REAd
Revista Eletrônica de Administração

RELAÇÃO ENTRE CULTURA E SEGURANÇA DA INFORMAÇÃO: COMO EVITAR FALHAS DECORRENTES DO "JEITINHO BRASILEIRO"?[1]

Jonas Rafael Silveira[2]

Guilherme Lerch Lunardi[3]

Lucas Santos Cerqueira[4]

http://dx.doi.org/10.1590/1413-2311.376.119225

RESUMO

Diversos pesquisadores têm buscado compreender o que leva os indivíduos a cumprir as Políticas de Segurança da Informação - PSIs instituídas pelas organizações. Uma dessas correntes defende que a cultura representa um importante fator, destacando-se a presença de estudos envolvendo cultura organizacional em detrimento da cultura nacional. Dadas as especificidades culturais do país, estudar a relação entre seus aspectos culturais e o cumprimento das PSIs pode trazer *insights* sobre a gestão da segurança da informação nas organizações brasileiras. Assim, objetivou-se neste estudo analisar como a cultura de segurança da informação influencia os indivíduos no cumprimento das políticas de segurança da informação e na diminuição da ocorrência de falhas de segurança associadas ao "jeitinho brasileiro". O estudo caracteriza-se como uma pesquisa *survey* aplicada a 196 funcionários de diferentes organizações brasileiras. Os resultados indicaram que a consciência de segurança da informação influencia positivamente o comportamento planejado dos indivíduos e negativamente o "jeitinho", sendo que ambos influenciam o cumprimento das normas de segurança da informação estabelecidas pela organização. Identificou-se, ainda, uma forte relação entre o cumprimento das normas e a diminuição de falhas de segurança associadas ao "jeitinho brasileiro".

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

[1] Recebido em 11/10/2021, aceito em 20/01/2023.

[2] Universidade Federal do Rio Grande – Programa de Pós-Graduação em Administração; Rio Grande – RS (Brasil); https://orcid.org/0000-0002-2303-708X; jonasrsilveira@gmail.com.

[3] Universidade Federal do Rio Grande – Programa de Pós-Graduação em Administração; Rio Grande – RS (Brasil); https://orcid.org/0000-0003-3250-2796; gllunardi@furg.br.

[4] Universidade Federal do Recôncavo da Bahia - e Universidade Federal do Rio Grande - Programa de Pós-Graduação em Administração; Cachoeira – BA e Rio Grande – RS (Brasil); https://orcid.org/0000-0001-5287-6133; lucasscerqueira@gmail.com.

RELATIONSHIP BETWEEN CULTURE AND INFORMATION SECURITY: HOW TO AVOID FAILURES ARISING FROM THE "BRAZILIAN WAY"?

Several researchers have sought to understand what drives individuals to comply with information security policies (ISP) defined by organizations. One of these currents argues that culture represents an important factor, highlighting, however, the presence of studies involving organizational culture to the detriment of national culture. Given the cultural specificities of the country, studying the relationship between its cultural aspects and compliance with ISP's can bring insights to information security managers in Brazilian organizations. Thus, the aim of this study was to analyze how the information security culture influences individuals in complying with information security policies and at reducing the occurrence of security failures associated with the "Brazilian way". The study was carried out through a survey with 196 employees from different Brazilian organizations. The results indicated that the awareness of information security positively influences the individuals' planned behavior and negatively the influence of the "Brazilian way", both influencing the compliance with the information security standards established by the organization. We also identified a strong relationship between compliance with the rules and the reduction of security failures associated with the "Brazilian way".
Keywords: Information Security. Culture. Organizational Culture. National Culture. Brazilian way.

RELACIÓN ENTRE CULTURA Y SEGURIDAD DE LA INFORMACIÓN: ¿CÓMO EVITAR FALLAS DERIVADAS DE LA "VÍA BRASILEÑA"?

Varios investigadores han tratado de comprender qué impulsa a las personas a cumplir con las políticas de seguridad de la información (PSI) instituidas por las organizaciones. Una de estas corrientes sostiene que la cultura representa un factor importante, destacando la presencia de estudios que involucran la cultura organizacional en detrimento de la cultura nacional. En razón de las especificidades culturales del país, estudiar la relación entre sus aspectos culturales y el cumplimiento de las ISP puede aportar conocimientos sobre la gestión de la seguridad de la información en las organizaciones brasileñas. Así, el objetivo de este estudio fue analizar cómo la cultura de seguridad de la información influye en las personas en el cumplimiento de las políticas de seguridad de la información y en la reducción de la ocurrencia de fallas de seguridad asociadas a la "vía brasileña". El estudio se caracteriza por ser una encuesta de investigación aplicada a 196 empleados de diferentes organizaciones brasileñas. Los resultados indicaron que la conciencia de la seguridad de la información influye positivamente en el comportamiento planificado de los individuos y negativamente en la influencia del "don", ambos influyen en el cumplimiento de los estándares de seguridad de la información establecidos por la organización. También se identificó una fuerte relación entre el cumplimiento de las reglas y la reducción de fallas de seguridad asociadas con la "habilidad brasileña".
Palabras clave: Seguridad de la Información. Cultura. Cultura Organizacional. Cultura Nacional. Vía Brasileña.

INTRODUÇÃO

O uso efetivo de Sistemas de Informação - SI tem se mostrado essencial para o sucesso das organizações, devido ao atual cenário de negócios altamente globalizado e orientado digitalmente (CRAM; D'ARCY; PROUDFOOT, 2019). Nesse contexto, os usuários de tecnologia 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. Várias quebras de segurança têm sido relatadas nos últimos anos, inclusive durante a pandemia (ÉPOCA NEGÓCIOS, 2020), causando prejuízos financeiros e de reputação para várias empresas, indivíduos e governos (MARTINS, 2019).

Assim, tecnologias que protegem computadores e sistemas contra vírus, acessos não autorizados, interrupções e outras ameaças, passaram a ganhar importância na sociedade atual (DINEV et al., 2009), sendo a segurança da informação um requisito essencial para os negócios. Isso tem exigido das organizações cada vez mais a presença de normativas, como as estabelecidas pela ISO 27001 – que corresponde à norma internacional responsável pelo gerenciamento das Políticas de Segurança da Informação - PSIs (CRAM; D'ARCY; PROUDFOOT, 2019). Ainda assim, a proteção de redes de computadores, suas comunicações ou dados de trânsito não dependem mais da implementação única de controles técnicos, dependendo também de outros requisitos de segurança, como conformidade, legislação e cultura ou meio ambiente, uma vez que a dimensão humana relacionada à Segurança da Informação não se resolve apenas com tecnologia (NEL; DREVIN, 2019).

Alguns pesquisadores interessados nessa temática têm apontado a cultura como um importante aspecto influenciador do comportamento do indivíduo relacionado à conformidade com as normas de Segurança da Informação, em relação à estrutura organizacional, aos seus colegas, às chefias e na própria relação com a tecnologia (THOMSON; VON SOLMS; LUW, 2006). Assim, analisar como tais aspectos podem influenciar os indivíduos no seu comportamento relacionado à segurança podem trazer novos *insights* sobre a gestão da segurança da informação nas organizações. Mais especificamente no Brasil, cuja cultura se mostra bastante rica e diversificada, sendo, entretanto, derivada de diferentes países com diferentes culturas (HOFSTEDE et al., 2010), analisar como os aspectos da cultura brasileira influenciam a 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 tem sido pesquisada principalmente na área de estudos organizacionais, destacando algumas das características presentes nas organizações brasileiras, como a hierarquização, o personalismo e o formalismo (CHU; WOOD JR., 2008). Além destes, o "jeitinho brasileiro" é considerado um traço específico da cultura brasileira, caracterizado como uma recurso para a resolução de problemas causados pela inadequação das regras formais à prática social (FERNANDES; HANASHIRO, 2015). De qualquer maneira, no momento em que um indivíduo recorre ao "jeitinho" para alcançar algum objetivo, deixando de cumprir normativas, ele vai contra o que a organização determina oficialmente. Assim, define-se a seguinte questão de pesquisa norteadora deste estudo: Como aspectos organizacionais relacionados à cultura de segurança da informação refletidos na consciência de segurança da informação influenciam o cumprimento das Políticas de Segurança da Informação pelos indivíduos, em conjunto com aspectos específicos da cultura brasileira, de modo a diminuir a ocorrência de falhas de segurança? A partir do problema de pesquisa identificado, pretende-se analisar como a cultura de segurança da informação influencia os indivíduos no cumprimento das políticas de segurança da informação e na diminuição da ocorrência de falhas de segurança associadas ao "jeitinho brasileiro".

1 CULTURA E SEGURANÇA DA INFORMAÇÃO

Inúmeros pesquisadores têm usado mais de uma definição de cultura, dependendo do assunto abordado e da época em que sua definição havia sido formulada (STRAUB et al., 2002). Na área de SI, mais especificamente nos estudos sobre Segurança da Informação, também existem distinções sobre o uso do termo. Utilizando conceitos da cultura organizacional, principalmente da cultura a partir da aprendizagem organizacional (SCHEIN, 1984), estudiosos da área propuseram o termo cultura de segurança da informação como as atitudes, suposições, crenças, valores e conhecimentos que usuários e demais partes interessadas usam para interagir com os sistemas e procedimentos da organização (ALHOGAIL; MIRZA, 2014; DA VEIGA; ELOFF, 2010). Para Da Veiga e Eloff (2010), essa interação resulta em um comportamento aceitável ou inaceitável (que pode causar 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.

Além da cultura organizacional relacionada à segurança da informação, outros estudiosos procuraram abordar como as diferenças culturais nacionais poderiam interferir no

comportamento de segurança da informação dos indivíduos, principalmente a partir de estudos transculturais. Vários destes estudos utilizaram como base as pesquisas realizadas por Hofstede (1980) sobre diferenças nacionais, retratadas a partir de diferentes valores. Karjalainen et al. (2013), por exemplo, analisaram o comportamento de segurança da informação de funcionários de diferentes países, com ambientes culturais bem variados (Finlândia, Suíça, Emirados Árabes Unidos e China). O estudo constatou que entre as razões que explicam o comportamento de segurança dos funcionários, independentemente da cultura, estão a experiência anterior de trabalho; a moral e a educação; o ambiente de trabalho; a identidade profissional; a mídia; e a conformidade social, enquanto que entre as razões dependentes da cultura estão as preferências dos funcionários em relação aos meios de aprendizagem do comportamento de segurança, este variando conforme a cultura nacional. 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 de indivíduos norte-americanos e sul-coreanos, descobrindo que existe uma diferença na percepção da gravidade das sanções aplicadas, no caso de descumprimento das PSIs, entre norte-americanos e sul-coreanos.

Como fator determinante para o desenvolvimento de uma cultura de segurança da organização, alguns estudiosos colocam a importância da conscientização sobre a segurança, essa obtida a partir de treinamentos e do suporte da organização em relação à segurança da informação (McCORMAC et al., 2017; DLAMINI; ELOFF; ELOFF, 2009), sendo a própria consciência sobre segurança da informação determinante para o cumprimento das políticas de segurança instituídas pela organização (AMANKWA; LOOCK; KRITZINGER, 2018). Percebe-se pelas diferentes abordagens utilizadas para verificar o comportamento de segurança dos indivíduos, que o desenvolvimento de uma cultura de segurança da informação requer esforços organizacionais, que resultam em uma maior consciência sobre segurança da informação e, consequentemente, em um comportamento desejado, mas que também deve considerar a influência da cultura nacional, podendo trazer novos *insights* sobre a efetividade das normas de segurança da informação e de conformidade dos funcionários com as PSIs.

1.1 O "jeitinho brasileiro"

Os estudos abordando a influência da cultura nacional na cultura organizacional foram impulsionados a partir dos anos 1980, motivados pela repercussão dos resultados das várias pesquisas realizadas por Hofstede nos anos 1970, em que 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 (MUZZIO, 2010) e um dos conceitos estudados é o "jeitinho brasileiro".

O "jeitinho" pode ser visto como uma solução para aquilo que não tem solução, não sendo as leis, as normas e a própria constituição nacional barreiras definitivas e irrevogáveis para o comportamento (BARLACH, 2013; BERNARDO; SHIMADA; ICHIKAWA, 2015). Para Motta e Caldas (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 da malandragem, mesmo estando próximo, pois não se caracteriza por "passar alguém pra trás". O "jeitinho" é ambíguo, podendo significar uma postura conformista de convivência com o *status quo* injusto e inaceitável; ou ser visto como uma forma de sobreviver ao cotidiano (CHU; WOOD JR., 2008). Islam (2012) coloca que o "jeitinho brasileiro", em sua concepção, é essencialmente o uso de laços personalistas para ultrapassar temporariamente as regras formais. É uma estratégia para suavizar as formas impessoais que regem as relações pessoais.

O construto "jeitinho" foi proposto por Fernandes e Hanashiro (2015) com base em dois traços bastante fortes, associados à cultura brasileira: o formalismo (marcado pela necessidade de leis e normas para reduzir o risco, a ambiguidade e a incerteza) e a flexibilidade (que se traduz na capacidade de ajustes a situações diversas e à capacidade de inovação) (CHU; WOOD JR., 2008). Assim, espera-se que o praticante do "jeitinho" perceba: i) a existência de regras inadequadas à prática social; ii) a necessidade de flexibilização na aplicação das regras; iii) a necessidade de contornar regras, visando resolver problemas ou situações especiais; e iv) a necessidade de ajudar alguém ou dar andamento ao trabalho, mesmo que regras tenham que ser contornadas ocasionalmente.

Portanto, é possível que o "jeitinho" se relacione com o comportamento de cumprir ou não as PSIs estabelecidas pela organização. Na área de segurança da informação, o contorno de regras, como o compartilhamento de senhas; o uso de mídias portáteis ou o acesso a sites ou programas não autorizados; dentre outras, ainda que feito para alcançar um objetivo específico, no caso, a resolução de algum problema através da flexibilização das normas, pode causar quebras de segurança, trazendo prejuízos à organização e ao próprio indivíduo. De qualquer maneira, no momento em que uma pessoa se utiliza do "jeitinho" para resolver algum problema no seu ambiente de trabalho, flexibilizando normas de segurança ou contornando regras

predefinidas, ainda que de forma ocasional, ela vai contra o que a organização determina oficialmente.

1.2 Políticas de Segurança da Informação (PSI)

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, operacionalizar a implantação da segurança e fornecer orientações para a conduta de funcionários. 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).

No Brasil, alguns estudos sobre Políticas de Segurança da Informação já foram realizados. Galegale, Fontes e Galegale (2017) identificaram que as PSIs nas organizações brasileiras pesquisadas eram consolidadas e maduras, e que 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, que envolve tanto pessoas internas como externas. Albuquerque Junior e Santos (2017) constataram, a partir da análise de PSIs de diferentes organizações brasileiras, que mesmo que as organizações possuam essas políticas bem determinadas, isso não significa que o usuário final compreende 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 cumprir pressões externas e não para atender as necessidades de proteção de informações na organização.

Mesmo com os mais variados tipos de pesquisas e teorias que visam analisar o que leva à conformidade ou não das PSIs, alguns pontos específicos merecem mais atenção. De acordo com Cram, D'arcy e Proudfoot (2019), especificamente quando falam de estudos que consideram os aspectos culturais como influentes na intenção ou conformidade com as PSIs, a maior parte desses estudos se baseia em aspectos organizacionais, desconsiderando aspectos de cultura nacional. Nesse sentido, estudos que contemplem aspectos culturais nacionais, em conjunto com aspectos organizacionais, podem auxiliar no preenchimento dessa lacuna, e mais especificamente, no Brasil, o que justifica a realização dessa pesquisa.

1.3 A Teoria do Comportamento Planejado e os estudos sobre conformidade com as PSIs

A Teoria do Comportamento Planejado, ou simplesmente TPB, do inglês, *Theory of Planned Behaviour*, se caracteriza por ser uma extensão da Teoria da Ação Racional, 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 "sob controle", maior é a intenção de a pessoa realizar um comportamento esperado (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 ao comportamento em questão. Já a norma subjetiva refere-se à pressão social percebida para executar, ou não, esse comportamento; enquanto que o controle comportamental percebido refere-se à facilidade ou dificuldade percebida de um indivíduo executar este comportamento, supondo-se que este reflita suas experiências passadas, bem como impedimentos e obstáculos previstos.

Para um uso correto da TPB, Ajzen (1991) 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 levou em conta aspectos cognitivos a partir da Teoria do Comportamento Planejado e as dimensões desenvolvidas por Hofstede (1980), Dinev et al. (2009), realizou-se uma pesquisa transcultural com norte-americanos e sul-coreanos, tendo por objetivo analisar como alguns fatores influenciavam a decisão dos usuários em usar tecnologias de proteção 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 os norte-americanos. Também descobriram que, embora em ambas as culturas o conhecimento das consequências negativas do *spyware* fosse suficiente para motivar os usuários a desenvolver atitudes positivas em relação às tecnologias de proteção e formar a intenção de usá-las, o papel da conscientização foi muito mais forte nos EUA do que na Coreia do Sul, consistente com as características de individualismo e masculinidade das duas culturas.

Bulgurcu, Cavusoglu e Benbasat (2010), usando a mesma teoria, 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, sugeriram 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, evidenciaram que a intenção de um funcionário cumprir as normas de segurança é significativamente influenciada por atitudes, crenças normativas e pela autoeficácia, evidenciando, também, que a CSI, em conjunto com as crenças, possui um papel crucial para que os funcionários possam ter uma atitude em conformidade com as PSIs.

Hu et al. (2012) analisaram os efeitos da alta administração e da cultura organizacional para entender o comportamento de segurança dos funcionários nas organizações e para desenvolver práticas eficazes de gerenciamento de segurança da informação. Os autores estabeleceram como crenças individuais os construtos da TPB e, para verificar a influência dos aspectos da cultura organizacional, concentraram-se 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 achados, encontraram que a cultura organizacional, especificamente a orientação de objetivos percebida e os valores de orientação de regras percebidos, tem um efeito significativo na atitude dos funcionários; e que a participação da alta gerência influencia fortemente os valores culturais percebidos, sugerindo que o impacto da alta administração na atitude dos funcionários é mediado pela cultura organizacional (HU et al., 2012). Além disso, os resultados sugeriram que mesmo que a cultura forneça uma estrutura normativa para interpretação e criação de sentido e uma abordagem mais geral, voltada à solução de problemas para funcionários em ambientes organizacionais, a cultura organizacional de Segurança da Informação sozinha não é suficiente para mudar o comportamento individual em relação às políticas ou aos programas específicos, como a conformidade com as normas de segurança da informação estabelecidas pela organização.

É importante destacar que o uso da TPB sofreu várias adaptações nos estudos sobre as PSIs, principalmente quanto aos seus antecedentes e até mesmo nos seus construtos principais (SOMMESTAD; KARLZÉN; HALLBERG, 2017), o que sugere a inclusão de outras variáveis capazes de explicar de forma mais completa o comportamento dos indivíduos quanto ao cumprimento, ou não, das normativas de segurança da informação estabelecidas pelas organizações.

1.3.1 A Teoria do Comportamento Planejado e a conformidade com as PSIs

Propõe-se nesta pesquisa que o comportamento de cumprimento das PSIs é influenciado pela atitude, pelas normas subjetivas e pelo controle percebido, que levam o indivíduo a tomar a ação de seguir as PSIs definidas pela organização onde atua. No caso das PSIs, a atitude frente à conformidade possui um importante papel no cumprimento das políticas de segurança da informação, pois quanto mais os usuários perceberem as políticas de segurança da informação como algo benéfico, necessário e importante, maior será a sua intenção de segui-las (BULGURCU; CAVUSOGLU; BENBASAT, 2010; AMANKWA; LOOCK; KRITZINGER, 2018). Já as normas subjetivas referem-se às pressões sociais que os indivíduos percebem para que determinado comportamento seja seguido (AJZEN; MADDEN, 1986). No Brasil, onde a pessoalidade no ambiente de trabalho ocorre através de uma confiança desenvolvida entre os pares, substituindo a impessoalidade na relação profissional e influenciando até mesmo na produtividade dos funcionários (FERNANDES; HANASHIRO, 2015), espera-se que a pressão social de pessoas consideradas importantes pelos indivíduos em seu ambiente de trabalho influencie nas normas subjetivas do indivíduo. Em relação ao controle percebido para seguir as PSIs, espera-se que quanto maior for a capacidade que o indivíduo acredita possuir para cumpri-las, maior será o cumprimento das normas de segurança definidas pela organização.

Complementarmente, o "jeitinho", cuja principal característica se dá pelo contorno de regras visando à resolução de problemas no ambiente de trabalho, teria uma influência negativa na conformidade com as PSIs. Se o cumprimento das regras de segurança pré-estabelecidas pela organização for considerado inadequado pelo indivíduo, ou grupo de indivíduos, ou considerado menos importante do que solucionar um problema vivenciado no trabalho, suas chances de se adaptar e criar novos mecanismos que vão contra as regras definidas oficialmente pela organização serão maiores. Assim, propõem-se as seguintes hipóteses: i) H1: A atitude de conformidade com as PSIs influencia positivamente o cumprimento das normas de segurança da informação; ii) H2: As normas subjetivas relacionadas à conformidade com as PSIs influenciam positivamente o cumprimento das normas de segurança da informação; iii) H3: O controle percebido da conformidade com as PSIs influencia positivamente o cumprimento das normas de segurança da informação; e iv) H4: O "jeitinho" influencia negativamente o cumprimento das normas de segurança da informação.

1.3.2 O papel da Consciência de Segurança da Informação

A TPB é aberta à inclusão de preditores adicionais, se for possível demonstrar que eles capturam uma proporção significativa da variação na intenção ou no comportamento do indivíduo, após as variáveis principais da teoria serem levadas em consideração (AJZEN; MADDEN, 1986). Assim, neste estudo, optou-se por utilizar o construto Consciência de Segurança da Informação - CSI, proposto por Bulgurcu, Cavusoglu e Benbasat (2010), como 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 para agir em conformidade com as normativas definidas pela organização.

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. Assim, a própria construção da consciência de segurança é colocada como um fator que requer da organização disposição de tempo e recursos. Da Veiga e Martins (2015) demonstraram que com o passar do tempo, os funcionários que receberam treinamentos prévios em segurança da informação foram mais positivos em relação à conformidade com as PSIs em comparação com aqueles que não receberam treinamento, supondo-se, então, que os funcionários que passaram por tais procedimentos 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.

Por outro lado, quanto mais consciente o indivíduo for quanto à importância da segurança da informação, bem como o nível de segurança exigido pela organização e suas responsabilidades individuais, menor necessidade será percebida pelo indivíduo em contornar ou descumprir as normas de segurança pré-estabelecidas pela organização. Assim, propõem-se as seguintes hipóteses: i) H5: A consciência de segurança da informação influencia positivamente a atitude

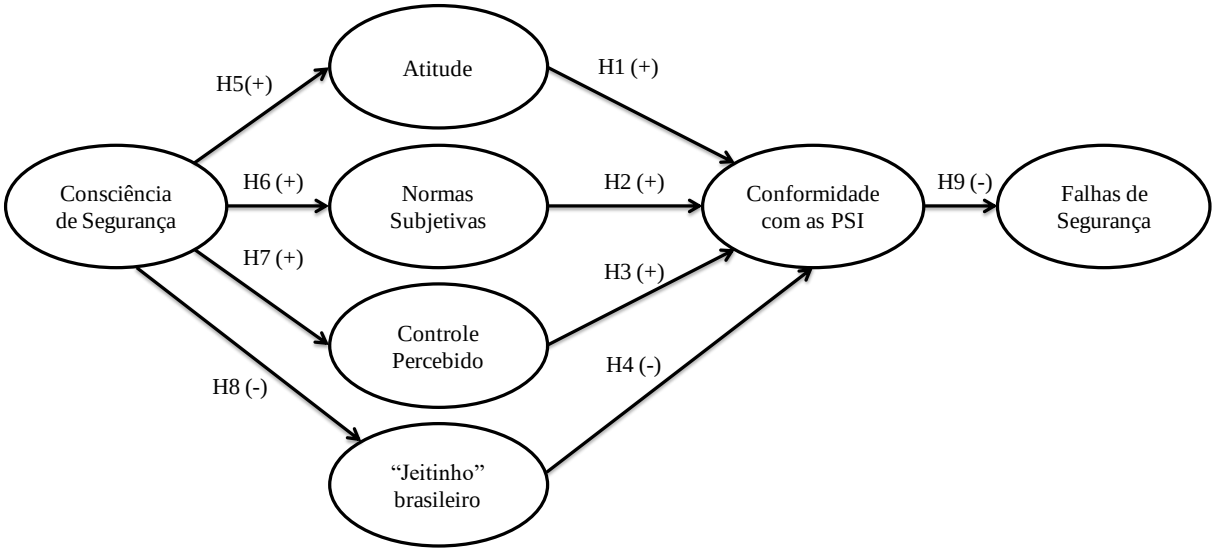
de conformidade com as PSIs; ii) H6: A consciência de segurança da informação influencia positivamente as normas subjetivas de conformidade com as PSIs; iii) H7: A consciência de segurança da informação influencia positivamente o controle percebido de conformidade com as PSIs; e iv) H8: A consciência de segurança da informação influencia negativamente o "jeitinho".

1.3.3 Falhas de segurança e sua relação com o "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. Mesmo que a organização busque desenvolver em seus funcionários a consciência sobre a importância da segurança da informação através do desenvolvimento de uma cultura de segurança, não se pode negar que a carga cultural que o indivíduo possui da sociedade que vive exerce um papel determinante em seus meios de pensar e agir (HOFSTEDE, 1980).

Em uma situação em que as PSIs entram em conflito com a eficácia do fluxo de trabalho, bem como com a integridade e o bem-estar pessoal dos indivíduos, é menos provável que os funcionários cumpram estas políticas (GLASPIE; KARWOWSKI, 2017; KARLSSON; KARLSSON; ASTRÖM 2017). Assim, o "jeitinho", através de seus traços, já que não se pode afirmar que seja uma característica comum a todos os brasileiros (MOTTA; CALDAS, 1997), compreendido aqui como o contorno de regras para se alcançar um objetivo visando à resolução de problemas no ambiente de trabalho, está presente entre as organizações brasileiras e interfere no cumprimento das PSIs. Por isso, define-se que quanto mais os funcionários cumprissem com as normas de segurança da informação no seu ambiente de trabalho, menores seriam as ocorrências de quebras de segurança relacionadas ao "jeitinho" e ao comportamento inconsequente do indivíduo. Assim, propõe-se a seguinte hipótese, H9: A conformidade com as PSIs influencia negativamente a incidência de quebras de segurança no ambiente de trabalho. A Figura 1 apresenta o modelo de pesquisa proposto no estudo.

Figura 1 - Modelo conceitual de pesquisa



Fonte: autores da pesquisa.

2 METODOLOGIA

Esta pesquisa se caracteriza como um estudo de natureza exploratório-descritiva, pois visa analisar um problema pouco estudado, especificamente no Brasil, que é a relação entre o cumprimento com as normas de segurança da informação e diferentes aspectos culturais; descritivos; e correlacionais, porque busca especificar a partir de uma pesquisa *survey* as propriedades e características de um conjunto de indivíduos e organizações, além de analisar o grau de associação entre diferentes variáveis (SAMPIERI; COLLADO; LUCIO, 2013).

O questionário desenvolvido para a realização do estudo foi estruturado em três blocos. O primeiro, apresenta um conjunto de questões de caracterização da amostra, referentes ao respondente (incluindo idade, gênero, escolaridade e tempo de empresa) e à organização em que atua (se pública ou privada; o setor econômico e ramo de atuação; o número de funcionários; e o porte da empresa). O segundo bloco apresenta três questões, contendo cenários hipotéticos, retratando possíveis situações de falhas de segurança da informação associadas ao "jeitinho brasileiro", os quais foram adaptados do estudo de Silveira et al. (2019). Os cenários avaliavam, na visão dos respondentes, a probabilidade dessas práticas não recomendadas ocorrerem em seu ambiente de trabalho, sendo operacionalizadas em uma escala tipo Likert de 7 pontos, variando de (1) Muito baixa a (7) Muito alta. Os cenários foram utilizados na pesquisa de forma conjunta, compondo a variável dependente Falhas de Segurança da Informação - FSI. O Apêndice A apresenta os cenários propostos. O terceiro, e último bloco do instrumento, apresenta 25 questões fechadas, relacionadas aos diferentes construtos utilizados no modelo

proposto. A sua operacionalização também ocorreu através de uma escala Likert de 7 pontos, variando de (1) Discordo totalmente a (7) Concordo totalmente. Todas as questões utilizadas foram retiradas de trabalhos previamente validados, e adaptadas ao contexto da pesquisa. As questões do instrumento, juntamente com a referência utilizada e suas estatísticas descritivas, estão disponíveis no Apêndice B.

Antes da aplicação do instrumento, uma primeira análise do questionário foi realizada por um grupo de especialistas em TI, familiarizados com o tema Segurança da Informação. Em seguida, realizou-se um pré-teste com 30 funcionários de empresas públicas e privadas que possuíam normas de segurança da informação bem estabelecidas e claramente informadas. Pequenos ajustes foram realizados no instrumento, especialmente quanto à sua diagramação.

A amostra do estudo se classifica como não probabilística, por conveniência, sendo utilizadas as redes sociais Facebook e Linkedin para compartilhamento do link da pesquisa. Como critérios de inclusão, o respondente deveria ter mais de 18 anos e trabalhar em alguma empresa que possuísse Políticas de Segurança da Informação, em maior ou menor grau. A coleta de dados ocorreu entre dezembro de 2019 e janeiro de 2020, sendo utilizada a plataforma QuestionPro para a sua operacionalização. Após o fim da coleta dos dados, foram consideradas válidas as respostas de 196 respondentes. De modo a verificar se o tamanho da amostra era adequado, utilizou-se o software G*Power 3.1.9.4, considerando como parâmetro do construto com o maior número de preditores (RINGLE; DA SILVA; BIDO, 2014). Assim, considerando o tamanho do efeito médio do f^2 (0,15), com uma margem de confiança de 95%, obteve-se como valor mínimo de casos uma amostra de 85 respondentes, o que sugere que a amostra total do estudo é adequada.

3 RESULTADOS E DISCUSSÃO

Esta seção apresenta os resultados da pesquisa, destacando primeiramente i) a caracterização da amostra e, em seguida, ii) a análise correlacional, realizada por meio da modelagem de equações estruturais.

3.1 Caracterização da amostra

A amostra final do estudo é formada 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%). Quanto ao nível hierárquico, a maior parte dos respondentes atua no nível operacional (59,2%); quanto ao tempo de empresa, a maioria tem entre 5 e 10 anos (26,5%) e a minoria tem entre 1 e 3 anos (20,4%). Referente às empresas em que atuam, a maioria afirmou trabalhar em organizações privadas (58,7%); do setor de serviços (69,4%); e em organizações com mais de 499 empregados (41,3%), sendo, em maior número, organizações de grande porte.

3.2 Análise correlacional

De modo a se analisar o relacionamento preditivo e causal entre os constructos do modelo, testando-se, portanto, as hipóteses propostas no estudo, empregou-se a técnica de modelagem de equações estruturais baseada na variância, através do software *SmartPLS* 3.0 (*Partial Least Squares*). Com base nessa metodologia, os dados são analisados e interpretados em duas etapas: i) a avaliação do modelo de mensuração; e ii) a avaliação do modelo estrutural, os quais são apresentados na sequência.

3.2.1 Modelo de mensuração

Para se avaliar o modelo de mensuração, foram verificadas as validades discriminante e convergente do modelo, através da Análise Fatorial Confirmatória (AFC, tabela 1). A validade discriminante é estabelecida quando um indicador apresenta a carga fatorial em seu construto original maior do que todas as suas cargas cruzadas com outros construtos. Espera-se, ainda, que as cargas fatoriais atinjam um mínimo de 0,707 no seu respectivo fator. Assim, foram avaliadas as cargas fatoriais de todos os construtos do modelo, decidindo-se por eliminar um item presente no construto Controle Percebido (COP1), por não atender a este critério. O algoritmo *Partial Least Square* (PLS) foi realizado novamente, confirmando a formação original dos demais construtos utilizados, cujos itens se mostraram estatisticamente significativos, ao nível de 5%, nos seus respectivos constructos. Além da AFC, foram utilizados outros dois testes para avaliar a validade discriminante: o critério de Fornell-Larcker, em que se compara a raiz quadrada dos valores da AVE com as correlações das demais variáveis latentes, devendo a raiz quadrada da AVE de cada construto ser maior do que a sua correlação mais alta com os demais construtos, critério também atendido (tabela 2); e a razão multitraço-monotraço (ou HTMT), em que se espera que a relação entre os construtos seja menor que 0,90, também confirmado na pesquisa.

Tabela 1 - Análise Fatorial Confirmatória - AFC

	ATI	COP	CPS	CSI	FSI	JB	NSU
ATI1	**0,916**	0,460	0,692	0,499	-0,311	-0,417	0,647
ATI2	**0,843**	0,466	0,579	0,504	-0,268	-0,344	0,511
ATI3	**0,885**	0,428	0,589	0,506	-0,263	-0,387	0,565
ATI4	**0,863**	0,411	0,620	0,490	-0,348	-0,367	0,537
COP2	0,327	**0,780**	0,520	0,468	-0,315	-0,178	0,413
COP3	0,422	**0,878**	0,537	0,554	-0,367	-0,339	0,479
COP4	0,497	**0,843**	0,559	0,626	-0,332	-0,294	0,462
CPS1	0,741	0,596	**0,909**	0,609	-0,426	-0,437	0,648
CPS2	0,612	0,507	**0,891**	0,535	-0,470	-0,444	0,638
CPS3	0,612	0,656	**0,885**	0,643	-0,459	-0,417	0,617
CPS4	0,541	0,530	**0,867**	0,437	-0,485	-0,387	0,521
CSI1	0,389	0,529	0,488	**0,829**	-0,227	-0,308	0,463
CSI2	0,364	0,598	0,533	**0,692**	-0,315	-0,279	0,409
CSI3	0,394	0,456	0,376	**0,737**	-0,148	-0,212	0,362
CSI4	0,575	0,441	0,508	**0,790**	-0,193	-0,337	0,498
FSI1	-0,298	-0,272	-0,392	-0,251	**0,751**	0,362	-0,309
FSI2	-0,194	-0,357	-0,383	-0,194	**0,789**	0,267	-0,313
FSIP3	-0,312	-0,336	-0,452	-0,247	**0,840**	0,417	-0,350
JB1	-0,371	-0,333	-0,431	-0,325	0,391	**0,814**	-0,358
JB2	-0,268	-0,268	-0,336	-0,265	0,347	**0,821**	-0,187
JB3	-0,412	-0,261	-0,432	-0,331	0,380	**0,894**	-0,300
JB4	-0,395	-0,248	-0,399	-0,321	0,340	**0,829**	-0,274
JB5	-0,351	-0,264	-0,381	-0,332	0,399	**0,836**	-0,242
NSU1	0,579	0,462	0,586	0,528	-0,333	-0,297	**0,913**
NSU2	0,553	0,556	0,657	0,576	-0,410	-0,304	**0,888**
NSU3	0,522	0,390	0,410	0,312	-0,281	-0,168	**0,701**
NSU4	0,589	0,450	0,662	0,512	-0,373	-0,336	**0,928**

Nota: ATI = Atitude de conformidade, COP = Controle Percebido, CPS = Conformidade com as PSIs, CSI = Consciência de Segurança da Informação, FSI = Falhas de Segurança da Informação, JB=Jeitinho brasileiro, NSU = Normas Subjetivas. Fonte: autores da pesquisa.

Complementarmente, avaliou-se a fidedignidade das escalas através da confiabilidade composta (do inglês, *Composite Reliability* - CR) e do Alfa de Cronbach, como indicado na tabela 2. Os escores dos dois testes realizados evidenciou que todos os construtos presentes 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.

Tabela 2 - Variância compartilhada, correlações e confiabilidade dos construtos

	Média	AC	CC	AVE	ATI	COP	CPS	CSI	FSI	JB	NSU
ATI	6,14	0,90	0,93	0,769	**0,877**						
COP	5,43	0,78	0,87	0,697	0,503	**0,835**					
CPS	5,74	0,91	0,94	0,788	0,709	0,646	**0,888**				
CSI	6,05	0,76	0,85	0,583	0,570	0,663	0,630	**0,764**			

FSI	4,51	0,71	0,84	0,631	-0,34	-0,405	-0,517	-0,291	**0,794**		
JB	3,70	0,90	0,92	0,704	-0,433	-0,328	-0,475	-0,377	0,443	**0,839**	
NSU	5,71	0,88	0,92	0,744	0,646	0,542	0,684	0,573	-0,409	-0,329	**0,863**

Nota: AC= Alfa de Cronbach, CC=Confiabilidade Composta, AVE= Variância Média Esperada, ATI= Atitude de conformidade, COP=Controle Percebido, CPS=Conformidade com as PSIs, CSI=Consciência de Segurança da Informação, FSI=Falhas de Segurança da Informação, JB=Jeitinho Brasileiro, NSU=Normas Subjetivas.
Fonte: autores da pesquisa.

3.2.2 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. Foram estimados os coeficientes de caminho (β) e sua significância estatística (t) para testar as hipóteses do modelo proposto, além de serem calculados os coeficientes de determinação (R^2) das variáveis endógenas. Além disso, calculou-se o fator de inflação da variância (VIF) para verificar o grau de multicolinearidade dos construtos; e o f^2, que mede o tamanho do efeito preditivo de cada variável exógena (independente) nas variáveis endógenas (dependentes).

Em relação à hipótese H1, identificou-se que a Atitude de Conformidade com as PSIs (ATI) influencia positivamente o cumprimento das PSIs (CPS), confirmando a hipótese proposta ($\beta = 0{,}325$; $\rho < 0{,}001$). Essa foi a relação do comportamento planejado do indivíduo mais intensa, o que significa que possuir 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 de cumprimento das normas do que a habilidade ou pressão percebida por pessoas importantes (FLORES; EKSTEDT, 2016). Já as Normas Subjetivas (NSU) também influenciam positivamente o cumprimento das normas de segurança da informação (CPS), validando a hipótese H2 ($\beta = 0{,}269$; $\rho < 0{,}001$). Isso significa que os funcionários são influenciados pela opinião de pessoas importantes no seu ambiente de trabalho quando decidem cumprir, ou não, as políticas de segurança da informação em suas organizações, sugerindo que quando líderes ou chefias incentivarem ou darem o exemplo sobre o correto cumprimento das normas de segurança, os funcionários da empresa também o farão. A hipótese H3, referente à influência positiva do Controle Percebido na Conformidade (COP) com o cumprimento das PSIs (CPS) também foi confirmada ($\beta = 0{,}287$; $\rho < 0{,}001$), sugerindo que quanto mais conhecimento e habilidades os indivíduos tiverem sobre como seguir as regras de segurança da informação, maior será a conformidade com as PSIs (HU et al., 2012; BULGURCU; CAVUSOGLU; BENBASAT, 2010). A maneira mais eficaz disso ocorrer é através de treinamentos extensivos, 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).

Já a influência negativa do "jeitinho" (JB) no cumprimento das PSIs (CPS) também foi confirmada (β = -0,152; ρ < 0,001), validando a hipótese H4. Esse resultado demonstra que as metas e os objetivos de segurança da informação precisam 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, retratada aqui a partir da consciência do indivíduo, influencia tanto o comportamento do indivíduo quanto 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 ocasionalmente como meio para resolução de problemas, esse comportamento influencia negativamente a conformidade com as normas e políticas de segurança da informação instituídas pela organização.

Continuando a análise do modelo, verificou-se que a Consciência de Segurança da Informação (CSI) exerce uma forte influência (positiva e significativa) sobre a Atitude dos indivíduos quanto à conformidade com as PSIs (ATI), validando a hipótese H5 (β = 0,570; ρ < 0,001). Esse resultado também foi confirmado no estudo de Bulgurcu, Cavusoglu e Benbasat (2010), o qual identificou que quanto maior a consciência do indivíduo sobre a importância da segurança da informação, maior será a sua atitude em relação à conformidade com as PSIs. A hipótese H6, referente à influência positiva da Consciência de Segurança da Informação (CSI) nas Normas Subjetivas (NSU), também foi confirmada (β = 0,573; ρ < 0,001, indicando que uma maior compreensão sobre a segurança da informação influencia fortemente na percepção sobre a opinião de pessoas consideradas importantes em seu ambiente de trabalho. 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). Complementarmente, identificou-se também uma associação positiva e significativa entre a Consciência de Segurança da Informação (CSI) e o Controle Percebido (COP) (β = 0,663; ρ < 0,001), confirmando a hipótese H7, sendo essa a relação mais forte identificada entre a consciência de segurança da informação e o comportamento planejado dos indivíduos. Em outras palavras, quanto maior for

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 (FLORES; EKSTEDT, 2016). Diante desse resultado, a alta gerência deve introduzir programas de conscientização e treinamento que enfatizem a importância do cumprimento das normas e políticas de segurança da informação. Além disso, ela precisa definir claramente as funções e responsabilidades dos funcionários em relação à segurança, nutrindo 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; LOOCK; KRITZINGER, 2018). Assim, constatou-se que quando o indivíduo possui consciência e conhece suficientemente os problemas, riscos e custos associados aos possíveis problemas de segurança da informação, maior será o seu comportamento planejado quanto ao cumprimento das normas de segurança da informação presentes na organização.

O modelo estrutural ainda confirmou a proposição de que a Consciência de Segurança da Informação (CSI) influencia negativamente o "jeitinho brasileiro" (β = -0,377; $p < 0,001$), confirmando a hipótese H8, o que mostra que quanto maior a consciência do indivíduo sobre a importância da segurança da informação, menores serão as chances de comportamentos relacionados ao "jeitinho" serem seguidos, mesmo que percebidos como uma forma de resolver problemas. Por fim, confirmou-se a hipótese H9, sobre a influência da Conformidade com as PSIs (CPS) nas Falhas de Segurança da Informação relacionadas ao "jeitinho brasileiro" (FSI), identificando-se uma forte relação negativa e significativa (β = -0,517; $\rho < 0,001$). O resultado indica que seguir as normas de segurança da informação estabelecidas pela organização diminui consideravelmente a probabilidade de ocorrerem falhas de segurança que podem prejudicar a organização, pois os funcionários tendem a se policiar quanto ao cumprimento das PSIs (GLASPIE; KARAWOWSKI, 2017).

Os construtos Atitude, Normas Subjetivas e Controle Percebido explicam, em conjunto, 67,1% da variância do construto Conformidade com as PSIs, o que pode ser considerado um elevado poder de explicação (COHEN, 1988). Já a Conformidade com as PSIs explica 26,7% da variância do construto Falhas de Segurança da Informação, o que pode ser considerado de médio impacto (COHEN, 1988). 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 (f^2=0,114) e o "jeitinho brasileiro" (f^2=0,056) com o cumprimento das PSIs. Enquanto que nas relações entre a Atitude (f^2=0,163) e o Controle Percebido (f^2=0,165) com a Conformidade; e na relação entre a Consciência sobre a Segurança da Informação e o "Jeitinho

brasileiro", (f^2=0,166) o tamanho do efeito foi médio. Nas relações da Consciência com os construtos da TPB (Atitude, f^2=0,480; Normas Subjetivas, f^2=0,488; e Controle Percebido, f^2=0,784) e relação entre os construtos Conformidade e Falhas de Segurança (f^2=0,365), os efeitos identificados foram grandes. Para avaliar o grau de multicolinearidade dos construtos estudados, foi calculado o VIF, cujos valores ficaram dentro do recomendado (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. A tabela 3 destaca os resultados do modelo proposto.

Tabela 3 - Resultados da Análise de Equações Estruturais

Relações	Hipótese	VIF	Coeficiente (β)	t-valor	p-valor	f^2	R^2
ATI → CPS	H1	1,967	0,325	4,142	0,000	0,163	
NSU → CPS	H2	1,926	0,269	4,068	0,000	0,114	0,671
COP → CPS	H3	1,526	0,287	4,185	0,000	0,165	
JEI → CPS	H4	1,256	-0,152	3,261	0,001	0,056	
CSI → ATI	H5	1,000	0,570	9,125	0,000	0,480	0,324
CSI → NSU	H6	1,000	0,573	9,828	0,000	0,488	0,328
CSI → COP	H7	1,000	0,663	15,743	0,000	0,784	0,439
CSI → JEI	H8	1,000	-0,377	6,684	0,000	0,166	0,142
CPS → FSI	H9	1,000	-0,517	10,570	0,000	0,365	0,267

Fonte: autores da pesquisa.

4 CONSIDERAÇÕES FINAIS

A pesquisa teve por objetivo analisar como os aspectos culturais e organizacionais, relacionados à segurança da informação, influenciam os indivíduos no cumprimento das políticas de segurança da informação e na diminuição da ocorrência de falhas de segurança associadas ao "jeitinho brasileiro". Para isso, através de uma pesquisa *survey*, buscou-se testar um modelo específico, a fim de melhor compreender o tema abordado. A partir da análise dos resultados pode-se concluir, quanto às relações de causalidade, que todas as hipóteses formuladas foram confirmadas, demonstrando que a probabilidade de diminuição das falhas de segurança da informação relacionadas ao "jeitinho" é diretamente influenciada pelo cumprimento das políticas de segurança, sendo este influenciado pelo processo cognitivo (HU et al., 2012), que se forma pelo grau de conscientização do indivíduo quanto às políticas e normas de segurança da informação instituídas pela organização, resultado do nível de cultura de segurança presente na empresa. Os resultados aqui identificados comprovam que uma maior consciência individual sobre a importância da segurança da informação, essa que surge a partir

de uma cultura forte de segurança da informação, pode resultar na diminuição das falhas de segurança em organizações brasileiras.

Como contribuições gerenciais do estudo, destaca-se a análise de fatores organizacionais que influenciam o comportamento de segurança da informação, demonstrando aos gestores que ações práticas, como treinamentos, programas de conscientização e, inclusive, a elaboração e distribuição de cartilhas, ajudam a conscientizar os funcionários quanto às potenciais ameaças e riscos que todos correm ao utilizarem incorretamente a tecnologia disponível no seu ambiente de trabalho. 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 usuários 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 no ambiente em que estão inseridos (DA VEIGA; MARTINS, 2015).

As organizações devem entender que as melhores tecnologias de segurança existentes no mercado não podem impedir que um engenheiro social se faça passar por um usuário para obter códigos de acesso, por exemplo. Além disso, dificilmente impedirão que um estranho ou uma pessoa não autorizada entre em uma organização de mãos vazias e saia com um laptop cheio de dados confidenciais. É por esta razão que campanhas de conscientização, e até mesmo simulações de quebras de segurança ou invasões, têm sido implementadas como forma de alertar e sensibilizar os usuários sobre como evitar ou prevenir quebras de segurança da informação, além da importância de relatar incidentes de segurança, quaisquer que sejam. Entretanto, cabe ressaltar que para permanecerem eficazes, tais campanhas, simulações e capacitações devem ser realizadas periodicamente, e não por meio de um único exercício, à medida que novas ameaças e contramedidas são introduzidas rapidamente (DLAMINI; ELOFF; ELOFF, 2009). O compartilhamento do conhecimento sobre segurança da informação na organização, não apenas aumenta a conscientização dos seus funcionários, mas, também, evidencia a importância do cumprimento das políticas e procedimentos de segurança instituídas pela organização.

Como contribuições teóricas pode-se destacar o uso de modelos da área de TI para avaliar diferentes aspectos culturais, de modo a compreender o comportamento dos indivíduos quanto ao cumprimento de políticas e normativas relacionadas à segurança da informação. Pode-se constatar, também, que o uso da TPB, em conjunto com o construto Conformidade

com as PSIs, apresentou bons resultados, como sugerido por Cram, D'arcy e Proudfoot (2019). Além do que, a adaptação do instrumento de pesquisa e das questões relacionadas ao "Jeitinho Brasileiro", originalmente desenvolvidas 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 na Europa. Além disso, estudar a influência da Cultura de Segurança da Informação presente nas organizações brasileiras, por exemplo, também pode ser considerada uma importante contribuição, uma vez que as pesquisas elaboradas sobre os aspectos culturais e organizacionais e sua relação com o cumprimento de normas de segurança são escassos no Brasil (NASCIMENTO, 2012; BECK; SANTOS, 2010). 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 principal limitação do estudo, destaca-se a forma de seleção da amostra (não probabilística), o que exige cuidados quanto a sua generalização; e, apesar do trabalho ter atingido 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 única organização, para verificar a utilidade e usabilidade do modelo como ferramenta de apoio gerencial e, ainda, verificar, a partir de outra pesquisa futura, se as penalizações no caso de não cumprimento das PSIs possuem relação com a sua conformidade em organizações brasileiras, uma vez que 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, I. The theory of planned behavior. **Organizational Behavior and Human Decision Processes**, v. 50, n. 2, p. 179-211, 1991.

AJZEN, I.; MADDEN, T. 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, A.; DOS SANTOS, E. Adoção de Medidas de Segurança da Informação: a Influência das Respostas Estratégicas das Subunidades na Conformidade Organizacional. In: **Encontro de Administração da Informação**, São Paulo, SP. 2017.

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

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

BARLACH, L. O jeitinho brasileiro: traço da identidade nacional? **Revista Gestão & Políticas Públicas**, v. 3, n. 2, p. 228-245, 2013.

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

BERNARDO, P.; SHIMADA, N.; ICHIKAWA, E. 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.

BUENO, J.; ARANTES, P. A influência dos traços da cultura mineira no relacionamento de empresas de agronegócio do Triângulo Mineiro com seus clientes e fornecedores. **Revista Gestão da Produção Operações e Sistemas**, v. 10, n. 2, p. 141, 2015.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. 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, L. 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.

CHU, R.; WOOD JR, T. Cultura organizacional brasileira pós-globalização: global ou local? **Revista de Administração Pública**, v. 42, n. 5, p. 969-991, 2008.

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

CRAM, W.; D'ARCY, J.; PROUDFOOT, J. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. **MIS Quarterly**, v. 43, n. 2, p. 525-554, 2019.

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

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

DIAMANTOPOULOS, A.; SIGUAW, J. 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, T. 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.

DLAMINI, M.; ELOFF, J.; ELOFF, M. Information security: The moving target. **Computers & security**, v. 28, n. 3-4, p. 189-198, 2009.

ÉPOCA NEGÓCIOS. Os ataques cibernéticos explodem durante pandemia e expõem vulnerabilidades das empresas. 2020. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html. Acesso em: 14 fev. 2021.

FERNANDES, R.; HANASHIRO, D. Explorando aspectos indígenas da gestão numa organização financeira: jeitinho e sociedade relacional. **Revista de Administração Contemporânea**, v. 19, n. 3º Especial, p. 328-347, 2015.

FLORES, W.; EKSTEDT, M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. **Computers & Security,** v. 59, p. 26-44, 2016.

GALEGALE, N.; FONTES, E.; GALEGALE, B. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras1. **Perspectivas em Ciência da Informação**, v. 22, p. 75-97, 2017.

GLASPIE, H.; KARWOWSKI, W. 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, S.; CHENGALUR-SMITH, I. Metrics for characterizing the form of security policies. **The Journal of Strategic Information Systems**, v. 19, n. 4, p. 281-295, 2010.

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

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

HOVAV, A.; D'ARCY, J. 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.

HU, Q. 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, P. 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.

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

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

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

MARTINS, D. 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 em: 30 ago. 2019.

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

MONTESDIOCA, G.; MAÇADA, A. Measuring user satisfaction with information security practices. **Computers & Security**, v. 48, p. 267-280, 2015.

MOREIRA, A.; BORBA ROCHA, M. 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, F.; CALDAS, M. Introdução: cultura organizacional e cultura brasileira. **Cultura organizacional e cultura brasileira**. São Paulo: Atlas, p. 15-21, 1997.

MUZZIO, H. Cultura organizacional na perspectiva cultural regional brasileira. **Revista Brasileira de Gestão de Negócios**, v. 12, p. 447-463, 2010.

NASCIMENTO, E. 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, F.; DREVIN, L. Key elements of an information security culture in organisations. **Information & Computer Security**, v. 27, n. 2, p. 146-164, 2019.

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

SAMPIERI, R.; COLLADO, C.; LUCIO, M. D. P. B. 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, E. Coming to a new awareness of organizational culture. **Sloan Management Review,** v. 25, n. 2, p. 3-16, 1984.

SHERIF, E.; FURNELL, S.; CLARKE, N. 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, J. 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.

SOMMESTAD, T.; KARLZÉN, H.; HALLBERG, J. The theory of planned behavior and information security policy compliance. **Journal of Computer Information Systems**, v. 59, n. 4, p. 344-353, 2017.

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

THOMSON, K.; VON SOLMS, R.; LOUW, L. Cultivating an organizational information security culture. **Computer Fraud & Security**, v. 2006, n. 10, p. 7-11, 2006.

Apêndice A - Cenários hipotéticos (Falhas de Segurança da Informação)

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 Flávia consegue gerar o arquivo único, e repassar 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 repassar aos seus colegas as conclusões da análise.

Apêndice B - Itens do questionário

	Questão	Média	Desvio Padrão
Conformidade com as Políticas de Segurança da Informação – Adaptado de Ifinedo (2012)			
CPS3	Estou certo de que cumpro as normas de segurança da informação da empresa.	5,71	1,42
CPS2	Eu sigo as normas de segurança da informação da empresa.	5,84	1,33
CPS1	Eu cumpro com as normas de segurança da informação da empresa.	5,84	1,39
CPS4	Eu obedeço as regras de segurança da informação da empresa.	5,57	1,54
Atitude de Conformidade com as PSIs - Adaptado de Bulgurcu, Cavusoglu e Benbasat (2010)			
ATI1	Para mim, cumprir os requisitos de segurança da informação estabelecidos pela empresa é necessário.	6,26	1,04
ATI3	Para mim, cumprir com as regras de segurança da informação determinadas pela empresa é importante.	6,21	1,02
ATI4	Para mim, praticar as normas de segurança da informação estabelecidas pela empresa é adequado.	6,09	1,27
ATI2	Para mim, seguir as normas de segurança da informação de acordo com a empresa é benéfico.	5,97	1,31
Normas Subjetivas - Adaptado de Hu et al. (2012)			
NSU4	As pessoas que eu respeito na empresa pensam que eu devo seguir as normas de segurança da informação.	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.	5,93	1,45
NSU2	Pessoas importantes na empresa possuem opiniões que eu valorizo sobre as normas de segurança da informação.	5,75	1,54
NSU3	Pessoas que são importantes para mim na empresa pensam que eu devo seguir as políticas de segurança da informação.	5,67	1,57

Controle Percebido - Adaptado de Bulgurcu, Cavusoglu e Benbasat (2010)			
COP3	Eu tenho recursos e conhecimento para seguir as normas de segurança da informação disponibilizadas pela minha empresa.	6,11	1,30
COP4	Possuo as habilidades necessárias para seguir as regras de segurança da informação da minha empresa.	4,88	1,93
COP1	Eu sou capaz de seguir as regras de segurança da informação estabelecidos pela minha empresa.*	*5,78*	*1,45*
COP2	Tenho treinamento e habilidades adequadas para seguir as normas de segurança da informação definidos pela minha empresa.	5,62	1,63
Consciência de Segurança da Informação - Adaptado de Bulgurcu, Cavusoglu e Benbasat (2010)			
CSI3	Eu compreendo os riscos relacionados à segurança da informação para a empresa.	6,34	0,95
CSI4	Eu entendo as preocupações em relação à segurança da informação e os riscos que elas representam em geral.	6,36	1,11
CSI1	No geral, estou ciente das possíveis ameaças à segurança e suas consequências negativas à empresa.	6,06	1,28
CSI2	Eu tenho conhecimento suficiente sobre o custo de possíveis problemas de segurança da informação para a empresa.	5,42	1,67
Falhas de Segurança da Informação - Adaptado de Silveira et al. (2019)			
P3	Uso de mídias portáteis	5,06	1,83
P2	Uso de sites não confiáveis	4,94	1,97
P1	Uso de aplicativos piratas	4,70	1,98
Jeitinho brasileiro - Adaptado de Fernandes e Hanashiro (2015)			
JB2	Percebo que na empresa em que trabalho, em situações especiais para solucionar problemas, faz-se necessário adaptar-se e não cumprir com as normas de segurança da informação.	4,47	1,96
JB5	Percebo que na empresa em que trabalho, para atendimento de um pedido de ajuda, eventualmente, alguma regra de segurança da informação é contornada.	4,24	2,12
JB3	Percebo que na empresa em que trabalho, as regras de segurança da informação são contornadas, dependendo da situação.	4,14	2,13
JB4	Percebo que na empresa em que trabalho, as pessoas flexibilizam as normas relacionadas à segurança da informação, quando necessário.	3,78	2,00
JB1	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.	2,73	1,91

* Item excluído após as etapas de validação do instrumento.