quais são apresentados a seguir.

5 RESULTADOS

Este capítulo apresenta os resultados da pesquisa, destacando primeiramente (i) a caracterização da amostra, através de estatísticas descritivas; seguido pela (ii) validação dos construtos utilizados no estudo, através da análise fatorial exploratória realizada no software SPSS v. 20.0; e finalizando com a (iii) análise correlacional, realizada por meio do software SmartPLS 3.0.

5.1 CARACTERIZAÇÃO DA AMOSTRA

Utilizou-se a análise descritiva como forma de caracterizar a amostra do estudo. Juntamente com as informações sociodemográficas, foram analisadas algumas informações referentes à segurança da informação e aos cenários utilizados no estudo.

5.1.2 Perfil dos respondentes

A amostra final da pesquisa é composta por 196 respondentes, sendo a maioria do gênero feminino (54,1%), com idade entre 31 e 45 anos (51,5%) e com pós-graduação completa (38,8%). Isso indica que a amostra é composta por pessoas com um nível educacional acima da média. Quanto ao nível hierárquico do cargo dos respondentes, a maioria se concentra no nível operacional (59,2%), e quanto ao tempo no qual trabalham nessas empresas, destaca-se que a maior parte trabalha entre 5 e 10 anos (26,5%), e a segunda maior parcela trabalha entre 1 e 3 anos (20,4%). A Tabela 1 especifica esses resultados.

Tabela 1 - Características dos respondentes

Descrição	Frequência	%
Gênero		
Masculino	89	45,4
Feminino	106	54,1
Não respondeu	1	,5
Idade		
Entre 18 e 30	65	33,2
Entre 31 e 45	101	51,5
Entre 46 e 60	26	13,3
Acima de 60	2	1,0
Não respondeu	2	1,0
Escolaridade		
Ensino Médio Completo	7	3,6
Ensino Superior Incompleto	46	23,5
Ensino Superior Completo	52	26,5

Descrição	Frequência	%
Pós-Graduação Incompleta	14	7,1
Pós-Graduação Completa	76	38,8
Não respondeu	1	,5
Nível de Cargo		
Operacional	116	59,2
Supervisão	33	16,8
Gerência	25	12,8
Direção	19	9,7
Não respondeu	3	1,5
Tempo de Empresa		
Até 6 meses	16	8,2
mais de 6 meses até 1 ano	23	11,7
mais de 1 ano até 3 anos	40	20,4
mais de 3 anos até 5 anos	29	14,8
mais de 5 anos até 10 anos	52	26,5
mais de 10 anos	35	17,9
Não respondeu	1	,5

Fonte: Autoria Própria

Referente às informações fornecidas sobre as empresas em que os respondentes trabalham, a maioria afirmou trabalhar em organizações privadas (58,7%), no setor de serviços (69,4%), em organizações com mais de 499 empregados (41,3%), sendo em sua maioria organizações de grande porte. A Tabela 2 apresenta essas informações de forma mais detalhada.

Tabela 2 - Características das organizações de atuação dos respondentes

Variável	Frequência	%
Tipo de Empresa		
Pública	80	40,8
Privada	115	58,7
Não respondeu	1	,5
Setor Principal		
Indústria	26	13,3
Comércio	29	14,8
Serviços	136	69,4
Agronegócio	3	1,5
Não respondeu	2	1,0
Número de Empregados		
Até 19	40	20,4
de 20 a 99	35	17,9
100 a 499	38	19,4
Mais de 499	81	41,3
Não respondeu	2	1,0
Total	**196**	**100,0**

Fonte: Autoria Própria

Quanto à localidade em que os respondentes trabalham, 58 são da cidade de Rio Grande/RS (29,6%), seguido de Porto Alegre/RS com 16 respondentes (8,2%) e Pelotas/RS com 15 (7,75%). Também se destacam entre as cidades com maior número de respondentes Manaus/AM e São Paulo/SP, cada uma com oito respondentes (4,1% cada), e Rio de Janeiro/RJ e Santa Cruz do Sul/RS com sete respondentes (3,6% cada). Referente ao estado no qual os respondentes trabalham, 111 (56,6%) trabalham no Rio Grande do Sul, 19 (9,7%) no estado de São Paulo e 11 (5,6%) no estado do Rio de Janeiro. Dos 26 estados, mais o Distrito Federal, obtiveram-se respostas de 21 diferentes estados, demonstrando a diversidade de respondentes.

5.1.2 Características da amostra em relação às Políticas de Segurança da Informação e Situações de vulnerabilidade

Quanto às características da amostra relacionadas à segurança da informação, no primeiro momento se questionou sobre a existência de regras de segurança nas empresas que os respondentes trabalhavam e, em seguida, se essas regras eram bem informadas. A Tabela 3 apresenta as respostas referentes a estas duas questões.

Tabela 3 – Presença de Políticas de Segurança da Informação

A empresa em que você trabalha possui regras definidas quanto ao uso dos componentes de TI (como computadores, impressoras e sistemas da empresa), visando a segurança das informações da empresa?	**Frequência**	**%**
Muitíssimo	29	14,8
Muito	51	26,0
Moderadamente	55	28,1
Um pouco	34	17,3
De maneira nenhuma	27	13,8
Total	**196**	**100,0**
A empresa em que você trabalha informa claramente aos seus funcionários as regras de segurança da informação?	**Frequência**	**%**
Muitíssimo	23	11,7
Muito	37	18,9
Moderadamente	47	24,0
Um pouco	48	24,5
De maneira nenhuma	41	20,9
Total	**196**	**100,0**

Fonte: Autoria Própria

Percebe-se que o maior grupo de respondentes afirma que as empresas em que trabalham possuem PSIs de forma moderada (28,1%) ou muito presentes (26%). Os resultados sugerem que para a maioria dos respondentes as empresas nas quais trabalham

possuem PSIs definidas. Entretanto, quando questionados se essas PSIs são informadas claramente, o maior grupo (24,5%) considera que ocorre pouco ou moderadamente (24%). Destaca-se aqui um terceiro grupo, que considera que a sua empresa não informa claramente suas PSIs (20,9%). Percebe-se que, de maneira geral, as organizações da amostra possuem PSIs, mas não as informam claramente aos seus funcionários. Destaca-se que uma PSI só é efetiva quando é passada aos seus funcionários, através de treinamentos, por exemplo (DA VEIGA; ELOFF, 2015).

Também se perguntou aos respondentes sobre a experiência prévia do indivíduo e de sua empresa com problemas envolvendo falhas de segurança da informação. A maioria dos respondentes alegou nunca ter passado por problemas de segurança, tanto nas empresas em que trabalham (62,2%) como na sua vida pessoal (72,4%). Percebe-se que, de acordo com os respondentes, os problemas relacionados à segurança da informação parecem ser mais comuns no ambiente de trabalho do que no uso pessoal da tecnologia.

Tabela 4 – Experiências prévias com falhas/quebras de Segurança da Informação

Já passou por algum problema de segurança da informação na empresa em que trabalha (por exemplo, perda/roubo de informação, HD ou servidor danificado, etc.)?	Frequência	%
Sim	73	37,2
Não	122	62,2
Não respondeu	1	0,5
Total	196	100,0
E já passou por algum problema relacionado à segurança da informação que afetasse sua vida pessoalmente, fora da empresa?	Frequência	%
Sim	51	26,0
Não	142	72,4
Não respondeu	3	1,5
Total	196	100,0

Fonte: Autoria Própria

5.1.3 Análise dos Cenários

De modo a se analisar os cenários referentes a possíveis quebras de segurança da informação, perguntou-se aos respondentes o quão realistas os mesmos consideravam cada cenário e qual a probabilidade de os mesmos ocorrerem em suas organizações. Para isso, utilizou-se a média e o desvio-padrão. A Tabela 5 analisa o realismo de cada cenário elaborado.

Tabela 5 - Realidade Percebida dos Cenários

Cenário	n	Mínimo	Máximo	Média	Desvio-Padrão
Uso de aplicativos não instalados pela TI	191	1	7	4,70	1,98
Uso de senha de colegas	193	1	7	5,39	1,81
Uso de pendrive para transferência de informações organizacionais	192	1	7	5,06	1,83
Uso de sites não confiáveis para atividades da empresa	186	1	7	4,94	1,97
Média	**196**			**5,02**	**1,90**

Fonte: Autoria Própria

Os resultados sugerem que os cenários propostos foram considerados realistas pelos respondentes, com uma média geral de 5,02, acima do ponto médio da escala utilizada (4). O cenário referente ao uso da senha de colegas apresentou a maior média (5,39), enquanto o cenário referente ao uso de aplicativos não instalados pela TI apresentou a menor média (4,70).

Quanto à probabilidade dessas falhas de segurança da informação – associadas ao jeitinho – acontecerem nas empresas em que os respondentes trabalham, a média geral dos quatro cenários ficou em 4,51, também acima do ponto médio da escala utilizada. A probabilidade de falha considerada mais alta foi a de uso de senhas de colegas (5,06), indicando que para os respondentes é alta a probabilidade de compartilhamento de senhas de uso pessoal em seu ambiente de trabalho para a resolução de tarefas. Já a de menor probabilidade foi o uso de aplicativos não instalados pela TI (3,82). Analisando-se a descrição dos dois cenários, percebe-se que o de maior média, referente à probabilidade de compartilhamento de senhas, depende apenas dos usuários de sistemas para ocorrer, enquanto que o uso de aplicativos não instalados pela TI perpassa por outros envolvidos, como o próprio hardware e o acesso a privilégios de máquina, por exemplo, demonstrando que falhas de segurança da informação relacionadas ao jeitinho são mais prováveis de ocorrer quando a resolução do problema depende apenas dos indivíduos do ambiente de trabalho (Tabela 6).

Tabela 6 - Probabilidade de ocorrência de Falhas de Segurança da Informação

Cenário	n	Mínimo	Máximo	Média	Desvio-Padrão
Uso de aplicativos não instalados pela TI	193	1	7	3,82	2,367
Uso de senha de colegas	196	1	7	5,06	2,139
Uso de pendrive para transferência de informações organizacionais	195	1	7	4,77	2,178
Uso de sites não confiáveis para atividades da empresa	192	1	7	4,40	2,311
Média	**196**			**4,51**	**2,249**

Fonte: Autoria Própria

5.2 VALIDAÇÃO DO INSTRUMENTO

Referente à validação dos construtos presentes no instrumento de pesquisa, optou-se por iniciá-la pela análise fatorial exploratória (AFE). Essa técnica foi utilizada com o objetivo de confirmar a formação original dos construtos do modelo de pesquisa, observando-se a sua unidimensionalidade ou multidimensionalidade dos construtos, suas comunalidades e cargas fatoriais. Foram definidos como valores aceitáveis comunalidades com valores superiores a 0,50 e cargas fatoriais acima de 0,60. Complementarmente, utilizou-se o cálculo do Alfa de Cronbach como forma de verificar a confiabilidade de cada escala utilizada, considerando-se um coeficiente acima de 0,70 como o adequado. De modo a facilitar a interpretação dos resultados da análise fatorial, em especial aqueles construtos multidimensionais, foi utilizada a rotação Varimax.

Inicialmente, buscou-se validar o construto denominado Falhas de Segurança da Informação (FSI), o qual é formado pelas questões referentes à probabilidade de as falhas descritas nos cenários hipotéticos ocorrerem. A AFE com as variáveis P1, P2, P3 e P4 indicou a formação de apenas um fator, apresentando todas as cargas fatoriais valores acima de 0,60. Já a comunalidade da variável P2 - referente ao uso de senhas compartilhadas no ambiente de trabalho - apresentou valor 0,410, abaixo do recomendado de 0,50, optando-se pela sua remoção das análises seguintes. Uma nova AFE foi realizada e todos os índices de qualidade da escala foram atendidos, com as comunalidades acima de 0,50 e as cargas fatoriais ultrapassando 0,70. A Tabela 7 apresenta a formação final do construto Falhas de Segurança da Informação (FSI).

Tabela 7 - Construto Falhas de Segurança da Informação

Construto	**Variável**	**Descrição**	**Carga Fatorial**
Falhas de Segurança da Informação	P1	Uso de aplicativos não instalados pela TI	0,828
	P3	Uso de pendrive para transferência de informações organizacionais	0,806
	P4	Uso de sites não confiáveis para atividades da empresa	0,752
Variância Explicada - Rotacionada (%) - 63,375			
Alfa de Cronbach			0,71
KMO (Medida de Adequação da Amostra)			0,664
Teste de Bartlet			sig. 0,000

Fonte: Autoria Própria

Referente ao construto Conformidade com as Políticas de Segurança da Informação (CPS), a AFE indicou que as variáveis correspondem a um único construto, atendendo todos

os coeficientes de qualidade, com as comunalidades acima de 0,50. Em relação à análise de médias e desvio-padrão, a média geral ficou em 5,74, considerada alta, e desvio-padrão médio de 1,42. Estes resultados indicam que, de modo geral, os respondentes cumprem as políticas de segurança da informação nas organizações em que trabalham (Tabela 8).

Tabela 8 - Construto Conformidade com as PSIs

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Conformidade com as Políticas de Segurança da Informação	CPS1	Eu cumpro com as normas de segurança da informação da empresa.	0,862	5,84	1,39
	CPS2	Eu sigo as normas de segurança da informação da empresa.	0,887	5,84	1,33
	CPS3	Estou certo de que cumpro as normas de segurança da informação da empresa.	0,916	5,72	1,42
	CPS4	Eu obedeço as regras de segurança da informação da empresa.	0,842	5,58	1,54
Variância Explicada - Rotacionada (%) - 80,35			**Geral**	5,74	1,42
Alfa de Cronbach					0,71
KMO (Medida de Adequação da Amostra)					0,84
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Em relação ao construto Atitude de Conformidade com as PSIs (ATI), o mesmo formou um único fator, apresentando também bons índices de qualidade. Quanto às médias das variáveis, estas ficaram altas, com uma média geral igual a 6,36 e com um desvio padrão baixo, com média de 1,17, evidenciando que os respondentes percebem que seguir as regras de segurança da informação estipuladas pela organização é importante (Tabela 9).

Tabela 9 - Construto Atitude de Conformidade com as PSIs

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-padrão
Atitude de Conformidade com as PSIs	ATI1	Para mim, cumprir os requisitos de segurança da informação estabelecidos pela empresa é necessário.	0,908	6,26	1,04
	ATI3	Para mim, cumprir com as regras de segurança da informação determinadas pela empresa é importante.	0,907	6,21	1,02
	ATI4	Para mim, praticar as normas de segurança da informação estabelecidas pela empresa é adequado.	0,897	6,09	1,30
	ATI2	Para mim, seguir as normas de segurança da informação de acordo com a empresa é benéfico.	0,874	5,97	1,31
Variância Explicada - Rotacionada (%) - 74,93			**Geral**	6,14	1,17
Alfa de Cronbach					0,89
KMO (Medida de Adequação da Amostra)					0,84
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Sobre as normas subjetivas (NSU), a AFE apontou o agrupamento das variáveis em um construto, sendo todos os coeficientes de qualidade atendidos. Em relação às médias das

variáveis, todas ficaram altas, com uma média geral de 5,71, demonstrando que para os respondentes as colocações sobre segurança da informação por pessoas que as mesmas consideram importantes são consideradas de forma intensa (Tabela 10).

Tabela 10 - Construto Normas Subjetivas

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Normas Subjetivas	NSU4	As pessoas que eu respeito na empresa pensam que eu devo seguir as normas de segurança da informação.	0,930	5,48	1,56
	NSU1	Pessoas que são influentes para mim na empresa acham que eu devo seguir as regras relacionadas à segurança da informação.	0,914	5,93	1,45
	NSU2	Pessoas importantes na empresa possuem opiniões que eu valorizo sobre as normas de segurança da informação.	0,883	5,75	1,54
	NSU3	Pessoas que são importantes para mim na empresa pensam que eu devo seguir as políticas de segurança da informação.	0,747	5,67	1,57
Variância Explicada - Rotacionada (%) - 75,93			**Geral**	5,71	1,53
Alfa de Cronbach					0,89
KMO (Medida de Adequação da Amostra)					0,803
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Referente ao Controle Percebido para seguir as PSIs (COP), a AFE também indicou a formação de um único construto; todos os índices de qualidade foram atendidos. Em relação às médias das variáveis, a média geral ficou em 5,60, com desvio-padrão de 1,58, indicando que os respondentes percebem que possuem capacidade para seguir as PSIs das organizações em que trabalham (Tabela 11).

Tabela 11 - Construto Controle Percebido

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Controle Percebido	COP3	Eu tenho recursos e conhecimento para seguir as normas de segurança da informação disponibilizadas pela minha empresa.	0,865	6,11	1,30
	COP4	Possuo as habilidades necessárias para seguir as regras de segurança da informação da minha empresa.	0,834	4,88	1,93
	COP1	Eu sou capaz de seguir as regras de segurança da informação estabelecidas pela minha empresa.	0,822	5,78	1,45
	COP2	Tenho treinamento e habilidades adequadas para seguir as normas de segurança da informação definidos pela minha empresa.	0,733	5,62	1,63
Variância Explicada - Rotacionada (%) - 6,43			**Geral**	5,60	1,58
Alfa de Cronbach					0,82
KMO (Medida de Adequação da Amostra)					0,786
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Para o construto Consciência de Segurança da Informação (CSI), a análise fatorial exploratória também indicou a existência de um único fator. Com relação aos indicadores de qualidade, apenas a comunalidade da variável CSI2 ficou abaixo do recomendado de 0,50 (0,426); entretanto, como a sua carga fatorial ultrapassou o limite mínimo de 0,60, optou-se por mantê-la na formação do construto original. Quanto às médias das variáveis, a média geral do construto ficou bem elevada, apresentando valor 6,05 (Tabela 12).

Tabela 12 - Construto Consciência de Segurança da Informação

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Consciência de Segurança da Informação	CSI3	Eu compreendo os riscos relacionados à segurança da informação para a empresa.	0,848	6,34	0,95
	CSI4	Eu entendo as preocupações em relação à segurança da informação e os riscos que elas representam em geral.	0,653	6,36	1,11
	CSI1	No geral, estou ciente das possíveis ameaças à segurança e suas consequências negativas à empresa.	0,775	6,06	1,28
	CSI2	Eu tenho conhecimento suficiente sobre o custo de possíveis problemas de segurança da informação para a empresa.	0,777	5,42	1,67
Variância Explicada - Rotacionada (%) - 58,776			**Geral**	6,05	1,25
Alfa de Cronbach					0,73
KMO (Medida de Adequação da Amostra)					0,757
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Para o construto Suporte da Cultura de Segurança da Informação (SCS), os resultados da AFE confirmaram a formação de um único construto, atendendo a todos os critérios de qualidade. Já a média geral do construto ficou em 4,57, apresentando um valor bem inferior se comparado à média dos outros construtos do modelo. A questão SCS1, por exemplo, apresentou média igual a 3,52 e desvio-padrão 2,15, o que indica que em relação a treinamentos, existe uma diferença maior de percepção entre as organizações que os respondentes trabalham, cuja percepção geral ficou abaixo do ponto médio da escala utilizada (Tabela 13).

Tabela 13 - Construto Suporte da Cultura de Segurança

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Suporte de Cultura de Segurança da Informação	SCS3	Incidentes com vazamento de informações são evitados porque a empresa em que trabalho se preocupa com isso.	0,796	4,74	1,89
	SCS1	A empresa em que trabalho oferece treinamentos que visam melhorar as questões relacionadas à segurança da informação.	0,809	3,52	2,15
	SCS4	A empresa em que trabalho se preocupa com as questões relacionadas à segurança da informação.	0,853	5,27	1,90
	SCS2	Programas de conscientização e treinamento enfatizam a importância da segurança da informação na empresa.	0,739	4,75	2,12
Variância Explicada - Rotacionada (%) - 64,07			**Geral**	4,57	2,01
Alfa de Cronbach					0,81
KMO (Medida de Adequação da Amostra)					0,728
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Em relação ao construto Participação da Alta Gerência, os procedimentos realizados na sua validação foram diferentes. Realizou-se a AFE, mas a questão ALG1 apresentou uma baixa comunalidade (0,332), além da sua carga fatorial também apresentar valor abaixo do esperado de 0,60 (0,576). Por isso, optou-se pela sua exclusão. Realizou-se uma nova AFE, na qual todos os parâmetros de qualidade do construto foram atendidos. Em relação à média geral, essa apresentou valor 4,83, com um desvio-padrão de 1,92, o que demonstra que existem diferenças quanto ao padrão de resposta dos respondentes (Tabela 14).

Tabela 14 - Construto Participação da Alta Gerência

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Participação da Alta Gerência	ALG3	O suporte da alta gerência para a segurança da informação é claro.	0,924	4,47	1,96
	ALG2	A alta gerência considera a segurança da informação uma importante prioridade da empresa.	0,913	5,09	1,94
	ALG4	As palavras e ações da alta gerência demonstram que a segurança da informação é uma prioridade para a empresa.	0,912	4,95	1,87
Variância Explicada - Rotacionada (%) - 83,97			**Geral**	4,83	1,92
Alfa de Cronbach					0,90
KMO (Medida de Adequação da Amostra)					0,754
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Seguindo as próprias indicações de Fernandes e Hanashiro (2015), referentes ao construto Jeitinho, foram incluídas duas novas questões às três dimensões originais. Devido a essas modificações e ao caráter multidimensional do construto, é pertinente realizar a AFE de modo a verificar se a formação original das questões se mantém a mesma ou acabou se

modificando. Primeiramente, executou-se a AFE incluindo-se todas as 12 questões utilizadas na quarta parte do questionário. Nessa análise, as questões se agruparam em dois blocos, diferentemente do proposto pela pesquisa de Fernandes e Hanashiro (2015). O primeiro bloco foi formado pelas questões JB35, JB36, JB42, JB34, JB38, JB43, JB33 e JB40, e o segundo pelas questões JB37, JB41, JB44, JB39.

Verificou-se que duas questões não apresentaram validade discriminante entre os blocos, em que as cargas fatoriais das variáveis JB44 e JB39 - variáveis do segundo fator – apresentaram cargas muito altas no primeiro fator. Assim, optou-se pela exclusão das duas questões, realizando-se uma nova AFE. As variáveis se agruparam novamente em dois fatores, sendo o primeiro formado pelas variáveis JB35, JB36, JB42, JB34, JB38, JB43, JB33 e JB40, e o segundo pelas questões JB37 e JB41. Por escolha do pesquisador, optou-se por excluir a variável JB41, pois esta apresentava uma carga fatorial muito elevada no segundo fator, formado apenas por duas questões, enquanto que a questão JB37 apresentou uma carga fatorial moderada também no primeiro fator. Assim, calculou-se a AFE pela terceira vez e o resultado final foi a formação de apenas um fator, formado pelas questões JB33, JB34, JB35, JB36, JB37, JB38, JB40, JB42 e JB43. Ao se verificarem as comunalidades, identificou-se que a questão JB37 apresentou valor 0,251, muito abaixo do recomendado. Assim, optou-se também pela sua exclusão, executando-se a AFE pela quarta vez. O fator formado agrupou as variáveis JB33, JB34, JB35, JB36, JB38, JB40, JB42 e JB43 em um único fator, com suas comunalidades acima de 0,50 e cargas fatoriais superiores a 0,60. Ao final, verificou-se a confiabilidade da escala através do cálculo do alfa de Cronbach, o qual apresentou valor igual a 0,93.

Os resultados da análise fatorial exploratória indicaram que, diferentemente do sugerido por Fernandes e Hanashiro (2015), quando o jeitinho é contextualizado na área de segurança da informação, não existe a percepção de múltiplas dimensões, mas apenas uma, a qual engloba as três principais características do jeitinho: a resolução de problemas no dia-a-dia, o contorno das regras e a flexibilização de tarefas. Por isso, entende-se que tanto a flexibilização das normas de segurança da informação como o contorno das regras de segurança estão diretamente relacionados à resolução de problemas no ambiente de trabalho. A média do construto evidenciou uma percepção moderada da presença do jeitinho; porém, o desvio-padrão sugere uma elevada dispersão nas repostas, o que demonstra que a percepção dos respondentes quanto ao jeitinho varia de maneira intensa, não podendo observar-se um consenso geral sobre a sua presença nas organizações dos respondentes. Esses resultados

sugerem que a força que o jeitinho relacionado à segurança da informação possui nas organizações varia de acordo com cada organização, e também com cada ambiente de trabalho. A Tabela 15 apresenta os resultados finais da AFE, juntamente com a média e o desvio-padrão das questões.

Tabela 15 - Construto Jeitinho

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Percebo que na empresa em que trabalho...					
Jeitinho Brasileiro relacionado à Segurança da Informação	JB35	as regras de segurança da informação são contornadas, dependendo da situação.	0,867	4,14	2,13
	JB42	para atendimento de um pedido de ajuda, eventualmente, alguma regra de segurança da informação é contornada.	0,851	4,24	2,12
	JB38	entre o Sim e o Não, o Pode e o Não Pode, sempre existe um Talvez quando se trata de cumprir as regras de segurança da informação.	0,849	4,07	2,02
	JB34	em situações especiais para solucionar problemas, faz-se necessário adaptar-se e não cumprir com as normas de segurança da informação.	0,842	4,47	1,96
	JB40	para se resolver problemas é necessário ignorar as normas de segurança da informação.	0,828	3,73	2,13
	JB43	resolver os problemas é mais importante que seguir as normas de segurança da informação.	0,800	4,08	2,07
	JB33	frente a uma situação especial, é necessário contornar alguma regra de segurança da informação para que seja encontrada uma saída.	0,793	2,73	1,91
	JB36	as pessoas flexibilizam as normas relacionadas à segurança da informação, quando necessário.	0,760	3,78	2,00
Variância Explicada - Rotacionada (%) - 67,98			**Geral**	3,90	2,04
Alfa de Cronbach					0,93
KMO (Medida de Adequação da Amostra)					0,912
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

5.3 ANÁLISE CORRELACIONAL

Para atender o objetivo de analisar a relação entre o jeitinho e o cumprimento das PSIs, testando-se, portanto, as hipóteses propostas nesta dissertação, empregou-se a técnica de modelagem de equações estruturais, baseada na variância, através do software SmartPLS 3.0 (*Partial Least Squares*). De acordo com Hair et al. (2019), esta técnica vem sendo amplamente aplicada em várias disciplinas das Ciências Sociais, como as áreas de Sistemas de Informação e Marketing. O PLS é apropriado para aplicações de predição e construção de teoria, sendo especialmente adequado para dados que não possuem necessariamente uma distribuição normal, como exigido pelas técnicas de modelagem de equações estruturais baseadas em covariância (CHIN, 1998). Além disso, o PLS permite estimar modelos

complexos, contendo muitos construtos, itens e caminhos estruturais, sem impor suposições distributivas sobre os dados (HAIR JR. et al., 2017).

Com base nessa metodologia, os dados são analisados e interpretados em duas etapas: (1) a avaliação do modelo de mensuração e (2) a avaliação do modelo estrutural. Essa sequência tem por objetivo garantir que sejam obtidas medidas válidas e confiáveis para cada construto, antes das conclusões sobre as relações existentes entre os mesmos (CHIN, 1998; HAIR et al., 2017). Após o modelo geral ter sido avaliado e confirmado, optou-se se por realizar a análise de mediação dos construtos e definiu-se pela utilização da análise multigrupo – também conhecida como MGA (*Multi-group analysis*) – para analisar a influência das diferentes variáveis de controle incluídas no modelo.

5.3.1 Modelo de Mensuração

Para se avaliar o modelo de mensuração, foram verificadas as validades convergente, discriminante e a fidedignidade das escalas. Esta última foi avaliada através da confiabilidade composta (do inglês, *Composite Reliability* – CR) e do Alfa de Cronbach. A confiabilidade composta é preferível ao alfa de Cronbach porque oferece uma melhor estimativa da variância compartilhada pelos seus indicadores, além de utilizar as cargas dos itens obtidos em uma rede nomológica, diferentemente do alfa de Cronbach (HAIR et al., 2014). Mesmo assim, tanto os escores da confiabilidade composta como do alfa de Cronbach de todos os construtos utilizados no modelo excederam o limite mínimo de 0,70, indicando uma boa confiabilidade das escalas.

A validade convergente dos construtos foi avaliada usando-se o critério da variância média esperada (do inglês, *Average Variance Expected* – AVE), cujos valores excederam o limite mínimo de 0,50. Tanto as cargas fatoriais quanto os valores da AVE servem de base para assegurar que os construtos do modelo proposto demonstram validade convergente.

Já a validade discriminante é estabelecida quando um indicador de carga em seu construto atribuído é maior do que todas as suas cargas cruzadas com outros construtos. Espera-se que as cargas fatoriais atinjam um mínimo de 0,70 no seu respectivo fator. Destaca-se que todos os itens apresentaram elevadas cargas fatoriais (superiores ou iguais a 0,70, conforme sugere a literatura), sendo estatisticamente significativas ao nível de 5%, nos seus respectivos construtos (indicando também a confiabilidade dos itens). O critério de Fornell-Larcker também deve ser utilizado para avaliar a validade discriminante, comparando-se a

raiz quadrada dos valores da AVE com as correlações das demais variáveis latentes. Especificamente, a raiz quadrada da AVE de cada construto deve ser maior do que a sua correlação mais alta com os demais construtos, critério também atendido por este teste.

Um terceiro e último critério utilizado para avaliar a validade discriminante foi a razão multitraço-monotraço (ou HTMT), no qual se espera que a relação entre os construtos seja menor que 0,90, o qual também foi testado nesta pesquisa (HAIR et al., 2017). Identificou-se que a relação entre quatro construtos ultrapassou o limite estabelecido de 0,90, sendo a relação entre o Controle Percebido (COP) e a Consciência de Segurança da Informação (CSI) igual a 0,92 e entre a Participação da Alta Gestão (ALG) e o Suporte de Cultura de Segurança (SCS) igual a 1,00. Assim, verificaram-se novamente as cargas fatoriais das relações descritas, onde foram identificados valores muito altos entre certas variáveis nestes construtos.

Na relação entre os construtos COP e CSI, verificou-se que a variável CP1 tinha uma carga de 0,85 no construto COP e 0,73 no construto CSI. Para melhor ajuste do modelo, optou-se pela sua exclusão, sendo gerado o algoritmo PLS pela segunda vez, em que se demonstrou que após a exclusão do item a correlação entre COP e CSI ficou dentro do recomendado (0,85). Referente à relação entre ALG e SCS, verificou-se que não havia muitas diferenças entre as cargas fatoriais das variáveis de ALG no próprio construto ALG e SCS, estando todos os valores das cargas fatoriais dos itens dessas variáveis acima de 0,70, sugerindo serem um mesmo construto. Então, retornou-se ao SPSS e realizou-se uma nova AFE com os itens dos dois construtos. A análise apontou a formação de apenas um fator. Verificou-se a comunalidade e optou-se por excluir a questão SCS2 por apresentar valor inferior ao sugerido pela literatura (0,473). Novamente a AFE foi calculada e todos os critérios de qualidade foram atendidos, apresentando este novo fator um alfa de Cronbach de 0,92.

Após a avaliação do enunciado das questões, optou-se por utilizar esse novo agrupamento de variáveis como um novo construto, chamado aqui de Suporte Organizacional de Segurança da Informação, considerando para isso aspectos das próprias teorias e pesquisas que embasam essa dissertação. Em relação à Cultura Organizacional Brasileira, derivada dos estudos da cultura nacional, a presença da alta gerência nas organizações é descrita como forte, pela própria questão da tendência à hierarquização (CHU; WOOD JR, 2008), possuindo uma tendência à centralização do poder em grupos sociais com alto grau de distanciamento entre os níveis e passividade e aceitação dos grupos inferiores dentro das organizações

(BUENO; ARANTES, 2015). Sendo a sociedade brasileira descrita por Hofstede (2019) como uma sociedade que acredita que a hierarquia deve ser respeitada e as desigualdades entre as pessoas são aceitáveis, o que reflete o entendimento relacionado aos aspectos da cultura de segurança da informação, pois para os respondentes dessa pesquisa, o nível de suporte de segurança da informação que a organização possui está diretamente associada à participação da alta gerência. Treinamentos relacionados à segurança da informação e a própria preocupação que a organização demonstra ter com essas questões é associada em conjunto ao nível de investimentos realizados pela alta gerência na proteção de seus ativos organizacionais. A Tabela 16 apresenta esse resultado.

Tabela 16 - Construto Suporte Organizacional de Segurança da Informação

Construto	Variável	Descrição	Carga Fatorial	Média	Desvio-Padrão
Suporte Org. de Segurança da Informação	**ALG-2**	A alta gerência considera a segurança da informação uma importante prioridade da empresa.	0,898	5,11	1,93
	ALG-3	O suporte da alta gerência para a segurança da informação é claro.	0,885	4,49	1,95
	ALG-4	As palavras e ações da alta gerência demonstram que a segurança da informação é uma prioridade para a empresa.	0,884	4,97	1,86
	SCS-1	A empresa em que trabalho oferece treinamentos que visam melhorar as questões relacionadas à segurança da informação.	0,871	3,54	2,15
	SCS-3	Incidentes com vazamento de informações são evitados porque a empresa em que trabalho se preocupa com isso.	0,805	4,74	1,87
	SCS-4	A empresa em que trabalho se preocupa com as questões relacionadas à segurança da informação.	0,768	5,26	1,88
Variância Explicada - Rotacionada (%) - 72,79			**Geral**	4,68	1,94
Alfa de Cronbach					0,92
KMO (Medida de Adequação da Amostra)					0,904
Teste de Bartlet					sig. 0,000

Fonte: Autoria Própria

Após a definição do novo construto, retornou-se ao SmartPLS e se gerou o algoritmo pela terceira vez. Foram verificados novamente os coeficientes que garantem a qualidade do modelo. Em relação à confiabilidade das escalas, tanto o Alfa de Cronbach como a Confiabilidade Composta atenderam o mínimo esperado (0,70 e 0,80, respectivamente). A validade convergente também foi atendida, com a Variância Média Extraída - AVE acima do recomendado de 0,50 em todos os construtos. A Tabela 17 apresenta os resultados referentes à confiabilidade das variáveis do modelo.

Tabela 17 - Confiabilidade das Escalas

	Alfa de Cronbach	Alfa de Cronbach Ajustado	Confiabilidade Composta	Variância Média Extraída
ATI	0,900	0,902	0,930	0,769
COP	0,782	0,788	0,873	0,697
CPS	0,910	0,912	0,937	0,788
CSI	0,760	0,763	0,847	0,582
FSI	0,707	0,714	0,836	0,631
JB	0,931	0,934	0,943	0,675
NSU	0,883	0,914	0,920	0,744
SOS	0,920	0,934	0,938	0,717

Fonte: Autoria Própria

A validade discriminante também foi atendida, com todas as variáveis apresentando cargas fatoriais acima de 0,70 em seus respectivos construtos, sendo essa carga fatorial maior do que na relação das variáveis nos demais construtos. A Tabela de cargas fatoriais (APÊNDICE A) apresenta os resultados da Análise Fatorial Confirmatória (AFC).

Como os valores quadráticos das AVEs de todos os construtos foram superiores aos valores das suas correlações, pode-se confirmar a validade discriminante do modelo, o qual também foi atendido pelo critério de Fornell-Larcker (Tabela 18).

Tabela 18 - Critério de Fornell-Lacker

	ATI	COP	CPS	CSI	FSI	JB	NSU	SOS
ATI	**0,877**							
COP	0,503	**0,835**						
CPS	0,709	0,646	**0,888**					
CSI	0,568	0,667	0,633	**0,763**				
FSI	-0,340	-0,405	-0,517	-0,295	**0,794**			
JB	-0,419	-0,330	-0,468	-0,367	0,448	**0,822**		
NSU	0,646	0,542	0,684	0,573	-0,409	-0,321	**0,863**	
SOS	0,460	0,525	0,616	0,424	-0,491	-0,307	0,667	**0,847**

Fonte: Autoria Própria

Por fim, o critério da razão multitraço-monotraço (ou HTMT) também foi atendido, com todos os valores abaixo de 0,90, como sugerido pela literatura (HAIR JR. et al., 2017). A Tabela 19 apresenta esses resultados.

Tabela 19 - Critério da razão multitraço-monotraço (HTMT)

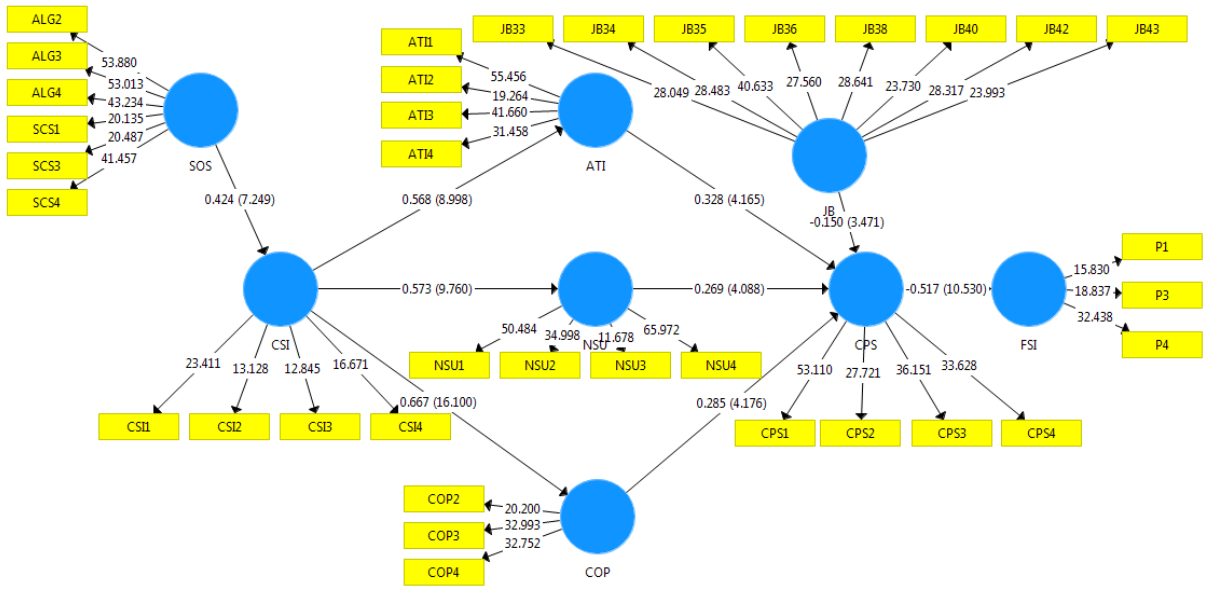
	ATI	COP	CPS	CSI	FSI	JB	NSU	SOS
ATI								
COP	0,594							
CPS	0,778	0,763						
CSI	0,683	0,854	0,747					
FSI	0,423	0,546	0,644	0,394				
JB	0,451	0,382	0,503	0,425		0,548		
NSU	0,730	0,649	0,748	0,678		0,513	0,339	
SOS	0,503	0,634	0,673	0,486		0,617	0,330	0,743

Fonte: Autoria Própria

5.3.2 Modelo Estrutural

Após assegurar-se a qualidade do modelo, utilizou-se a técnica de *bootstrapping* com 5.000 amostras para avaliar a aderência geral do modelo, bem como de seus parâmetros. Assim, são estimados os coeficientes de caminho (β) e sua significância estatística (t) para testar as hipóteses, além de serem calculados os coeficientes de determinação (R^2) das variáveis endógenas, de modo a avaliar a capacidade de previsão do modelo (Figura 4). Além disso, calculou-se o VIF para a análise de multicolinearidade; e o f^2, que mede o tamanho do efeito da variável exógena na endógena.

Figura 4 - Modelo Estrutural



Fonte: Software SmartPLS

Em relação à hipótese H1, identificou-se que a Atitude de Conformidade com as PSIs (ATI) influencia positivamente o cumprimento das PSIs (CPS), validando a hipótese (β = 0,328; ρ < 0,001). Isso significa que para os respondentes, quanto mais favorável for a sua atitude quanto ao cumprimento das normas de segurança da informação, maior será a sua conformidade com as PSIs. A Atitude é considerada na literatura como um importante antecedente do cumprimento ou intenção de cumprir com as PSIs (AMANKWA et al., 2018), sendo essa relação já estabelecida em outros estudos (IFINEDO et al., 2014, HU et al., 2012). Essa foi a relação validada mais intensa, o que significa que manter uma atitude que é importante e necessária para se adaptar a um comportamento adequado, e acreditar que a adaptação desse comportamento terá um resultado positivo parece ser mais importante para o

comportamento do que a habilidade ou pressão percebida por pessoas importantes (FLORES; EKSTEDT, 2016).

Já as Normas Subjetivas (NSU) também possuem influência positiva e significativa no cumprimento das normas de segurança da informação (CPS), validando a H2 ($\beta = 0,269$; $\rho < 0,001$). Isso significa que os respondentes consideram a opinião de pessoas importantes no seu ambiente de trabalho quando decidem por cumprir ou não as políticas de segurança da informação em suas organizações. Nesse sentido, Hu et al. (2012) destacam em sua pesquisa que como todas as perguntas foram enquadradas no contexto organizacional, a compreensão dos entrevistados sobre "pessoas importantes e influentes que respeitam" estariam em seus círculos profissionais de colegas, superiores e subordinados dentro da organização, resultando em um efeito mais forte da norma subjetiva no comportamento individual, se comparado a outros estudos (BULCURGU et al. 2010), sendo essa observação também identificada aqui.

A hipótese H3, referente à influência positiva do Controle Percebido (COP) na Conformidade com as PSIs (CPS) também foi confirmada ($\beta = 0,285$; $\rho < 0,01$), o que sugere que quanto mais capazes de seguir as regras de segurança da informação os indivíduos se sentirem, maior será a conformidade com as PSIs (HU et al., 2012; BULGURCU et al., 2010). Isso demonstra que é necessário que o funcionário perceba sua capacidade de cumprir com as normas de segurança da informação para que a conformidade com as mesmas seja efetiva. A maneira mais eficaz de conseguir isso é através de treinamento extensivo, não apenas sobre as políticas e procedimentos em si, mas também sobre as tecnologias e habilidades subjacentes para executar essas políticas e procedimentos (HU et al., 2012).

Continuando a análise do modelo, verificou-se que a Consciência de Segurança da Informação (CSI) possui uma forte influência (positiva e significativa) na Atitude de Conformidade com as PSIs (ATI), validando a hipótese H4 ($\beta = 0,568$; $\rho < 0,001$). Esse resultado foi confirmado também no estudo de Bulcurgu et al. (2010), destacando que quanto maior for a consciência do indivíduo sobre a importância da segurança da informação, maior será a sua atitude em relação à conformidade com as PSIs, tornando o cumprimento das normas como algo bem visto. Diante desse resultado, a gerência deve introduzir programas de conscientização e treinamento que enfatizem a importância do cumprimento das normas e políticas de segurança da informação. Além disso, a gerência deve definir claramente as funções e responsabilidades dos funcionários em relação à segurança da informação. A implementação dessas recomendações nutrirá, portanto, uma cultura em que os funcionários ilustrem atitudes, intenções de comportamento, suposições, crenças e valores que são

propícios para a proteção dos ativos de informação da organização (AMANKWA et al., 2018).

A hipótese H5, referente à influência positiva da Consciência de Segurança da Informação (CSI) nas Normas subjetivas (NSU) também foi confirmada ($\beta = 0{,}573$; $\rho < 0{,}001$), o que indica que a compreensão sobre a segurança da informação influencia fortemente na percepção sobre o grau que a opinião de pessoas que as mesmas consideram importantes em seu ambiente de trabalho possui. Em pesquisas realizadas nessa área, já se constatou que a importância das normas subjetivas pode variar de acordo com diferentes culturas (DINEV et al., 2009). Considerando a força das relações pessoais como forma de se adaptar a impessoalidade no ambiente de trabalho nas organizações brasileiras (FERNANDES; HANASHIRO, 2015), os funcionários quando são mais conscientes se importam mais com as opiniões de seus parceiros no trabalho sobre o cumprimento das regras, o que leva a uma maior conformidade com as PSIs.

Complementarmente, identificou-se uma associação positiva e significativa entre a Consciência de Segurança da Informação (CSI) e o Controle Percebido (COP) ($\beta = 0{,}667$; $\rho < 0{,}001$), confirmando a hipótese H6, sendo essa a relação mais forte identificada entre a consciência de segurança da informação e os construtos da TPB. Em seu estudo sobre a intenção de resistir à engenharia social, Flores e Ekstedt (2016) encontraram que quanto maior a consciência de segurança da informação, maior seria a capacidade do indivíduo de ter o comportamento desejado. Em outras palavras, quanto maior a compreensão dos indivíduos sobre os aspectos relacionados à segurança da informação na organização, mais capaz ele se sentirá para cumprir as PSIs definidas pela organização.

A relação entre o Suporte Organizacional de Segurança da Informação (SOS) e a Consciência de Segurança da Informação (CSI) também se mostrou positiva e significativa ($\beta = 0{,}424$; $\rho < 0{,}001$), validando a hipótese H7/H8. Este resultado indica que o apoio e o suporte que a organização oferece para a segurança da informação, através de atividades como treinamentos, por exemplo, auxilia no desenvolvimento da consciência dos funcionários sobre os riscos relacionados ao não cumprimento das PSIs. Ao se considerar a cultura organizacional brasileira, percebe-se que as ações da alta gerência refletem diretamente no comportamento dos indivíduos dentro do ambiente organizacional, e isso se deve ao distanciamento entre os níveis dentro da organização, centralizando as decisões referentes à empresa (BUENO; ARANTES, 2015). Se a Alta Gerência da organização investe em

segurança da informação, isso se reflete no suporte que o funcionário percebe ter, através de ações como treinamentos e PSIs que sejam de fácil entendimento.

Já a influência negativa do jeitinho (JB) no cumprimento das PSIs (CPS) também foi confirmada (β = -0,150; ρ < 0,001), validando a hipótese H10. Esse resultado demonstra que as metas e objetivos de segurança da informação precisariam estar alinhados à cultura organizacional formal e à cultura nacional (SHERIF; FURNELL; CLARKE, 2015). Assim, a carga cultural que o indivíduo possui, em conflito com a cultura de segurança da informação desenvolvida pela organização, influencia em conjunto o comportamento do indivíduo – no caso dessa pesquisa, o cumprimento das normas de segurança da informação. Se os programas de segurança forem vistos como obstáculos no dia a dia dos funcionários, estes podem influenciar comportamentos negativos (GLASPIE; KARWOWSKI, 2017). Então, é necessário que o fluxo de trabalho dos indivíduos não seja prejudicado por PSIs que não correspondam a essa realidade. Complementando, o jeitinho exerce influência, ainda que pequena, sobre o cumprimento das normas de segurança da informação, ou seja, mesmo que compreendido e utilizado principalmente como meio para resolução de problemas, o jeitinho influencia negativamente a conformidade com as normas e políticas de segurança da informação, pois no momento que os funcionários optam pelo uso da pessoalidade como meio de burlar as normas, utilizam essa estratégia para suavizar as relações de impessoalidade (ISLAM, 2012).

Por fim, confirmou-se a hipótese H11, sobre a influência da Conformidade com as PSIs (CPS) nas Falhas de Segurança da Informação (FSI), em que se identificou uma forte correlação negativa e significativa (β = -0,517; ρ < 0,001). O resultado indica que seguir as normas de segurança da informação estabelecidas pela organização diminui a ocorrência de falhas que podem ser prejudiciais à organização, pois os funcionários tendem a se policiar quanto ao cumprimento das PSIs (GLASPIE; KARWOWSKI, 2017), o que só será alcançado através de uma cultura de segurança da informação forte e consolidada. As falhas relacionadas ao jeitinho são diminuídas a partir do momento em que a cultura da organização está voltada para a segurança da informação, mesmo que seja influenciada por aspectos da cultura nacional (LEIDNER; KAYWORTH, 2006; GALLIVAN; SRITE, 2005), como o jeitinho.

Em conjunto, os construtos Atitude, Normas Subjetivas, Controle Percebido e Jeitinho Brasileiro explicam 67,1% (R^2 = 0,671) da variância do construto Conformidade com as PSIs, o que pode ser considerado um valor bastante alto (COHEN, 1988). Já a Conformidade com

as PSIs explica 26,7% da variância do construto Falhas de Segurança da Informação (R^2 = 0,267), o que pode ser considerado de médio impacto (COHEN, 1988). Sobre o ajuste do modelo, calculado pelo VIF (o qual avalia o grau de multicolinearidade dos construtos), todos eles apresentaram valores dentro do recomendado, abaixo de 3 (DIAMANTOPOULOS; SIGUAW, 2006), indicando que não existem problemas significativos de multicolinearidade em relação aos dados, da mesma forma que não foi detectado qualquer viés comum do método aparente.

Quanto ao tamanho do efeito das variáveis exógenas nas endógenas (COHEN, 1988), o valor do f^2 foi pequeno para as relações entre as Normas Subjetivas e o cumprimento das PSIs (f^2 = 0,114), e na relação entre o jeitinho e o cumprimento (f^2 = 0,055). Já para as relações entre a Atitude (f^2 = 0,168) e o Controle Percebido (f^2 = 0,162) com a Conformidade, e na relação entre o Suporte Organizacional e a Consciência sobre a Segurança da Informação (f^2= 0,219), o tamanho do efeito foi médio. Nas relações da Consciência com os construtos da TPB (Atitude, f^2 = 0,475; Normas Subjetivas, f^2 = 0,489; e Controle Percebido, f^2 = 0,802) e a relação entre os construtos Conformidade e Falhas de Segurança (f^2 = 0,365), os efeitos identificados foram grandes. A Tabela 20 destaca os resultados do modelo proposto.

Tabela 20 - Resultados do Modelo Conceitual da pesquisa

Relacionamentos	Hipótese	VIF	f^2	Coeficiente	t-valor	p-valor	R^2
ATI → CPS	H1	1,950	0,168	0,328	4,165	0,000	0,671
COP → CPS	H3	1,530	0,162	0,285	4,176	0,000	
JB → CPS	H10	1,242	0,055	-0,150	3,471	0,001	
NSU → CPS	H2	1,926	0,114	0,269	4,088	0,000	
CPS → FSI	H11	1,000	0,365	-0,517	10,530	0,000	0,267
CSI → ATI	H4	1,000	0,475	0,568	8,998	0,000	0,322
CSI → COP	H6	1,000	0,802	0,667	16,100	0,000	0,445
CSI → NSU	H5	1,000	0,489	0,573	9,760	0,000	0,328
SOS → CSI	H8/H9	1,000	0,219	0,424	7,249	0,000	0,180

Fonte: Autoria Própria

5.3.3 Análise da Mediação dos Construtos

Para analisar o efeito da mediação dos diferentes construtos presentes no modelo, verificaram-se os efeitos diretos e indiretos totais (Tabela 21). Para isso, considera-se que a mediação é total quando o efeito indireto é significante e o efeito direto é nulo; e parcial quando o efeito indireto e o direto são significativos, a um nível de 95% (BIDO; SILVA, 2019). Os resultados deste teste demonstraram que os efeitos nas relações entre os construtos

foram todos parciais, uma vez que tanto os efeitos diretos quanto indiretos foram significativos ($p < 0,05$).

Tabela 21 - Análise dos efeitos de mediação

Relacionamentos	Coeficiente	Erro padrão	Valor-t	Valor-p
SOS → CSI → ATI	0,241	0,046	5,221	**0,000**
SOS → CSI → COP	0,283	0,049	5,826	**0,000**
CSI → ATI → CPS	0,186	0,050	3,738	**0,000**
SOS → CSI → ATI → CPS	0,079	0,025	3,160	**0,002**
CSI → COP → CPS	0,190	0,048	3,959	**0,000**
SOS → CSI → COP → CPS	0,081	0,026	3,131	**0,002**
CSI → JB → CPS	0,055	0,020	2,751	**0,006**
SOS → CSI → JB → CPS	0,023	0,009	2,496	**0,013**
CSI → NSU → CPS	0,154	0,040	3,865	**0,000**
SOS → CSI → NSU → CPS	0,065	0,020	3,207	**0,001**
ATI → CPS → FSI	-0,170	0,042	4,028	**0,000**
CSI → ATI → CPS → FSI	-0,096	0,026	3,653	**0,000**
SOS → CSI → ATI → CPS → FSI	-0,041	0,013	3,033	**0,002**
COP → CPS → FSI	-0,148	0,039	3,788	**0,000**
CSI → COP → CPS → FSI	-0,098	0,028	3,574	**0,000**
SOS → CSI → COP → CPS → FSI	-0,042	0,015	2,846	**0,004**
JB → CPS → FSI	0,078	0,025	3,108	**0,002**
CSI → JB → CPS → FSI	-0,029	0,011	2,515	**0,012**
SOS → CSI → JB → CPS → FSI	-0,012	0,005	2,269	**0,023**
NSU → CPS → FSI	-0,139	0,037	3,796	**0,000**
CSI → NSU → CPS → FSI	-0,080	0,022	3,596	**0,000**
SOS → CSI → NSU → CPS → FSI	-0,034	0,011	2,971	**0,003**
SOS → CSI → JB	-0,156	0,036	4,311	**0,000**
SOS → CSI → NSU	0,243	0,050	4,854	**0,000**

Fonte: Autoria Própria

5.3.4 Análise das Variáveis de Controle

Para analisar a influência das variáveis de controle presentes no modelo, optou-se por utilizar a análise multigrupo (MGA), disponível no software SmartPLS 3.0. Essa análise é apropriada, pois permite a classificação em grupos distintos de variáveis categóricas e contínuas. Nesse sentido, foram realizadas as análises referentes às variáveis idade, considerando dois grupos, o primeiro de 18 a 30 anos (n = 65) e o segundo grupo acima de 30 anos (n = 129); o tempo de serviço na organização, considerando o grupo 1 com até 3 anos de casa (n = 79) e o segundo grupo com respondentes que trabalham há mais de 3 anos (n = 116); o tipo de organização, se pública (n = 80) ou privada (n = 115); e a experiência prévia com incidentes de Segurança da Informação, nesse caso considerando a ocorrência de problemas de segurança em organizações, sendo as respostas Sim (n = 73) e Não (n = 122) e problemas de segurança pessoais, sendo as respostas Sim (n = 51) e Não (n = 142). Todos os

modelos elaborados respeitaram os índices de qualidade de ajuste recomendados. Os resultados obtidos nos relacionamentos foram consistentes com os resultados obtidos na análise primária.

Em relação à idade, a análise MGA não indicou diferenças significativas entre os dois grupos (p >0,05) em nenhuma das relações. Aqui se destaca que diferentemente do modelo original, para os respondentes com até 30 anos, a relação entre o controle percebido e a conformidade com as PSIs é menos significativa (p > 0,05) que para o grupo formado por respondentes acima de 30 anos (p < 0,01). Isso pode indicar que a facilidade ou dificuldade em seguir as PSIs não influencia tão intensamente o cumprimento das mesmas pelos funcionários mais jovens. Outro resultado interessante é que para o grupo com até 30 anos a relação entre o jeitinho e o cumprimento das PSIs também não se mostrou significativa (p > 0,05), enquanto que para os respondentes acima de 30 anos essa relação se confirmou (p < 0,01). Esse resultado sugere que no grupo mais jovem o contorno de regras para se atingir um objetivo, mesmo que tenha um impacto negativo na conformidade da PSIs, não é considerado tão intenso quanto para o grupo de respondentes com mais de 30 anos (Tabela 22).

Tabela 22 - Comparação entre respondentes com até 30 anos e maiores de 30 anos

Relacionamentos	Até 30		Mais de 30		MGA	
	CE	p-valor	CE	p-valor	CE	p-valor
ATI → CPS	0,391	**0,008**	0,276	**0,002**	0,115	0,513
COP → CPS	0,238	0,056	0,311	**0,000**	-0,073	0,611
CPS → FSI	-0,596	**0,000**	-0,483	**0,000**	-0,113	0,242
CSI → ATI	0,589	**0,000**	0,545	**0,000**	0,044	0,722
CSI → COP	0,739	**0,000**	0,624	**0,000**	0,114	0,179
CSI → NSU	0,629	**0,000**	0,513	**0,000**	0,116	0,345
JB → CPS	-0,096	0,236	-0,189	**0,001**	0,093	0,337
NSU → CPS	0,287	**0,048**	0,280	**0,000**	0,006	0,955
SOS → CSI	0,472	**0,000**	0,416	**0,000**	0,056	0,638

Fonte: Autoria Própria

Referente ao tipo de empresa, o MGA não identificou diferenças significativas entre os grupos (p > 0,05). Destaca-se que a relação entre a atitude e o cumprimento das PSIs não se mostrou significativa entre os funcionários de empresas privadas (p > 0,05), permanecendo significativa entre os funcionários de empresas públicas (p < 0,01). Isso pode apontar que a atitude de conformidade com as PSIs não possui a mesma influência que o cumprimento dessas normas de segurança para funcionários de empresas privadas. Na relação entre o jeitinho e o cumprimento das PSIs também apareceram diferenças. Mesmo que a relação

tenha sido significativa nos dois grupos, para funcionários de empresas privadas essa relação se mostrou mais fraca ($p < 0,05$) quando comparada com a de funcionários de organizações públicas ($p < 0,01$), o que significa que o impacto negativo do jeitinho é percebido com menos intensidade no cumprimento das PSIs entre os funcionários que atuam em empresas privadas (Tabela 23).

Tabela 23 - Comparação entre respondentes de empresas públicas e privadas

Relacionamentos	Privada		Pública		MGA	
	CE	p-valor	CE	p-valor	CE	p-valor
ATI → CPS	0,179	0,123	0,400	**0,000**	-0,221	0,150
COP →CPS	0,335	**0,000**	0,219	**0,018**	0,116	0,366
CPS → FSI	-0,483	**0,000**	-0,566	**0,000**	0,083	0,380
CSI → ATI	0,606	**0,000**	0,535	**0,000**	0,072	0,584
CSI → COP	0,677	**0,000**	0,672	**0,000**	0,005	0,964
CSI → NSU	0,513	**0,000**	0,578	**0,000**	-0,064	0,579
JB → CPS	-0,123	**0,021**	-0,220	**0,002**	0,097	0,265
NSU → CPS	0,366	**0,000**	0,260	**0,001**	0,106	0,389
SOS → CSI	0,386	**0,000**	0,489	**0,000**	-0,103	0,361

Fonte: Autoria Própria

Para o tempo de empresa, a análise MGA não identificou diferenças significativas, nem grandes diferenças entre os dois grupos. Os grupos permaneceram estáveis quando comparados ao modelo principal, indicando não haver diferenças significativas quanto aos aspectos relacionados à segurança da informação medidos nesse estudo, pelo menos entre esses dois grupos de respondentes (Tabela 24).

Tabela 24 - Comparação entre respondentes com até 3 anos e mais de 3 anos

Relacionamentos	Até 3 anos		Mais de 3 anos		MGA	
	CE	p-valor	CE	p-valor	CE	p-valor
ATI → CPS	0,323	**0,001**	0,330	**0,004**	-0,007	0,967
COP → CPS	0,342	**0,001**	0,246	**0,010**	0,096	0,487
CPS → FSI	-0,567	**0,000**	-0,503	**0,000**	-0,064	0,487
CSI → ATI	0,574	**0,000**	0,555	**0,000**	0,019	0,868
CSI → COP	0,647	**0,000**	0,693	**0,000**	-0,046	0,629
CSI → NSU	0,507	**0,000**	0,600	**0,000**	-0,093	0,430
JB → CPS	-0,135	**0,020**	-0,155	**0,017**	0,020	0,818
NSU → CPS	0,275	**0,005**	0,273	**0,001**	0,002	0,991
SOS → CSI	0,391	**0,000**	0,479	**0,000**	-0,088	0,450

Fonte: Autoria Própria

Quanto à experiência prévia com problemas de segurança da informação nas organizações, o resultado do MGA não identificou diferenças significativas nas relações entre os constructos. Além disso, os resultados indicaram que a relação entre a atitude e o cumprimento das PSIs nos indivíduos que relataram que já haviam passado por problemas de

segurança da informação em seu trabalho deixou de ser significativa (p > 0,05), indicando que para quem já enfrentou falhas de segurança nas empresas em que trabalham, o grau em que o indivíduo acredita que seguir as normas é um comportamento importante ou necessário não vai influenciar que o mesmo cumpra com essas normas (Tabela 25).

Tabela 25 - Comparação entre respondentes sobre experiência na empresa com problemas de segurança da informação

Relacionamentos	Não		Sim		MGA	
	CE	p-valor	CE	p-valor	CE	p-valor
ATI → CPS	0,435	**0,000**	0,171	0,181	0,264	0,112
COP → CPS	0,245	**0,007**	0,321	**0,001**	-0,076	0,573
CPS → FSI	-0,565	**0,000**	-0,458	**0,000**	-0,107	0,266
CSI → ATI	0,590	**0,000**	0,493	**0,000**	0,097	0,442
CSI → COP	0,733	**0,000**	0,598	**0,000**	0,135	0,150
CSI → NSU	0,610	**0,000**	0,513	**0,000**	0,097	0,433
JB → CPS	-0,113	**0,038**	-0,215	**0,005**	0,102	0,269
NSU → CPS	0,225	**0,020**	0,322	**0,002**	-0,098	0,482
SOS → CSI	0,492	**0,000**	0,397	**0,000**	0,095	0,430

Fonte: Autoria Própria

Por fim, quanto à experiência prévia dos respondentes que afirmaram já ter tido problemas pessoais de segurança da informação, os resultados indicaram que existe diferença significativa na relação entre as normas subjetivas e a conformidade com as PSIs (p < 0,05). Isso indica que para os respondentes que já passaram por problemas pessoais de segurança da informação, a opinião de pessoas importantes do seu ambiente de trabalho tem influência sobre o seu cumprimento das PSIs. Outro resultado que se destaca é que a relação entre o jeitinho e o cumprimento das PSIs daqueles que já haviam passado por problemas de segurança da informação pessoais não foi significativa (p > 0,05) sugerindo que o jeitinho não é percebido de forma significativa para o cumprimento das PSIs, quando comparado respondentes que não passaram por problemas pessoais de segurança da informação. (Tabela 26).

Tabela 26 - Comparação entre respondentes sobre experiência com problemas pessoais de segurança da informação

Relacionamentos	Não		Sim		MGA	
	CE	p-valor	CE	p-valor	CE	p-valor
ATI → CPS	0,348	**0,000**	0,343	**0,016**	0,005	1,000
COP → CPS	0,324	**0,000**	0,194	**0,011**	0,130	0,234
CPS → FSI	-0,532	**0,000**	-0,499	**0,000**	-0,033	0,772
CSI → ATI	0,576	**0,000**	0,545	**0,000**	0,031	0,807
CSI → COP	0,690	**0,000**	0,629	**0,000**	0,061	0,497
CSI → NSU	0,575	**0,000**	0,614	**0,000**	-0,039	0,700
JB → CPS	-0,183	**0,001**	-0,085	0,225	-0,098	0,260
NSU → CPS	0,159	0,053	0,487	**0,000**	-0,327	**0,013**
SOS → CSI	0,433	**0,000**	0,552	**0,000**	-0,119	0,313

Fonte: Autoria Própria

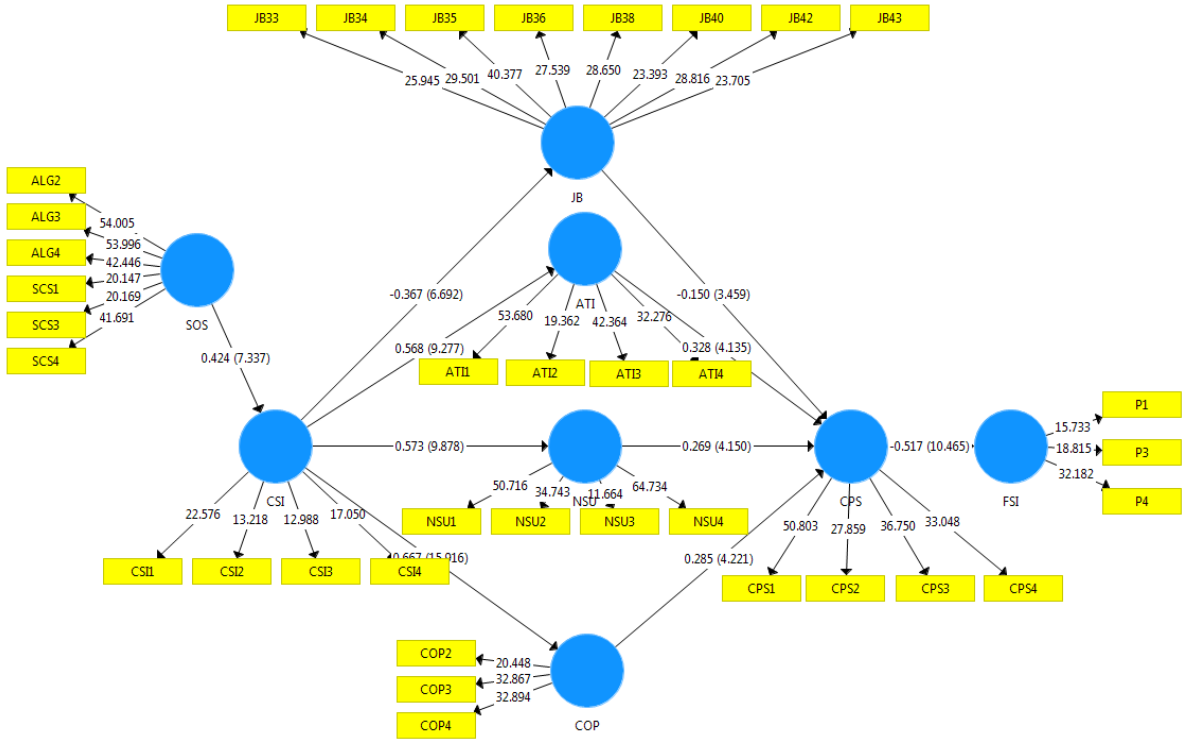
5.3.5 Análise do "Jeitinho Brasileiro" como variável mediadora

De forma complementar a essa pesquisa, optou-se por realizar uma última análise inserindo-se o jeitinho como variável mediadora no modelo. Como se constatou anteriormente que o jeitinho influencia negativamente a conformidade com as PSIs, torna-se interessante compreender como mitigar esse comportamento dentro do ambiente de trabalho, pois mesmo que o jeitinho não seja visto como algo prejudicial pelos respondentes na organização onde atuam, mas sim como um meio de resolver problemas no ambiente de trabalho, a não conformidade com as PSIs pode trazer impactos negativos às organizações. Para compreender melhor essa questão, optou-se por analisar os fatores que poderiam diminuir a força do jeitinho dentro da organização. Como já dissertado nessa pesquisa, quanto mais consciente sobre segurança da informação for o indivíduo, maior será a importância que ele dará ao comportamento de segurança, à opinião de pessoas importantes e à facilidade para executar o comportamento planejado. Então, se o indivíduo for consciente sobre a importância de seguir as PSIs propostas pela organização, o efeito que o jeitinho teria em seu ambiente de trabalho seria menor, pois mesmo que ele acredite que através do jeitinho ele pode solucionar problemas mais rapidamente, com a consciência sobre segurança da informação a força do jeitinho seria diminuída.

Assim, de modo a verificar essa possível relação, a mesma foi adicionada ao modelo e analisada no SmartPLS. O modelo de mensuração mostrou-se semelhante ao modelo geral, em que todos os critérios de qualidade do modelo, como a confiabilidade das escalas, a validade convergente e discriminante, foram atendidos. Já o modelo estrutural confirmou a

proposição levantada, em que a Consciência de Segurança da Informação (CSI) influenciou negativamente o "jeitinho brasileiro" (β = -0,367; p < 0,001), o que mostra que quanto maior a consciência do indivíduo sobre a segurança da informação, menor será a influência do jeitinho no seu comportamento. A Figura 5 destaca o modelo estrutural alternativo.

Figura 5 – Modelo final com o efeito mediador do jeitinho



Fonte: Autoria Própria

6. CONSIDERAÇÕES FINAIS

Essa pesquisa teve como objetivo analisar como os aspectos culturais organizacionais relacionados à segurança da informação no Brasil e a cultura organizacional brasileira influenciam na conformidade com as Políticas de Segurança da Informação por funcionários de diferentes organizações brasileiras. Para isso, através de uma pesquisa *survey*, se propôs testar um novo modelo a fim de elucidar essa questão. Além disso, esse trabalho busca enriquecer a área de Segurança da Informação no Brasil, uma vez que conta com pouquíssimos estudos que visam identificar a partir de teorias sociais, como a teoria cultural, diferentes aspectos que podem influenciar no comportamento relacionado à segurança da informação dos brasileiros (ALBUQUERQUE JUNIOR; SANTOS, 2014; 2013).

Referente à análise descritiva, os resultados indicam que as empresas nacionais analisadas possuem PSIs em diferentes graus de desenvolvimento; entretanto, na sua grande maioria, não informam claramente aos seus funcionários essas normas. Além disso, problemas com segurança da informação, como perda de senhas e acessos indevidos são mais comuns de ocorrerem dentro das organizações do que na vida pessoal dos funcionários, isso de acordo com os respondentes. Também se destaca que os cenários utilizados nessa pesquisa, adaptados do estudo de Silveira et al. (2019), para considerarem o jeitinho e as falhas de segurança da informação em conjunto, foram considerados como realistas pelos respondentes, com destaque ao cenário de compartilhamento de senhas no ambiente de trabalho. Quanto à probabilidade dessas falhas relacionadas ao jeitinho ocorrerem, novamente se destaca o cenário associado ao compartilhamento de senhas. Ressalta-se que esta situação não depende diretamente de controles físicos de TI para ocorrer, o que revela a importância do desenvolvimento de uma cultura de segurança da informação forte, que seja capaz de diminuir a ocorrência de falhas como essa no ambiente de trabalho.

O primeiro objetivo específico definido nesta dissertação buscou adaptar e validar as questões de jeitinho, desenvolvidas por Fernandes e Hanashiro (2015), para o contexto da Segurança da Informação, o qual foi plenamente atendido. Mas diferentemente do estudo original, quando o comportamento do jeitinho é especificado para o contexto da segurança da informação, apenas uma dimensão foi encontrada, que considera o uso do jeitinho, através da flexibilização das normas de segurança e o contorno das mesmas para solucionar problemas no ambiente de trabalho. Quanto ao segundo objetivo proposto, o mesmo também foi atendido, a partir do desenvolvimento de um modelo causal considerando a influência de

diferentes aspectos culturais organizacionais, no caso dessa pesquisa a cultura de segurança da informação, e nacionais, como o jeitinho, no comportamento de segurança da informação dos indivíduos, conforme a indicação de trabalhos anteriores da área de Sistemas de Informação (STRAUB et al., 2002, GALLIVAN; SRITE, 2005; LEIDNER; KAYWORTH, 2006) e da área especifica de Segurança da Informação (CRAM et al., 2019).

Em relação ao objetivo geral proposto, este também foi atendido, a partir da análise de como esses diferentes aspectos culturais influenciam a conformidade com as PSIs na percepção dos respondentes. Diferentemente do esperado, os construtos Apoio da Alta Gerência e Cultura de Suporte Organizacional de Segurança da Informação foram compreendidos pelos respondentes como um único aspecto, evidenciando que as ações que as organizações realizam com o intuito de desenvolver a cultura de segurança da informação estão intimamente ligadas ao apoio que a alta gerência da organização oferece. Quanto às relações de causalidade, todas foram significativas estatisticamente, demonstrando que a diminuição das falhas de segurança da informação relacionadas ao jeitinho é diretamente influenciada pelo cumprimento das PSIs pelos funcionários, sendo este influenciado pelo processo cognitivo (HU et al., 2012), que se forma a partir da influência de diferentes aspectos organizacionais que são influenciados por diferentes níveis culturais.

Quanto ao jeitinho, este influencia o não cumprimento das PSIs. Mesmo não sendo uma característica de todos os brasileiros (FREITAS, 1997), é um traço que permeia a nossa cultura e se faz presente nas organizações brasileiras. O jeitinho não possui a mesma força individualmente que outros aspectos, o que reforça que o desenvolvimento de uma cultura de segurança da informação forte e a sua manutenção podem resultar na diminuição das falhas de segurança, pois a importância de diferentes culturas tende a se modificar de acordo com o ambiente em que o indivíduo se encontra (STRAUB et al., 2002). Então, se o indivíduo trabalha em uma organização que se preocupa com a proteção de suas informações, na qual se busca desenvolver um ambiente que propicie a absorção da importância da Segurança da Informação pelos seus funcionários, através do desenvolvimento de ações de conscientização, os valores culturais que não estão de acordo com o que a organização almeja, no caso dessa a influência negativa do jeitinho brasileiro que atua sobre o comportamento de segurança da informação de seus funcionários, perdem a sua força, pois comportamentos que agreguem valores indesejados passam a ser controlados e vigiados pelos próprios membros da organização, sendo inibidos. Do contrário, se não houver esse investimento da organização, valores culturais que não estão de acordo com os requisitos dos sistemas que a organização

deseja ganham relevância no ambiente de trabalho, sendo aceitos pelos seus funcionários, o que leva a não conformidade das PSIs.

O terceiro objetivo específico também foi atendido, através da análise de como subgrupos da amostra poderiam influenciar os aspectos relacionados ao comportamento de segurança da informação nas organizações. Destaca-se que que para os respondentes que já passaram por problemas pessoais de segurança da informação a opinião de pessoas importantes no ambiente de trabalho influencia positivamente o cumprimento das normas de segurança, sendo este resultado interessante, pois a experiência com problemas pessoais pode influenciar uma melhor aceitação da opinião sobre segurança da informação dentro do ambiente de trabalho. Também destaca-se que para os respondentes mais jovens (com até 30 anos), o controle percebido para executar o comportamento de segurança e o jeitinho deixam de se relacionar com a conformidade com as PSIs. Entre os respondentes de empresas privadas, a atitude de cumprir as normas de segurança da informação também deixou de ser significativa quanto ao cumprimento das PSIs. Já a relação entre a atitude e a conformidade com as normas de segurança também deixou de ser significativa entre os respondentes que já haviam passado por problemas de segurança da informação em suas organizações, enquanto que para os respondentes que já tiveram problemas pessoais relacionados à segurança da informação, a relação entre o jeitinho e o cumprimento das PSIs deixou de ser significativa. Estes resultados reafirmam que as percepções sobre os aspectos relacionados à segurança da informação podem variar de acordo com diferentes características individuais, sendo necessário desenvolver a consciência da informação em todos os indivíduos no ambiente de trabalho (FLORES; EKSTEDT, 2016).

Como contribuições gerenciais destacam-se a análise de fatores organizacionais que influenciam o comportamento de segurança da informação, demonstrando aos gestores que as ações práticas, como treinamentos, programas de conscientização e até mesmo a elaboração e distribuição de cartilhas, ajudam a conscientizar os funcionários sobre as potenciais ameaças e riscos que os mesmos correm ao utilizarem incorretamente a tecnologia disponível no ambiente de trabalho. Isso só é possível se a alta gerência da organização, isto é, direção e gestores de alto escalão estiverem comprometidos com o enfrentamento dos problemas relacionados à segurança da informação. Outro ponto importante é a necessidade de políticas de segurança claras e formalizadas, de fácil acesso e que sejam compreendidas pelos funcionários (NEL; DREVIN, 2019). Incutir uma cultura na qual a informação é governada e protegida pelos funcionários em todos os momentos, de acordo com a política organizacional

e os requisitos regulamentares, não é tarefa fácil, sendo crucial entender as percepções, atitudes e comportamentos dos funcionários da organização, a fim de moldar a cultura de segurança da informação em um ambiente em que a natureza, a confidencialidade e a sensibilidade da informação são compreendidas, e estas tratadas em conformidade (DA VEIGA; MARTINS, 2015). A imersão do indivíduo na cultura da empresa, de acordo com sua intensidade, influenciará os modos de pensar, ser e agir desse indivíduo (SCHEIN, 1984).

Outro ponto que é importante destacar é que as PSIs necessitam estar adequadas ao trabalho realizado pelos funcionários, pois isso inibe as chances de falhas ocorrerem. Talvez a criação de muitas regras que visem garantir a segurança pode provocar diferenças entre o que é escrito e o que de fato é realizado (CHU; WOOD JR., 2018), o que levaria à prática do jeitinho no ambiente organizacional (BERNARDO et al., 2015). A solução seria a implementação de processos que considerem o real trabalho desenvolvido por cada indivíduo, principalmente o acesso a sistemas que correspondam à necessidade para a execução das suas tarefas.

Como contribuições teóricas pode-se destacar o uso de modelos da área de TI para agregar em um modelo causal diferentes níveis de cultura, sendo elas a nacional e a organizacional, para compreender o comportamento relacionado à segurança da informação dos indivíduos. O uso da TPB, em conjunto com o construto Conformidade com as PSIs evidenciou bons resultados, indo de acordo com as sugestões de Cram et al. (2019). Além disso, a adaptação do instrumento e das questões sobre o Jeitinho Brasileiro, originalmente desenvolvido por Fernandes e Hanashiro (2015), contribui para o uso de teorias sociais nacionais nos estudos da área de Sistemas de Informação, agregando conhecimento sobre como os brasileiros são influenciados por fatores que vão além das pesquisas realizadas nos EUA e em países europeus. O estudo da temática da Cultura de Segurança da Informação no Brasil, por exemplo, também é uma contribuição, uma vez que as pesquisas que consideram como os aspectos culturais organizacionais influenciam no cumprimento das PSIs são escassos. Vale destacar que a definição desses traços culturais é utilizada para perceber que alguns elementos ajudam a formar uma identidade nacional e explicam determinados comportamentos nas organizações (BUENO; ARANTES, 2015), dentre eles o comportamento relacionado à segurança da informação.

Como principais limitações do trabalho destaca-se o tipo de amostragem realizado, através do método bola de neve, pois não é possível confirmar se as empresas dos respondentes realmente possuem PSIs formalizadas, e se essas normas são informadas aos

seus funcionários, bem como ocorreu essa aplicação. Outro ponto importante é que, apesar do trabalho atingir seus objetivos, o estudo de aspectos culturais requer um maior aprofundamento (SCHEIN, 1984), podendo os resultados serem complementados por métodos qualitativos de pesquisa, como entrevistas, por exemplo, que poderiam agregar mais informações sobre as relações estudadas.

Como trabalhos futuros, sugere-se a aplicação do instrumento de pesquisa em uma ou mais organizações nas quais seja possível comprovar a existência de PSIs, e que se possa conhecer um pouco da possível cultura de segurança da informação existente nessas organizações. Finalmente, outra sugestão de pesquisa futura seria analisar se as penalizações no caso de não cumprimento das PSIs possuem relação com a conformidade (CRAM et al., 2019; AMANKWA et al., 2018). Estudos da área de organizações destacam que as penalidades que ocorrem dentro das organizações brasileiras são consequências do autoritarismo presente (CHU; WOOD JR, 2008), e isto poderia influenciar o comportamento relacionado à segurança da informação dos indivíduos nas organizações onde atuam.

REFERÊNCIAS

AJZEN, Icek. **Constructing a TPB questionnaire: Conceptual and methodological considerations**. Working Paper, University of Massachusetts, Amherst, September 2002a (available online at http://www-unix.oit.umass.edu/~aizen/pdf/tpb.measurement.pdf).

AJZEN, Icek. The theory of planned behavior. **Organizational Behavior and Human Decision Processes**, v. 50, n. 2, p. 179-211, 1991.

AJZEN, Icek; MADDEN, Thomas J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. **Journal of Experimental Social Psychology**, v. 22, n. 5, p. 453-474, 1986.

ALBUQUERQUE JUNIOR, Antonio Eduardo de et al. A Adopção de Medidas Formais, Informais e Técnicas de Segurança da Informação e sua Relação com as Pressões do Ambiente Institucional. **RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação**, n. 30, p. 17-33, 2018.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M Adoção de Medidas de Segurança da Informação: a Influência das Respostas Estratégicas das Subunidades na Conformidade Organizacional. **Encontro de Administração da Informação**, São Paulo, SP, 2017.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Análise das publicações brasileiras sobre segurança da informação sob a ótica social em periódicos científicos entre 2004 e 2013. **Encontroda Associação Nacional de Pós-Graduação em Administração**, Rio de Janeiro, RJ, Brasil, v. 38, 2014.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Produção científica sobre segurança da informação em anais de eventos da ANPAD. **Encontro de Administração da Informação**, Bento Gonçalves, RS, v. 4, 2013.

ALHOGAIL, Areej; MIRZA, Abdulrahman. A framework of information security culture change. **Journal of Theoretical & Applied Information Technology**, v. 64, n. 2, 2014.

ALNATHEER, Mohammed A. Information security culture critical success factors. **In: 2015 12th International Conference on Information Technology-New Generations**. IEEE, 2015. p. 731-735.

AMANKWA, Eric; LOOCK, Marianne; KRITZINGER, Elmarie. Establishing information security policy compliance culture in organizations**. Information & Computer Security**, v. 26, n. 4, p. 420-436, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

AURIGEMMA, Salvatore; PANKO, Raymond. A composite framework for behavioral compliance with information security policies. **In: 2012 45th Hawaii International Conference on System Sciences**. IEEE, 2012. p. 3248-3257.

BARALE, Rômulo Ferreira; SANTOS, Benedito Rodrigues dos. Cultura organizacional: revisão sistemática da literatura. **Revista Psicologia Organizações e Trabalho**, v. 17, n. 2, p. 129-136, 2017.

BARLACH, Lisete. O jeitinho brasileiro: traço da identidade nacional?. **Revista Gestão & Políticas Públicas**, v. 3, n. 2, 2015.

BARTEL-RADIC, Anne. "Estrangeirismo" and flexibility: intercultural learning in Brazilian MNCs. **Management International/International Management/Gestiòn Internacional,** v. 17, n. 4, p. 239-253, 2013.

BECK, Fabrício da Porciúncula; SANTOS, André Moraes dos. Avaliando a Cultura da Segurança da Informação: o caso de uma organização industrial. **XXXIV Encontro da ANPAD**, Rio de Janeiro - RJ. EnANPAD, 2010.

BERNARDO, Patrícia; SHIMADA, Nayara Emi; ICHIKAWA, Elisa Yoshie. O formalismo e o "jeitinho" a partir da visão de estratégias e táticas de Michel de Certeau: apontamentos iniciais. **Revista Gestão & Conexões**, v. 4, n. 1, p. 45-67, 2015.

BIDO, Diógenes; SILVA, Dirceu. SmartPLS 3: especificação, estimação, avaliação e relato. **Administração: Ensino e Pesquisa**, v. 20, n. 2, p. 1-31, 2019.

BOSS, Scott et al. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. **MIS Quarterly**, v. 39, n. 4, p. 837-864, 2015.

BUENO, Janaina Maria; ARANTES, Pedro Paulo Melo. A influência dos traços da cultura mineira no relacionamento de empresas de agronegócio do Triângulo Mineiro com seus clientes e fornecedores. **Revista GEPROS**, v. 10, n. 2, p. 141, 2015.

BULGURCU, Burcu; CAVUSOGLU, Hasan; BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly**, v. 34, n. 3, p. 523-548, 2010.

CHENG, Lijiao et al. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. **Computers & Security**, v. 39, p. 447-459, 2013.

CHIN, Wynne W. et al. The partial least squares approach to structural equation modeling. **Modern Methods for Business Research**, v. 295, n. 2, p. 295-336, 1998.

CHU, Rebeca Alves; WOOD JR, Thomaz. Cultura organizacional brasileira pós-globalização: global ou local?. **Revista de Administração Pública,** v. 42, n. 5, p. 969-994, 2008.

COHEN, Jacob. Statistical Power Analysis for the Behavioral Sciences. 2. ed. New York: **Psychology Press**, 1988.

CORTEZ, Igor Siqueira; KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista de Administração**, v. 48, n. 4, p. 757-769, 2013.

CRAM, W. Alec; D'ARCY, John; PROUDFOOT, Jeffrey G. Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. **MIS Quarterly**, v. 43, n. 2, 2019.

DA VEIGA, Adéle; ELOFF, Jan HP. A framework and assessment instrument for information security culture. **Computers & Security**, v. 29, n. 2, p. 196-207, 2010.

DA VEIGA, Adele; MARTINS, Nico. Improving the information security culture through monitoring and implementation actions illustrated through a case study. **Computers & Security**, v. 49, p. 162-176, 2015.

DALMORO, Marlon; VIEIRA, Kelmara Mendes. Dilemas na construção de escalas Tipo Likert: o número de itens e a disposição influenciam nos resultados? **Revista Gestão Organizacional**, v. 6, n. 3, 2014.

DAMASCENO, Larissa Mayara da Silva; RAMOS, Anatália Saraiva Martins; PEREIRA, Fernando Antonio de Melo. Fatores que Influenciam a Predisposição em Seguir uma Política de Segurança da Informação em uma Instituição de Ensino Superior. **Revista de Gestão e Projetos-GeP**, v. 6, n. 3, p. 01-16, 2016.

DIAMANTOPOULOS, Adamantios; SIGUAW, Judy A. Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. **British Journal of Management**, v. 17, n. 4, p. 263-282, 2006.

DINEV, Tamara et al. User behaviour towards protective information technologies: the role of national cultural differences. **Information Systems Journal**, v. 19, n. 4, p. 391-412, 2009.

DINEV, Tamara; HU, Qing. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. **Journal of the Association for Information Systems**, v. 8, n. 7, p. 23, 2007.

EGITO, Rafaela Simoes; MONTEIRO, Wilka Ferreira. O JEITINHO BRASILEIRO: Analisando suas características como ferramenta de conveniência e seus prejuízos sociais. **Revista Estudos e Pesquisas em Administração**, v. 2, n. 2, p. 128-146, 2018.

ERNEST & YOUNG. 20ª Pesquisa Global de Segurança da Informação. **Ernest e Young**, 2017. Disponível em https://www.ey.com/br/pt/services/pesquisa-global-da-ey-sobre-seguranca-da-informacao. Acesso em 30 de agosto de 2019.

FERNANDES, Ricardo Antonio; HANASHIRO, Darcy Mitiko Mori. Explorando aspectos indígenas da gestão numa organização financeira: jeitinho e sociedade relacional. **Revista de Administração Contemporânea**, v. 19, n. spe3, p. 328-347, 2015.

FERREIRA, Márcia. R.; DOLCI, Décio Bittencourt; TONDOLO, Vilmar Antônio Gonçalves. Uma Proposta de Diagnóstico e Autoavaliação da Gestão da Segurança da Informação. **XL Encontro da ANPAD**, Costa do Sauípe-BA. EnANPAD, 2016

FREITAS, AB de. Traços brasileiros para uma análise organizacional. **Cultura Organizacional e Cultura Brasileira**. São Paulo: Atlas, p. 38-54, 1997.

FREITAS, Maria Ester de. Cultura organizacional grandes temas em debate. **Revista de Administraçao de Empresas**, v. 31, n. 3, p. 73-82, 1991.

GALEGALE, Napoleão Verardi; FONTES, Edison Luiz Gonçalves; GALEGALE, Bernardo Perri. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. **Perspectivas em Ciência da Informação**, v. 22, n. 3, p. 75-97, 2017.

GALLIVAN, Michael; SRITE, Mark. Information technology and culture: Identifying fragmentary and holistic perspectives of culture. **Information and Organization**, v. 15, n. 4, p. 295-338, 2005.

GLASPIE, Henry W.; KARWOWSKI, Waldemar. Human factors in information security culture: a literature review. In: **International Conference on Applied Human Factors and Ergonomics**. Springer, Cham, 2017. p. 269-280.

GOEL, Sanjay; CHENGALUR-SMITH, InduShobha N. Metrics for characterizing the form of security policies. **The Journal of Strategic Information Systems**, v. 19, n. 4, p. 281-295, 2010.

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Revista Direito GV**, v. 14, n. 2, p. 513-536, 2018.

HAIR JR, Joseph F. et al. **Advanced Issues in Partial Least Squares Structural Equation Modeling**. Sage Publications, 2017.

HAIR, Joseph F. et al. When to use and how to report the results of PLS-SEM. European **Business Review**, v. 31, n. 1, p. 2-24, 2019.

HOVAV, Anat; D'ARCY, John. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. **Information & Management**, v. 49, n. 2, p. 99-110, 2012.

HOFSTEDE. Geert. Country Comparison. **Hofstede Insights**, 2019. Disponível em: https://www.hofstede-insights.com/country-comparison/brazil/ (Acesso: 16 de outubro de 2019).

HOFSTEDE, Geert. Culture and organizations. **International Studies of Management & Organization**, v. 10, n. 4, p. 15-41, 1980(a).

HOFSTEDE, Geert. Motivation, leadership, and organization: do American theories apply abroad? **Organizational Dynamics**, v. 9, n. 1, p. 42-63, 1980(b).

HOFSTEDE, Geert et al. Comparing regional cultures within a country: Lessons from Brazil. **Journal of Cross-Cultural Psychology**, v. 41, n. 3, p. 336-352, 2010.

HSU, Jack Shih-Chieh et al. The role of extra-role behaviors and social controls in information security policy effectiveness. **Information Systems Research**, v. 26, n. 2, p. 282-300, 2015.

HU, Qing; HU, Qing; DINEV, Tamara. Is spyware an internet nuisance or public menace?. **Communications of the ACM,** v. 48, n. 8, p. 61-66, 2005.

HU, Qing et al. Managing employee compliance with information security policies: The critical role of top management and organizational culture. **Decision Sciences,** v. 43, n. 4, p. 615-660, 2012.

IFINEDO, Princely. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. **Information & Management**, v. 51, n. 1, p. 69-79, 2014.

IFINEDO, Princely. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. **Computers & Security**, v. 31, n. 1, p. 83-95, 2012.

ISO, International Organization for Standardization. The ISO Survey 2018. **The ISO Survey**. 2019. Disponível em: https://www.iso.org/the-iso-survey.html (Acesso em: 21 de outubro de 2019).

ISLAM, Gazi. Between unity and diversity: Historical and cultural foundations of Brazilian management. **European Journal of International Management**, v. 6, n. 3, p. 265-282, 2012.

KARLSSON, Fredrik; KARLSSON, Martin; ÅSTRÖM, Joachim. Measuring employees' compliance–the importance of value pluralism. **Information & Computer Security**, v. 25, n. 3, p. 279-299, 2017.

KARJALAINEN, Mari et al. One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. In: **PACIS**. 2013. p. 98.

LEIDNER, Dorothy E.; KAYWORTH, Timothy. A review of culture in information systems research: Toward a theory of information technology culture conflict. **MIS Quarterly**, v. 30, n. 2, p. 357-399, 2006.

MANSUR, Juliana Arcoverde; SOBRAL, Filipe João Bera De Azevedo. Política na terra do" jeitinho": consequências dos comportamentos políticos em organizações no brasil. **RAM. Revista de Administração Mackenzie**, v. 12, n. 6, p. 165-191, 2011.

MARCIANO, João Luiz Pereira; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. **Ciência da Informação**, v. 35, n. 3, 2006.

MARTINS, Danylo. Invasões cibernéticas criminosas ameaçam os negócios. **Jornal Valor** (online), 2019. Disponível em: https://www.valor.com.br/financas/5552593/invasoes-ciberneticas-criminosas-ameacam-os-negocios%20. (Acesso: 30 de agosto de 2019).

MCCORMAC, Agata et al. Individual differences and information security awareness. **Computers in Human Behavior**, v. 69, p. 151-156, 2017.

MENARD, Philip; WARKENTIN, Merrill; LOWRY, Paul Benjamin. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. **Computers & Security**, v. 75, p. 147-166, 2018.

MOREIRA, Ana de Albuquerque; ROCHA, Maria Borba. To Understand the "Brazilian Way" of School Management: How National Culture Influences the Organizational Culture and School Leadership. **Education Sciences**, v. 8, n. 2, p. 88, 2018.

MOTTA, Fernando C. Prestes; CALDAS, Miguel P. Introdução: cultura organizacional e cultura brasileira. **Cultura Organizacional e Cultura Brasileira**. São Paulo: Atlas, p. 15, 1997.

MUZZIO, Henrique. Cultura organizacional na perspectiva cultural regional brasileira. RBGN: **Revista Brasileira de Gestão de Negócios**, v. 12, n. 37, p. 447-463, 2010.

NASCIMENTO, Eduardo Camargos Lagares. Fatores culturais e estruturais que impactam na implantação da política de segurança da informação: um estudo de caso sobre o Ministério do Desenvolvimento Agrário. **Universitas: Gestão e TI**, v. 2, n. 1, 2012.

NEL, Frans; DREVIN, Lynette. Key elements of an information security culture in organisations. **Information & Computer Security**, v. 27, n. 2, 146-164, 2019.

ONWUBIKO, Cyril; LENAGHAN, Andrew P. Challenges and complexities of managing information security. **International Journal of Electronic Security and Digital Forensics**, v. 2, n. 3, p. 306-321, 2009.

ÖĞÜTÇÜ, Gizem; TESTIK, Özlem Müge; CHOUSEINOGLOU, Oumout. Analysis of personal information security behavior and awareness. **Computers & Security**, v. 56, p. 83-93, 2016.

PARSONS, Kathryn Marie et al. The influence of organizational information security culture on information security decision making. **Journal of Cognitive Engineering and Decision Making**, v. 9, n. 2, p. 117-129, 2015.

PINSONNEAULT, Alain; KRAEMER, Kenneth. Survey research methodology in management information systems: an assessment. **Journal of management information systems**, v. 10, n. 2, p. 75-105, 1993.

PRESTES MOTTA, Fernando Claudio. Cultura e Organizações no Brasil. **Cultura Organizacional e Cultura Brasileira**. São Paulo: Atlas. 1997.

REPRESENTANTE, Participantes et al. **Tecnologia da Informação-Técnicas de Segurança–Código de Prática para Controles de Segurança da Informação**. 2013.

RINGLE, Christian M.; DA SILVA, Dirceu; BIDO, Diógenes de Souza. Modelagem de equações estruturais com utilização do SmartPLS. **Revista Brasileira de Marketing**, v. 13, n. 2, p. 56-73, 2014.

RIOS, Orlivaldo Kléber Lima; FILHO, José Gilson de Almeida Teixeira; RIOS, Vânia Patrícia da Silva. Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. **NAVUS-Revista de Gestão e Tecnologia**, v. 7, n. 2, p. 49-65, 2017.

SAMPIERI, Roberto; COLLADO, Carlos; LUCIO, María. Definição do alcance da pesquisa a ser realizada: exploratória, descritiva, correlacional ou explicativa. **Metodologia de Pesquisa**. 5ª ed. Porto Alegre: Penso, p. 99-110, 2013.

SCHEIN, Edgar H. Coming to a new awareness of organizational culture. **Sloan Management Review**, v. 25, n. 2, p. 3-16, 1984.

SHERIF, Emad; FURNELL, Steven; CLARKE, Nathan. An identification of variables influencing the establishment of information security culture. In: **International Conference on Human Aspects of Information Security, Privacy, and Trust**. Springer, Cham, 2015. p. 436-448.

SILVEIRA, Jonas Rafael et al. Segurança da Informação: Uma análise da percepção de ameaças que influenciam a Intenção de Cumprir as Políticas de Segurança da Informação por usuários de organizações do estado do Rio Grande do Sul. **Revista de Tecnologia Aplicada**, v. 8, n. 1, 2019.

SIPONEN, Mikko; MAHMOOD, M. Adam; PAHNILA, Seppo. Employees' adherence to information security policies: An exploratory field study. **Information & Management**, v. 51, n. 2, p. 217-224, 2014.

SIPONEN, Mikko; VANCE, Anthony. Neutralization: new insights into the problem of employee information systems security policy violations. **MIS Quarterly**, p. 487-502, 2010.

SMIRCICH, Linda. Concepts of culture and organizational analysis. **Administrative Science Quarterly**, v. 28, n. 3, p. 339-358, 1983.

SOMMESTAD, Teodor; KARLZÉN, Henrik; HALLBERG, Jonas. The theory of planned behavior and information security policy compliance. **Journal of Computer Information Systems**, v. 59, n. 4, p. 344-353, 2019.

SOOMRO, Zahoor Ahmed; SHAH, Mahmood Hussain; AHMED, Javed. Information security management needs more holistic approach: A literature review. **International Journal of Information Management**, v. 36, n. 2, p. 215-225, 2016.

STRAUB, Detmar et al. Toward a theory-based measurement of culture. **Journal of Global Information Management**, v. 10, n. 1, p. 13-23, 2002.

SYMANTEC. **Internet security threat report**. 2018 Disponível em: https://www.symantec.com/pt/br/security-center/threat-report. (Acesso em: 15 outubro de 2019)

TAJFEL, Henri Ed. Differentiation between social groups: Studies in the social psychology of intergroup relations. **Academic Press**, 1978.

TAJFEL, Henri. Experiments in intergroup discrimination. **Scientific American**, v. 223, n. 5, p. 96-103, 1970.

THOMSON, Kerry-Lynn; VON SOLMS, Rossouw; LOUW, Lynette. Cultivating an organizational information security culture. **Computer Fraud & Security**, v. 2006, n. 10, p. 7-11, 2006.

UNISYS. Unisys Security Index Brazil. **Unisys Corporation**, 2017. Disponível em: https://static.poder360.com.br/2017/10/estudo-unisys-security-index.pdf (Acesso 30 de agosto de 2019).

VAN NIEKERK, J. F.; VON SOLMS, Rossouw. Information security culture: A management perspective. **Computers & Security**, v. 29, n. 4, p. 476-486, 2010.

VANCE, Anthony; SIPONEN, Mikko; PAHNILA, Seppo. Motivating IS security compliance: insights from habit and protection motivation theory. **Information & Management**, v. 49, n. 3-4, p. 190-198, 2012.

WARKENTIN, Merrill et al. Continuance of protective security behavior: A longitudinal study. **Decision Support Systems**, v. 92, p. 25-35, 2016.

APÊNDICE A - CARGAS FATORIAIS DA ANÁLISE FATORIAL CONFIRMATÓRIA

	ATI	COP	CPS	CSI	FSI	JB	NSU	SOS
ATI1	0,916	0,460	0,692	0,497	-0,311	-0,404	0,647	0,456
ATI2	0,843	0,466	0,579	0,505	-0,268	-0,343	0,511	0,388
ATI3	0,885	0,428	0,589	0,503	-0,263	-0,369	0,565	0,372
ATI4	0,863	0,411	0,620	0,488	-0,348	-0,351	0,537	0,394
COP2	0,327	0,781	0,520	0,476	-0,315	-0,191	0,413	0,590
COP3	0,422	0,878	0,537	0,558	-0,367	-0,345	0,479	0,430
COP4	0,497	0,843	0,559	0,626	-0,332	-0,283	0,462	0,321
CPS1	0,741	0,596	0,909	0,612	-0,426	-0,423	0,648	0,555
CPS2	0,612	0,507	0,891	0,534	-0,470	-0,448	0,638	0,538
CPS3	0,612	0,657	0,885	0,650	-0,459	-0,410	0,617	0,596
CPS4	0,541	0,530	0,867	0,440	-0,485	-0,381	0,521	0,495
CSI1	0,389	0,529	0,488	0,826	-0,227	-0,298	0,463	0,336
CSI2	0,364	0,598	0,533	0,709	-0,315	-0,281	0,409	0,472
CSI3	0,394	0,456	0,376	0,728	-0,148	-0,201	0,362	0,157
CSI4	0,575	0,441	0,508	0,783	-0,193	-0,323	0,498	0,290
P1	-0,298	-0,272	-0,392	-0,254	0,751	0,374	-0,309	-0,356
P3	-0,194	-0,357	-0,383	-0,198	0,789	0,283	-0,313	-0,428
P4	-0,312	-0,336	-0,452	-0,250	0,840	0,404	-0,350	-0,388
JB33	-0,371	-0,333	-0,431	-0,327	0,391	0,800	-0,358	-0,368
JB34	-0,268	-0,268	-0,336	-0,266	0,347	0,830	-0,187	-0,215
JB35	-0,412	-0,261	-0,432	-0,331	0,380	0,874	-0,300	-0,207
JB36	-0,395	-0,248	-0,399	-0,320	0,340	0,775	-0,274	-0,248
JB38	-0,326	-0,281	-0,373	-0,299	0,348	0,836	-0,201	-0,206
JB40	-0,284	-0,253	-0,319	-0,246	0,372	0,813	-0,203	-0,178
JB42	-0,351	-0,264	-0,381	-0,333	0,399	0,840	-0,242	-0,243
JB43	-0,313	-0,253	-0,377	-0,267	0,365	0,802	-0,308	-0,325
NSU1	0,579	0,462	0,586	0,528	-0,333	-0,282	0,913	0,521
NSU2	0,553	0,556	0,657	0,577	-0,410	-0,302	0,888	0,649
NSU3	0,522	0,390	0,410	0,312	-0,281	-0,170	0,701	0,572
NSU4	0,589	0,450	0,662	0,511	-0,373	-0,324	0,928	0,578
ALG2	0,438	0,447	0,571	0,411	-0,393	-0,259	0,662	0,891
ALG3	0,400	0,498	0,538	0,400	-0,434	-0,259	0,590	0,888
ALG4	0,372	0,455	0,521	0,382	-0,408	-0,264	0,553	0,890
SCS1	0,317	0,421	0,455	0,281	-0,385	-0,191	0,433	0,751
SCS3	0,376	0,447	0,520	0,283	-0,447	-0,324	0,526	0,777
SCS4	0,426	0,409	0,525	0,366	-0,446	-0,271	0,597	0,872

Fonte: Autoria Própria

ANEXO 1 - QUESTÕES UTILIZADAS NO INSTRUMENTO DE COLETA DE DADOS

Participação da Alta Gestão	
A alta gerência considera a segurança da informação uma importante prioridade da empresa.	Knapp (2006)
As palavras e ações da alta gestão demonstram que a segurança da informação é uma prioridade.	Knapp (2006)
O suporte visível para as metas de segurança da informação da gerência sênior é claro.	Knapp (2006)
A alta gestão oferece suporte forte e consistente à segurança da informação.	Knapp (2006)
Cultura de Suporte de Segurança da Informação	
A empresa em que trabalho se preocupa com as questões relacionadas à segurança da informação.	Amankwa et al (2018)
A empresa em que trabalho oferece treinamentos que visam melhorar as questões relacionadas à segurança da informação.	Amankwa et al (2018)
Incidentes com vazamento de informações são evitados porque a empresa em que trabalho se preocupa com isso.	Amankwa et al (2018)
Programas de conscientização e treinamento enfatizam a importância da segurança da informação na empresa.	Amankwa et al (2018)
Consciência Sobre Segurança da Informação	
Eu tenho conhecimento suficiente sobre o custo de possíveis problemas de segurança da informação para a empresa.	Bulgurcu et al (2010)
Eu entendo as preocupações em relação à segurança da informação e os riscos que elas representam em geral.	Bulgurcu et al (2010)
No geral, estou ciente das possíveis ameaças à segurança e suas consequências negativas a empresa.	Bulgurcu et al (2010)
Eu compreendo os riscos relacionados à segurança da informação para a empresa.	Criada
Normas Subjetivas	
Pessoas que são influentes para mim na empresa acham que eu devo seguir as normas, regras e procedimentos relacionados à segurança da informação.	Hu et al (2012)
Pessoas que são importantes para mim na empresa pensam que eu devo seguir as políticas e procedimentos de segurança da informação.	Hu et al (2012)
As pessoas que eu respeito na empresa pensam que eu devo seguir as normas e procedimentos de segurança da informação.	Hu et al (2012)
Pessoas importantes na empresa possuem opiniões que eu valorizo sobre as normas e procedimentos de segurança da informação.	Criada
Atitude	
Para mim, cumprir os requisitos de segurança da informação estabelecidos pela empresa é necessário.	Bulgurcu et al (2010)
Para mim, cumprir com as normas de segurança da informação de acordo com a empresa é benéfico.	Bulgurcu et al (2010)
Para mim, cumprir com as regras de segurança da informação determinadas pela empresa é importante.	Bulgurcu et al (2010)
Para mim, praticar as normas de segurança da informação estabelecidas pela empresa é adequado.	Bulgurcu et al (2010)
Controle Percebido	
Eu sou capaz de seguir as normas, regras e procedimentos de segurança da informação estabelecidos pela minha empresa.	Hu et al (2012)
Eu tenho recursos e conhecimento para seguir as regras e procedimentos de segurança da informação disponibilizados pela minha empresa.	Hu et al (2012)
Tenho treinamento e habilidades adequadas para seguir as normas e procedimentos de segurança da informação definidos pela minha empresa.	Hu et al (2012)
Possuo as habilidades necessárias para seguir as regras e normas de segurança da informação da minha empresa.	Criada
Conformidade com as PSIs	
Eu cumpro com as normas e regras de segurança da informação da empresa.	Ifinedo (2014)

Estou certo de que sigo os procedimentos de segurança da informação da minha empresa.	Ifinedo (2014)
Eu sigo as normas e regras de segurança da informação da empresa.	Ifinedo (2014)
Eu sigo os procedimentos e regras de segurança da informação da empresa.	Ifinedo (2014)
Contorno de Regras	
Percebo que na empresa em que trabalho as pessoas flexibilizam as normas relacionadas à segurança da informação quando necessário.	Fernandes e Hanashiro (2015)
Percebo que na empresa em que trabalho as regras de segurança da informação são contornadas, dependendo da situação.	Fernandes e Hanashiro (2015)
Percebo que na empresa em que trabalho entre o Sim e o Não, o Pode e o Não Pode, sempre existe um Talvez quando se trata de cumprir as regras de segurança da informação.	Fernandes e Hanashiro (2015)
Percebo que na empresa em que trabalho para atendimento de um pedido de ajuda, eventualmente, alguma regra de segurança da informação é contornada.	Fernandes e Hanashiro (2015)
Flexibilização	
Percebo que na empresa em que trabalho é necessário ter jogo de cintura já que as normas de segurança da informação não são adequadas a todas as situações do dia a dia.	Fernandes e Hanashiro (2015)
Percebo que na empresa em que trabalho frente a uma situação especial, é necessário contornar alguma regra de segurança da informação para que seja encontrada uma saída.	Fernandes e Hanashiro (2015)
Percebo que na empresa em que trabalho para o bom andamento dos trabalhos, algumas regras de segurança são flexibilizadas.	Fernandes e Hanashiro (2015)
Estratégia informal de resolução de problemas	
Percebo que na empresa em que trabalho resolver os problemas é mais importante que seguir as normas de segurança da informação.	Fernandes e Hanashiro (2015)
Percebo que na empresa em que trabalho em situações especiais, para solucionar problemas, faz-se necessário dar um jeitinho.	Fernandes e Hanashiro (2015)
Percebo que na empresa em que trabalho, se necessário, é preferível resolver os problemas e se dar um jeitinho.	Criada
Percebo que na empresa em que trabalho para se resolver problemas é necessário ignorar as normas de segurança da informação.	Criada

ANEXO 2 – QUESTIONÁRIO APLICADO NO PRÉ-TESTE

UNIVERSIDADE FEDERAL DO RIO GRANDE
INSTITUTO DE CIÊNCIAS ECONÔMICAS, ADMINISTRATIVAS E CONTÁBEIS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO

Convido você a participar de uma pesquisa de Mestrado em Administração, realizada pelo Núcleo de Pesquisas e Estudos Regionais da Universidade Federal do Rio Grande (NUPER/FURG).

A pesquisa tem por objetivo **conhecer diferentes fatores que influenciam no cumprimento das Políticas de Segurança da Informação nas empresas**. Uma Política de Segurança da Informação descreve as funções e responsabilidades dos funcionários, abordando questões específicas de segurança, na proteção dos recursos de informações da organização onde trabalha.

É importante destacar que não existe resposta certa ou errada. Apenas queremos saber a sua opinião. Também não será necessário, em momento algum, a identificação do respondente. Os dados fornecidos serão analisados de forma agregada, sendo confidenciais e de uso restrito do estudo.

Contamos com o seu apoio, através do preenchimento desse questionário, que leva em torno de 10 minutos para respondê-lo.

Lembre-se, a sua participação nesta pesquisa é de extrema importância! Obrigado.

INTRODUÇÃO

A organização em que trabalho possui regras bem definidas quanto ao uso dos componentes de TI (como computadores, impressoras e sistemas da empresa), visando a segurança das informações da organização?

De maneira nenhuma	Um pouco	Moderadamente	Muito	Muitíssimo
1	2	3	4	5

A organização em que trabalho informa claramente aos seus funcionários as regras de segurança da informação?

De maneira nenhuma	Um pouco	Moderadamente	Muito	Muitíssimo
1	2	3	4	5

PARTE 1: Informações Gerais

Gênero: [1] masculino [2] feminino [3] outro

Idade: [1] Entre 18 e 35 [2] Entre 21 e 45 [3] Entre 46 e 60 [4] Acima de 60

Escolaridade – Nível mais alto concluído:

[1] Ensino Médio incompleto [2] Ensino Médio [3] Ensino Superior incompleto
[4] Ensino Superior [5] Pós-Graduação Incompleta [6] Pós-Graduação Completa

Tipo de empresa em que atua: [1] Pública [2] Privada

Cidade/Estado em que trabalha: _____

Setor Econômico principal e número de empregados:
[1] Indústria [2] Comércio [3] Serviços

Nível do cargo que possui na empresa:
[1] operacional [2] supervisão [3] gerência [4] direção

Tempo em que trabalha na empresa:
[1] Até 6 meses [2] mais de 6 meses até 1 ano [3] mais de 1 ano até 3 anos
[4] mais de 3 anos até 5 anos [5] mais de 5 anos até 10 anos [6] mais de 10 anos

Já passou por algum problema de segurança da informação na empresa em que trabalha (por exemplo, perda/roubo de informação, HD ou servidor danificado, etc.)
[1] sim
[2] não

E já passou por algum problema relacionado à segurança da informação que afetasse sua vida pessoalmente, fora da empresa?
[1] sim
[2] não

PARTE 1/3: Com relação aos 4 cenários a seguir, nos quais se descrevem ações relacionadas com segurança da informação em um ambiente dentro de uma empresa, leia com atenção, e responda as questões abaixo dos cenários, seguindo a indicação a seguir:

Muito baixa					→	**Muito alta**
1	2	3	4	5	6	7

1) Paulo trabalha editando documentos importantes para sua empresa. Ele precisa editar um documento que será utilizado por seus colegas, mas a versão do seu aplicativo está muito antiga, o que está dificultando seu trabalho. A Política de Segurança da Informação proíbe o uso de aplicativos não instalados pela TI da empresa, mas Paulo consegue uma versão mais atual do aplicativo, instala no seu computador e termina a edição dos documentos.

Qual a probabilidade dessa prática ocorrer no seu ambiente de trabalho?

1	2	3	4	5	6	7

Como você considera a realidade desse cenário?

1	2	3	4	5	6	7

2) Cláudia possui acesso ao computador da empresa através de uma senha de uso pessoal. Ela está no meio de uma viagem de negócios, e seus colegas precisam de um arquivo em seu computador para finalizar um relatório. A Política de Segurança da Informação da empresa proíbe o compartilhamento de senhas de uso pessoal, mas Cláudia compartilha a sua senha com seus colegas, que conseguem o arquivo e finalizam o trabalho.

Qual a probabilidade dessa prática ocorrer no seu ambiente de trabalho?

1	2	3	4	5	6	7

Como você considera a realidade desse cenário?

1	2	3	4	5	6	7

3) Rodrigo tem acesso a importantes informações da empresa em que trabalha. A empresa solicita a ele que analise algumas dessas informações com urgência, e informe aos seus colegas a conclusão da análise. Rodrigo resolve levar alguns documentos importantes em um pendrive. A Política de Segurança da Informação proíbe o usuário de usar informações organizacionais fora do ambiente de trabalho, mas usando os documentos do pendrive, Rodrigo consegue terminar seu trabalho durante a viagem, e repassa aos seus colegas as conclusões da análise.

Qual a probabilidade dessa prática ocorrer no seu ambiente de trabalho?

1	2	3	4	5	6	7

Como você considera a realidade desse cenário?

1	2	3	4	5	6	7

4) Flávia necessita gerar um arquivo pdf construído a partir de outros documentos, sendo estes sigilosos para sua empresa, de modo que seus colegas possam consultar essas informações rapidamente. Como a empresa não possui o software para executar essa função, Flávia usa uma aplicação online gratuita para juntar os documentos em um arquivo único. A Política de Segurança da Informação proíbe o uso de sites desconhecidos para atividades da empresa, mas Flávia consegue gerar o arquivo único, e repassa aos seus colegas.

Qual a probabilidade dessa prática ocorrer no seu ambiente de trabalho?

1	2	3	4	5	6	7

Como você considera a realidade desse cenário?

1	2	3	4	5	6	7

PARTE 2/3: Em relação às questões abaixo, relacionadas ao cumprimento das políticas de segurança da informação, responda utilizando um dos pontos da escala, seguindo a orientação a seguir:

Discordo Totalmente						Concordo Totalmente
1	2	3	4	5	6	7

A alta gestão oferece suporte forte e consistente à segurança da informação.	1	2	3	4	5	6	7
Incidentes com vazamento de informações são evitados porque a empresa em que trabalho se preocupa com isso.	1	2	3	4	5	6	7
Eu obedeço as regras de segurança da informação da empresa.	1	2	3	4	5	6	7
Possuo as habilidades necessárias para seguir as regras de segurança da informação da minha empresa.	1	2	3	4	5	6	7
Eu compreendo os riscos relacionados à segurança da informação para a empresa.	1	2	3	4	5	6	7
Provavelmente serei punido se não seguir as normas de segurança da informação.	1	2	3	4	5	6	7
Para mim, cumprir com as regras de segurança da informação determinadas pela empresa é importante.	1	2	3	4	5	6	7
Pessoas importantes na empresa possuem opiniões que eu valorizo sobre as normas de segurança da informação.	1	2	3	4	5	6	7
Eu sigo as normas de segurança da informação da empresa.	1	2	3	4	5	6	7
Para mim, cumprir os requisitos de segurança da informação estabelecidos pela empresa é necessário.	1	2	3	4	5	6	7
As pessoas que eu respeito na empresa pensam que eu devo seguir as normas de segurança da informação.	1	2	3	4	5	6	7
Eu tenho recursos e conhecimento para seguir as normas de segurança da informação disponibilizados pela minha empresa.	1	2	3	4	5	6	7
Para mim, seguir as normas de segurança da informação de acordo com a empresa é benéfico.	1	2	3	4	5	6	7
Receberei repreensão pessoal em relatórios de avaliação (oral ou escrita) se descumprir as regras de segurança da informação da empresa.	1	2	3	4	5	6	7
O suporte da alta gerência para a segurança da informação é claro.	1	2	3	4	5	6	7
A empresa em que trabalho oferece treinamentos que visam melhorar as questões relacionadas à segurança da informação.	1	2	3	4	5	6	7
Para mim, praticar as normas de segurança da informação estabelecidas pela empresa é adequado.	1	2	3	4	5	6	7
Pessoas que são importantes para mim na empresa pensam que eu devo seguir as políticas de segurança da informação.	1	2	3	4	5	6	7
Eu entendo as preocupações em relação à segurança da informação e os riscos que elas representam em geral.	1	2	3	4	5	6	7
A alta gerência considera a segurança da informação uma importante prioridade da empresa.	1	2	3	4	5	6	7
Eu sou capaz de seguir as regras de segurança da informação estabelecidas pela minha empresa.	1	2	3	4	5	6	7
Eu cumpro com as normas de segurança da informação da empresa.	1	2	3	4	5	6	7
Pessoas que são influentes para mim na empresa acham que eu devo seguir as regras relacionadas à segurança da informação.	1	2	3	4	5	6	7
No geral, estou ciente das possíveis ameaças à segurança e suas consequências negativas à empresa.	1	2	3	4	5	6	7
A empresa em que trabalho se preocupa com as questões relacionadas à segurança da informação.	1	2	3	4	5	6	7
Tenho treinamento e habilidades adequadas para seguir as normas de segurança da informação definidos pela minha empresa.	1	2	3	4	5	6	7
Estou certo de que cumpro as normas de segurança da informação da empresa.	1	2	3	4	5	6	7
Punições explícitas ou não explícitas ocorrerão caso eu não cumpra as normas de segurança da informação definidas pela empresa.	1	2	3	4	5		7
Eu tenho conhecimento suficiente sobre o custo de possíveis problemas de segurança da informação para a empresa.	1	2	3	4	5	6	7
As palavras e ações da alta gerência demonstram que a segurança da informação é uma prioridade para a empresa.	1	2	3	4	5	6	7
Programas de conscientização e treinamento enfatizam a importância da segurança da informação na empresa.	1	2	3	4	5	6	7
Eu sofrerei penalidades financeiras ou não financeiras se não seguir as regras de segurança da informação.	1	2	3	4	5	6	7

PARTE 3/3: Em relação às questões abaixo, relacionadas com o cumprimento das políticas de segurança da informação, responda utilizando um dos pontos da escala, seguindo a orientação a seguir:

Discordo Totalmente						Concordo Totalmente
1	2	3	4	5	6	7

Percebo que na empresa em que trabalho....

para o bom andamento dos trabalhos, algumas regras de segurança são flexibilizadas.	1	2	3	4	5	6	7
as regras de segurança da informação são contornadas, dependendo da situação.	1	2	3	4	5	6	7
resolver os problemas é mais importante que seguir as normas de segurança da informação.	1	2	3	4	5	6	7
é necessário ter jogo de cintura, já que as normas de segurança da informação não são adequadas a todas as situações do dia a dia.	1	2	3	4	5	6	7
entre o Sim e o Não, o Pode e o Não Pode, sempre existe um Talvez quando se trata de cumprir as regras de segurança da informação.	1	2	3	4	5	6	7
em situações especiais para solucionar problemas, faz-se necessário adaptar-se e não cumprir com as normas de segurança da informação.	1	2	3	4	5	6	7
as pessoas flexibilizam as normas relacionadas à segurança da informação, quando necessário.	1	2	3	4	5	6	7
frente a uma situação especial, é necessário contornar alguma regra de segurança da informação para que seja encontrada uma saída.	1	2	3	4	5	6	7
se necessário, é preferível resolver os problemas e desconsiderar as normas de segurança da informação.	1	2	3	4	5	6	7
flexibilizar as regras de segurança da informação é possível para se atingir um objetivo no trabalho.	1	2	3	4	5	6	7
para se resolver problemas é necessário ignorar as normas de segurança da informação.	1	2	3	4	5	6	7
para atendimento de um pedido de ajuda, eventualmente, alguma regra de segurança da informação é contornada.	1	2	3	4	5	6	7

MUITO OBRIGADO PELA SUA PARTICIPAÇÃO!

Críticas, comentários ou sugestões sobre o questionário, a pesquisa como um todo, ou a questões de segurança (ou falhas de segurança) da informação podem ser descritas abaixo. O espaço está disponível para suas contribuições.

Se quiser receber os resultados dessa pesquisa, deixe seu e-mail: _____

ANEXO 3 - PÁGINA INICIAL DO QUESTIONÁRIO ONLINE

Políticas de Segurança da Informação

1%

Sair da pesquisa

Olá,
Convido você a participar de uma pesquisa de **Mestrado em Administração**, realizada pelo **Núcleo de Pesquisas e Estudos Regionais** da **Universidade Federal do Rio Grande** (NUPER/FURG).

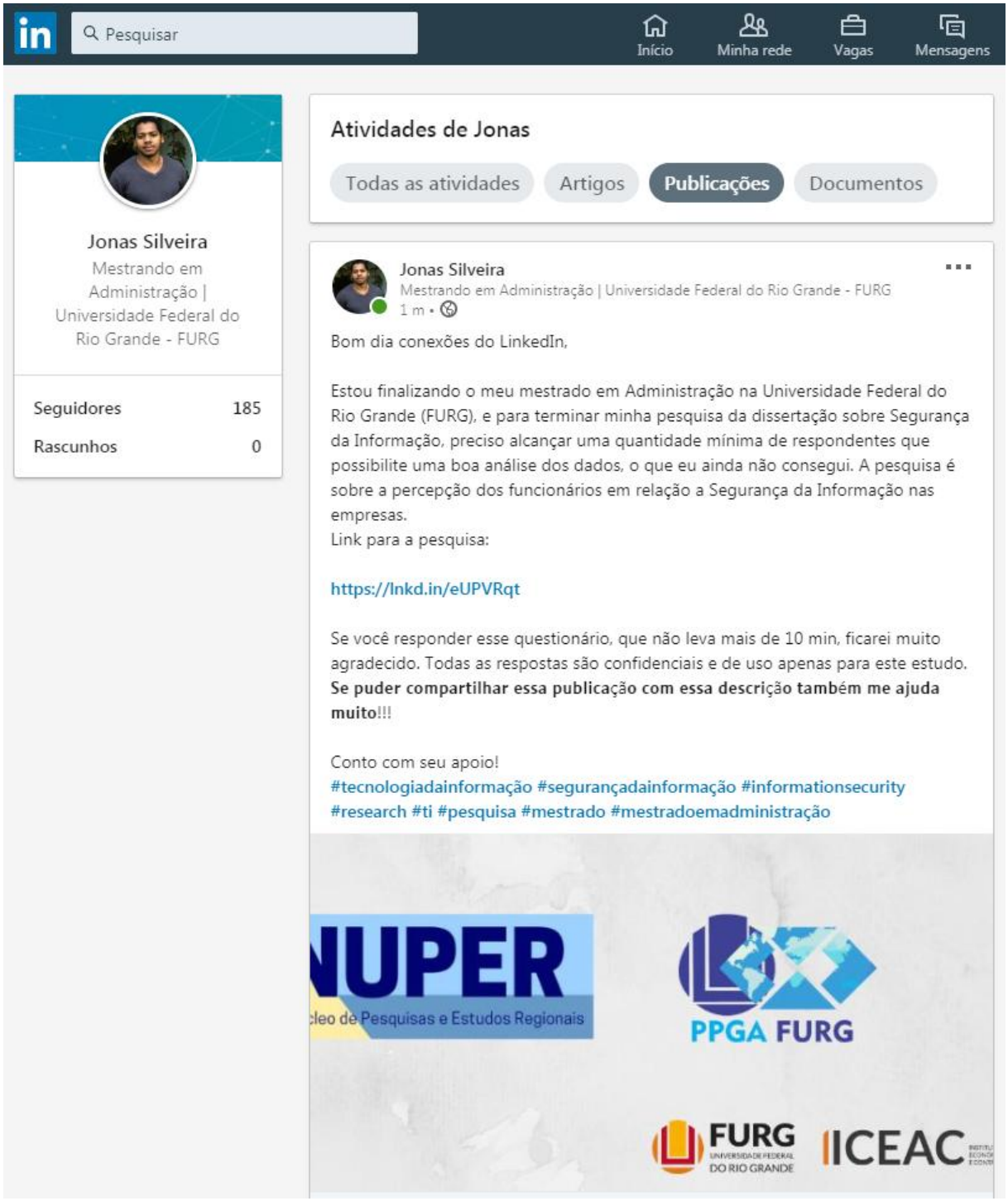
A pesquisa tem por objetivo **conhecer diferentes fatores que influenciam no cumprimento das Políticas de Segurança da Informação nas empresas**. Uma Política de Segurança da Informação descreve as **funções e responsabilidades** dos funcionários, abordando questões específicas de segurança, na proteção dos recursos de informações da organização onde trabalha.

É importante destacar que **não existe resposta certa ou errada**. Apenas queremos saber a sua opinião. Também não será necessário, em momento algum, a identificação do respondente. Os dados fornecidos serão analisados de forma agregada, **sendo confidenciais e de uso restrito do estudo.**

Contamos com o seu apoio, através do preenchimento desse questionário, que leva em torno de 10 minutos para respondê-lo. Quando estiver pronto para começar, basta clicar no botão abaixo.Lembre-se, a sua participação nesta pesquisa é de extrema importância!

Obrigado.

ANEXO 4 - PUBLICAÇÃO DA PESQUISA NAS REDES SOCIAIS LINKEDIN E FACEBOOK




Pesquisar
Jonas
Jonas Silveira
22 de janeiro ·
Boa tarde amigos do Facebook,
Estou no final do período de coleta de dados para a minha pesquisa de dissertação, do mestrado em Administração na Universidade Federal do Rio Grande (FURG). Preciso alcançar uma quantidade mínima de respondentes que possibilite uma boa análise dos dados, o que eu ainda não consegui. A pesquisa é sobre a percepção dos funcionários em relação a Segurança da Informação nas empresas.
Link para a pesquisa:
https://segurancainformacao.questionpro.com
Se você responder esse questionário, que não leva mais de 10 min, ficarei muito agradecido. Todas as respostas são confidenciais e de uso apenas para este estudo.
Se puder compartilhar essa publicação com essa descrição também me ajuda muito!!!
Conto com seu apoio!
NUPER
leo de Pesquisas e Estudos Regionais
PPGA FURG
FURG
UNIVERSIDADE FEDERAL DO RIO GRANDE
ICEAC
SEGURANCAINFORMACAO.QUESTIONPRO.COM
Pesquisa sobre Políticas de Segurança da Informação | Pesquisa sobre Políticas de Segurança da Informação - Onli...
4
1 compartilhamento