UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

SUENY LÉDA ARAÚJO RIBEIRO

COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO: estudo aplicado às Universidades Federais do Brasil

João Pessoa
2023

SUENY LÉDA ARAÚJO RIBEIRO

COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO: estudo aplicado às Universidades Federais do Brasil

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação (PPGCI) da Universidade Federal da Paraíba (UFPB), vinculado à linha de pesquisa Ética, Gestão e Políticas de Informação, como requisito final à obtenção do título de Doutor em Ciência da Informação.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

João Pessoa

2023

R484c Ribeiro, Sueny Léda Araújo.
Comportamento humano em segurança da informação : estudo aplicado às Universidades Federais do Brasil / Sueny Léda Araújo Ribeiro. - João Pessoa, 2023.
172 f. : il.

Orientação: Wagner Junqueira de Araújo.
Coorientação: Marcelo de Santana Porte.
Tese (Doutorado) - UFPB/CCSA.

1. Segurança da informação. 2. Comportamento humano. 3. Teoria da Motivação de Proteção. 4. Universidades. I. Araújo, Wagner Junqueira de. II. Porte, Marcelo de Santana. III. Título.

UFPB/BC CDU 007:004.056(043)

SUENY LÉDA ARAÚJO RIBEIRO

COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO: estudo aplicado às Universidades Federais do Brasil

Data: 29 de março de 2023.

Resultado: Aprovada

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação (PPGCI) da Universidade Federal da Paraíba (UFPB), vinculado à linha de pesquisa Ética, Gestão e Políticas de Informação, como requisito final à obtenção do título de Doutor em Ciência da Informação.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br WAGNER JUNQUEIRA DE ARAUJO
Data: 06/04/2023 15:24:48-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Wagner Junqueira de Araújo
Orientador – PPGCI/UFPB

Documento assinado digitalmente
gov.br MARCELO DE SANTANA PORTE
Data: 04/04/2023 22:43:19-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Marcelo de Santana Porte
Coorientador - UFRN

Profa. Dra. Emeide Nóbrega Duarte
Membro Interno - PPGCI/UFPB

Prof. Dr. Fellipe Sá Brasileiro
Membro Externo - PPGC/UFPB

Documento assinado digitalmente
gov.br ALZIRA KARLA ARAUJO DA SILVA
Data: 06/04/2023 11:56:36-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Alzira Karla Araújo da Silva
Membro Interno - PPGCI/UFPB

Profa. Dra. Gabriela Fernandes Rocha
Membro Externo - UniFacisa

Prof. Dr. Marckson Roberto F. de Sousa
Membro Suplente Interno - PPGCI/UFPB

Prof. Dr. Danysson Axel Ribeiro Mota
Membro Suplente Externo - UFCA

Dedico

Ao meu marido, Fabiano, por me amar apesar de ... e aos meus filhos, José Roberto e Maria Fernanda, por compreender minhas ausências e suportar minhas impaciências durante este percurso. Vocês são o meu bem mais precioso!

AGRADECIMENTOS

Inicialmente agradeço ao meu **Deus** por ter me abençoado da forma sobrenatural durante todas as etapas desta pesquisa, principalmente quando achei que não conseguiria. Toda honra e toda glória rendo a Ti, Senhor.

Agradeço aos meus amados pais, **José Antônio Silva Araújo** e **Solane Gomes Léda Araújo** que, apesar da distância, sempre apoiaram minhas escolhas e me amaram da forma mais doce e leve que só pais conseguem fazê-lo.

Agradeço ao meu amor, marido, companheiro e cúmplice, **Fabiano de Moura Ribeiro**, pelo apoio sem restrição em todos os momentos desta pesquisa.

Agradeço aos meus filhos, **José Roberto** e **Maria Fernanda** pelo amor incondicional, pelo sorriso nos momentos difíceis, e por me mostrar que perto deles tudo se torna muito pequeno.

Agradeço ao meu orientador, **Prof. Dr. Wagner Junqueira de Araújo**, pela parceria, amizade, atenção e paciência no desenvolvimento desta pesquisa.

Agradeço ao meu coorientador, **Prof. Dr. Marcelo de Santana Porte**, pela orientação e paciência durante a construção desta tese.

Agradeço aos docentes **Profa. Dra. Emeide Nóbrega Duarte, Profa. Dra. Alzira Karla Araújo da Silva, Prof. Dr. Marckson Roberto Ferreira de Sousa**, **Prof. Dr. Fellipe Sá Brasileiro e Profa. Dra. Gabriela Fernandes Rocha** por participarem da Banca Examinadora e pelas valorosas contribuições.

Agradeço as amigas **Christiane** (Chris) e **Rafaela Romaniuc** (Rafa) por não permitir que essa escrita fosse um processo tão solitário.

Agradeço à amiga e professora **Profa. Dra. Rafaela Formiga**, pelo exemplo de amor e dedicação à pesquisa, além da valorosa contribuição.

Agradeço à amiga **Clarissa Sá**, pela ajuda e ombro amigo em todos os momentos desta caminhada.

Agradeço à amiga **Renata Batista** que colaborou de forma tão carinhosa com as últimas etapas desta pesquisa.

Agradeço à equipe da Divisão de Educação e Capacitação Profissional (DECP), aos amigos **Marcia Sandra, Rebeca, Edivânia, Antônio, Francisco e Jura** pelo incentivo e pelas gargalhadas tão necessárias nos momentos difíceis.

Agradeço ao grupo **Conectados para Edificar**, representado pela amiga e **irmã Kainara** e pelo **Pastor Crisojônio**, e aos membros da minha célula, representado por **Ricardo e Rafaela** pelas orações, indispensáveis em todos os momentos desta pesquisa.

Agradeço à amiga **Tatiana Aguiar** por seus preciosos ensinamentos e apoio.

E por fim, agradeço a **todos os amigos** que responderam e compartilharam, de forma tão intensa, ao questionário dessa pesquisa.

Para todas as coisas tenho força graças Àquele que me dá o poder.
(Filipenses 4:13)

RESUMO

Constituindo-se como elemento essencial para o desenvolvimento da sociedade, responsável pelas transformações tecnológicas, administrativas e organizacionais, a informação tem sido considerada um dos ativos mais importantes para as organizações. Em virtude da importância desses ativos de informação, as organizações, de modo geral, necessitam protegê-los contra destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada. Nesse sentido, a gestão da informação, importante constituinte da expansão organizacional, precisa considerar a aplicabilidade da segurança da informação como um dos procedimentos essenciais de sua estratégia, com base em uma abordagem completa cujas dimensões tecnológicas, normativas e humanas sejam contempladas, perante a necessidade urgente da aplicação de uma abordagem interdisciplinar em que o fator humano deve desempenhar um papel fundamental. Nesse contexto, esta pesquisa teve como objetivo analisar o comportamento em segurança da informação dos servidores das universidades federais brasileiras, sob a ótica da Teoria da Motivação de Proteção. Para tanto, a pesquisa caracterizou-se como aplicada, cujos objetivos classificam-na como descritiva e correlacional com apoio na abordagem quali-quantitativa, onde foram utilizadas entrevistas com especialistas e a aplicação de questionário *on-line* aos gestores de segurança e aos servidores (técnicos e docentes) das universidades federais, e, para análise dos dados, aplicamos a estatística descritiva e inferencial. Os resultados indicaram que, dos controles relacionados ao comportamento humano, a política de segurança da informação, o controle de acesso físico e a política de uso do correio eletrônico são os mais utilizados. A conscientização e a capacitação em segurança da informação ainda são abordadas de forma inexpressiva pelas universidades. No que concerne ao aspecto quantitativo, a análise de correlação entre as variáveis desta pesquisa possibilitou o entendimento da relação entre a Teoria da Motivação de Proteção e a intenção do comportamento de prevenção dos servidores, uma vez que tanto as variáveis primárias da Teoria da Motivação de Proteção (vulnerabilidade percebida, gravidade percebida da ameaça, eficácia de resposta e autoeficácia), com exceção do custo de resposta, quanto as variáveis adicionadas ao modelo (gravidade percebida das sanções, normas injuntivas, normas descritivas, conscientização, capacitação e fortalecimento da política) apresentaram uma relação significativa com o comportamento de prevenção. A identificação das variáveis que apresentaram uma relação significativa com a intenção de comportamento de prevenção em segurança da informação mostra uma direção para alcançar um aumento dessa intenção comportamental e, assim, contribuir para a redução do número de incidentes em segurança nas universidades públicas federais brasileiras. Portanto, esse estudo não apenas expande nossa compreensão teórica sobre a intenção de comportamento de prevenção, mas também, fornece uma orientação prática às universidades sobre as ações estratégicas voltadas ao comportamento dos servidores dessas instituições.

Palavras-chave: segurança da informação; comportamento; teoria da motivação de proteção; universidades.

ABSTRACT

As an essential element for the development of the society, responsible for technological, administrative and organizational transformations, information has been considered one of the most important assets for organizations. Due to the importance of these information assets, organizations, in general, need to protect them against destruction, temporary unavailability, tampering or unauthorized disclosure. In this sense, the management of information assets, an important pilar of organizational progress, needs to consider the applicability of information security as one of the essential procedures of its strategy, based on a complete approach where technologies, organizational norms and human are dimensions contemplated, in view of the urgent need to apply an interdisciplinary approach in which the human factor must play a fundamental role. In this context, this research aimed to analyze the behavior in information security of public employees of federal universities in Brazil, from the perspective of the Theory of Protection Motivation. Therefore, the research was characterized as applied, whose objectives classify it as descriptive and correlational with support in the quali-quantitative approach, where interviews with specialists and the application of online questionnaires to public employees, managers of information security, as well as public employees in general were used (technicians and professors) from federal universities all over Brazil. And, for data analysis, we applied descriptive and inferential statistics. The results indicated that, of the controls related to human behavior, the information security policy, the physical access control and the e-mail usage policy are the most used. Information security awareness and training are still poorly addressed by universities. With regard to the quantitative aspect, the correlation analysis between the variables of this research made it possible to understand the relationship between the Theory of Protection Motivation and the intention of the employees' prevention behavior, since both the primary variables of the Theory of Motivation of Protection (perceived vulnerability, perceived threat severity, response effectiveness and self-efficacy), with the exception of response cost, as well as the variables added to the model (perceived severity of sanctions, injunctive norms, descriptive norms, awareness, capacity building and policy strengthening) both showed a significant relationship with prevention behavior. The identification of the variables that showed a significant relationship with the intention of information security prevention behavior shows a direction to achieve an increase in this behavioral intention and, thus, contribute to the reduction of the number of security incidents in federal public universities of Brazil. Therefore, this study not only expands our theoretical understanding of the intention of prevention behavior, but also provides practical guidance to universities on strategic actions aimed at the behavior of the employees at these institutions.

Keywords: *information security; behavior; protection motivation theory; universities.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

As organizações, crescentemente, veem a informação como um dos seus ativos mais valiosos, constituindo-se como um elemento essencial para o desenvolvimento da sociedade, sendo responsável pelas transformações tecnológicas, administrativas e organizacionais (BUNKER, 2012; LEIDNER, 2010). Em virtude da importância desses ativos de informação, as organizações, de modo geral, necessitam protegê-los contra destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada (ABNT NBR ISO/IEC 27002, 2013). Para tanto, a segurança da informação tem se tornado um aspecto crítico e importante no ambiente organizacional (KEARNEY; KRUGER, 2016). À medida que a importância da informação cresce, crescem também os incentivos indevidos relativos ao acesso e ao abuso da informação cometidos por hackers, descontentes, criminosos e terroristas (DOHERTY; TAJUDDIN, 2018).

Nessa conjuntura, por representar um conceito amplo, a segurança da informação tem sido estudada por múltiplas áreas, tanto nas ciências exatas (estudando a tecnologia), como nas ciências sociais (estudando o comportamento humano e os processos). Dentre as áreas das ciências sociais preocupadas com essa temática de pesquisa, inclui-se a ciência da informação. A partir da divisão da ciência da informação em seis subáreas proposta, a temática segurança da informação encontra-se inserida na subárea de gestão do conhecimento, concentrando suas pesquisas nas dimensões de processos e pessoas (ARAÚJO, 2014).

As pesquisas nessas ciências, com base nas necessidades organizacionais, ou do indivíduo, estruturaram a segurança da informação como uma disciplina que abrange ações necessárias, que buscam garantir, conforme necessidades específicas, a preservação da informação com base em três propriedades: confidencialidade, integridade e disponibilidade (SÊMOLA, 2014). Essas propriedades representam a sobrevivência de qualquer organização, cuja interferência, direta ou indireta, em algum de seus processos, pode acarretar grandes prejuízos. Assim, ressalta-se a necessidade de uma gestão da segurança da informação que contemple, de forma eficiente, os diversos tipos de informações que são criadas, manuseadas e/ou protegidas pelas organizações.

Algumas organizações ainda possuem uma abordagem centrada estritamente em soluções baseadas em tecnologia para abordar a segurança da informação. Para Safa *et al.* (2015) essa abordagem não garante a seguridade do negócio no contexto da gestão da segurança da informação, destacando que a tecnologia, unicamente como equipamento tecnológico e

componentes lógicos computacionais, não é capaz de estabelecer a proteção da informação contra ameaças, evidenciando que falhas humanas devem ser consideradas. Corroborando essa ideia, para Yupanqui e Oré (2018), uma proteção da segurança da informação baseada apenas em uma perspectiva tecnológica, culmina em uma abordagem incompleta, demonstrando a necessidade de uma visão ampla com base em uma abordagem interdisciplinar, na qual o humano é considerado como principal componente da segurança da informação.

Doherty e Tajuddin (2018) destacam que incidentes de segurança da informação, como violações de confidencialidade, fraude de computador, utilização indevida dos sistemas de informação e infecções por vírus são comumente identificados, em vez de problemas técnicos. De acordo com o relatório anual da IBM (2022), os vetores relacionados ao comportamento humano em segurança da informação representaram 30% dos ataques, gerando um custo médio de US$ 13,19 milhões para as empresas que participaram da pesquisa. Desse modo, para garantia de um ambiente seguro para a informação, os aspectos humanos devem ser tomados em consideração, além dos aspectos tecnológicos, para que possa haver uma efetiva gestão da segurança da informação, cuja raiz das falhas dos usuários da informação são, essencialmente, a falta de conscientização da segurança da informação, a ignorância, a negligência, a apatia, a resistência e a malícia dos funcionários (SAFA; VON SOLMS; FURNELL, 2016).

Nesse contexto, embora as pessoas sejam frequentemente referidas como o elo mais fraco na segurança da informação, são exatamente elas que podem desempenhar um papel essencial na salvaguarda da informação (CONNOLLY *et al.*, 2017; DANG-PHAM; PITTAYACHAWAN; BRUNO, 2017; JANSEN; VAN SCHAIK, 2018; PARSONS *et al.*, 2017; SAMPAIO; MANCINI, 2007; SNYMAN; KRUGER, 2017; SOHRABI SAFA; VON SOLMS; FURNELL, 2016). Entretanto, para que ocorra a prática de um comportamento preventivo, é necessário que os indivíduos estejam conscientes dos riscos e vulnerabilidades, bem como capacitados para o enfrentamento de possíveis ameaças. Nessas circunstâncias, é imprescindível uma abordagem no comportamento humano em segurança da informação (JANSEN; VAN SCHAIK, 2018).

Para Safa *et al.* (2018), no ambiente organizacional, as ameaças internas vêm atraindo a atenção de vários especialistas em segurança da informação em que, com base em suas observações exploratórias, identificaram duas considerações particularmente importantes: a motivação e a oportunidade (2018). A partir desses aspectos, tornou-se possível analisar de forma direcionada o comportamento dos usuários/funcionários da informação organizacional. Assim, torna-se salutar estudar o comportamento em segurança da informação dos

usuários/funcionários, observando suas motivações perante um possível comportamento preventivo em organizações, sejam nas dimensões públicas ou privadas.

De acordo com a 24ª edição do Relatório do Symantec (2019), o Brasil foi o quarto país que mais sofreu ciberataques[1], entre os 157 países analisados, ficando atrás apenas dos Estados Unidos, China e Índia. Ainda, segundo o mesmo relatório, as instituições públicas representam o quinto setor com maior número de ataques por *phishing*[2]. Nesse contexto de vulnerabilidade, estão inseridas as universidades públicas federais, instituições produtoras de conhecimento que necessitam de uma gestão de segurança da informação que contemple de forma eficiente os diversos tipos de informações que são por elas criadas, manuseadas e/ou protegidas, que variam de informações ostensivas a sigilosas. Ainda nesse sentido, para Menard *et al.* (2018) as universidades estão entre as organizações globais menos seguras, pois apenas algumas universidades desenvolveram políticas de segurança da informação abrangentes que envolvem programas de capacitação e conscientização adequados.

As universidades públicas, bem como todos os órgãos da administração pública federal, direta e indireta, dispõem de orientações para gestão de segurança da informação que devem ser observadas e implementadas pelos respectivos órgãos com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional (BRASIL, 2020). Esses órgãos produzem e tratam informações diariamente na rotina de trabalho de seus agentes públicos[3], ocupando relevância fundamental para a gestão da máquina pública e para o processo de tomada de decisões quanto às políticas públicas federais. Em seu processo administrativo, o tratamento dos ativos de informação precisa ser realizado de modo ético e responsável pelos agentes dos órgãos e entidades públicas federais e com respeito à legislação vigente (BRASIL, 2014).

Nessa direção, este estudo desenvolveu uma pesquisa sobre o comportamento em segurança da informação dos servidores das universidades federais brasileiras, perante a necessidade e relevância da temática tanto no contexto da segurança da informação, como no âmbito da administração pública federal. Com essa pesquisa, pretende-se preencher a lacuna identificada na Revisão Sistemática de Literatura (RSL), realizada e apresentada neste trabalho,

[1] Também chamado de ataque cibernético, é qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo.
[2] *Phishing* é uma maneira desonesta que cibercriminosos usam para enganar o usuário a revelar informações confidenciais ou pessoais. Geralmente, o remetente se disfarça como legítimo e solicita que o destinatário execute uma ação, como clicar em um *link* fornecido.
[3] Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF (BRASIL, 2014).

em que não foi identificado nenhum estudo aplicado ao comportamento em segurança da informação dos servidores em universidades federais do Brasil. Lacuna apresentada anteriormente na pesquisa de Yupanqui e Oré (2017) em que os autores não identificaram, durante sua RSL, nenhuma pesquisa desenvolvida na América do Sul e na América Central.

Quanto ao suporte teórico, nesta pesquisa, os comportamentos dos servidores das universidades foram estudados a partir da Teoria da Motivação de Proteção (TMP). A escolha pela TMP deu-se por ser a teoria comportamental mais utilizada nas pesquisas identificadas durante a RSL. Essa teoria tem ganhado cada vez mais atenção nas pesquisas em segurança da informação (HAAG; SIPONEN; LIU, 2021; JANSEN; VAN SCHAIK, 2018a; LI *et al.*, 2019; ORAZI; JOHNSTON; WARKENTIN, 2019). Isso ocorre porque a motivação representa as razões para as ações, necessidades e desejos das pessoas. A motivação define a direção e as razões de um padrão comportamental específico. Um motivo leva a pessoa a se comportar de uma maneira específica (SAFA; VON SOLMS, 2016). Para Rajab e Eydgahi (2019), a TMP fornece o melhor arcabouço teórico para compreender o comportamento dos funcionários das universidades em relação à segurança da informação.

Diante do exposto, a pesquisa respondeu aos seguintes questionamentos: Qual o comportamento em segurança da informação dos servidores das universidades federais do Brasil, a partir da TMP? Quais os controles de segurança da informação, relacionados ao comportamento humano, compõem a gestão da segurança da informação das universidades federais do Brasil?

A definição das hipóteses da pesquisa foi estabelecida com base nos dois processos cognitivos centrais da TMP que influenciam a intenção do comportamento de prevenção: avaliação de ameaça e avaliação de enfrentamento. A TMP organiza suas variáveis em torno desses dois processos, que resultam em cinco variáveis: da avaliação de ameaça surgem – vulnerabilidade percebida e gravidade percebida; da avaliação de enfrentamento surgem – eficácia de resposta, autoeficácia e custo de resposta (FLOYD; PRENDICE-DUNN; ROGERS, 2000).

Embora essa teoria seja a espinha dorsal desta pesquisa, inserimos outras variáveis, adaptadas a partir de pesquisas de Hina, Selman e Lowry (2019); Rajab e Eydgahi, (2019) e Jansen e Van Schaik (2017), identificadas na RSL. Na avaliação de ameaças, inserimos a variável gravidade percebida das sanções, e na avaliação de enfrentamento, inserimos as variáveis normas injuntivas, normas descritivas, fortalecimento da política de segurança da informação, capacitação e conscientização. De certo modo, a experiência e as crenças dos servidores em relação à segurança, as ações de conscientização e a capacitação oferecida por

suas instituições têm um efeito significativo na percepção da gravidade da segurança da informação (LI *et al.*, 2019). A ampliação da TMP, a partir da inclusão de novas variáveis, tornou a teoria mais adequada para uma melhor compreensão sobre o comportamento em segurança da informação dos servidores das universidades federais. Assim, foram estabelecidas as seguintes hipóteses de pesquisa, conforme podem ser observadas no Quadro 1.

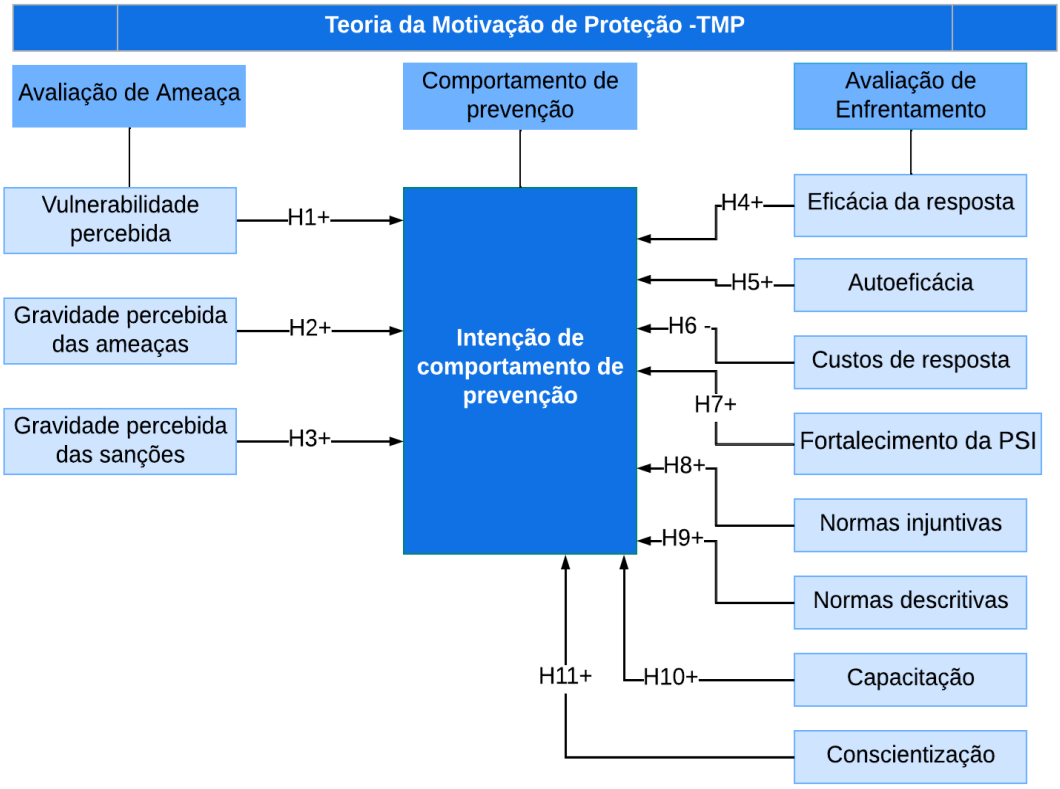
Quadro 1 - Hipóteses da pesquisa

Avaliação de ameaça
H1 A vulnerabilidade percebida está relacionada positivamente com a intenção de comportamento de prevenção.
H2 A gravidade percebida da ameaça está relacionada positivamente com a intenção de comportamento de prevenção.
H3 A gravidade percebida das sanções está relacionada positivamente com a intenção de comportamento de prevenção.
Avaliação de enfrentamento
H4 A eficácia da resposta está relacionada positivamente com a intenção de comportamento de prevenção.
H5 A autoeficácia está relacionada positivamente com a intenção de comportamento de prevenção.
H6 O custo de resposta está relacionado negativamente com a intenção de comportamento de prevenção.
H7 As normas injuntivas estão relacionadas positivamente com a intenção de comportamento de prevenção.
H8 As normas descritivas estão relacionadas positivamente com a intenção de comportamento de prevenção.
H9 A conscientização está relacionada positivamente com a intenção de comportamento de prevenção.
H10 O fortalecimento da política está relacionado positivamente com a intenção de comportamento de prevenção.
H11 A capacitação está relacionada positivamente com a intenção de comportamento de prevenção.

Fonte: Elaborado pela autora (2023).

A partir da TMP e da formulação das hipóteses, foi construído um modelo de pesquisa, apresentado na Figura 1, que foi testado no contexto das universidades federais.

Figura 1 - Modelo da pesquisa



Fonte: Elaborado pela autora (2023).

Para responder aos questionamentos da pesquisa e testar o modelo proposto, foi necessário atingir o objetivo geral de analisar o comportamento em segurança da informação dos servidores das universidades federais brasileiras, sob a ótica da Teoria da Motivação de Proteção. Para tanto, foi preciso alcançar os seguintes objetivos específicos:

a) Realizar uma Revisão Sistemática de Literatura – RSL sobre a temática comportamento humano em segurança da informação;
b) Identificar quais controles, relacionados ao comportamento humano, são utilizados pelos servidores das universidades federais;
c) Investigar as relações entre: vulnerabilidade percebida. gravidade percebida das ameaças, gravidade percebida das sanções, eficácia da resposta, autoeficácia, normas injuntivas, normas descritivas, conscientização, fortalecimento da política e capacitação com a intenção de comportamento de prevenção dos servidores;
d) Desenvolver um modelo de comportamento preventivo para as universidades federais, baseado na Teoria da Motivação de Proteção.

A pesquisa foi desenvolvida com base em uma metodologia científica no campo das ciências sociais que procurou obter conhecimentos no contexto do comportamento em

segurança da informação dos servidores das universidades federais. Para tanto, a pesquisa caracterizou-se como aplicada, cujos objetivos classificam-na como descritiva e correlacional com apoio na abordagem quali-quantitativa. A utilização da pesquisa aplicada justifica-se por essa metodologia permitir que o conhecimento gerado possa ser direcionado para a solução de problemas específicos do cotidiano. A pesquisa descritiva e correlacional foram adotadas pela necessidade de atingir os objetivos específicos b) e c), respectivamente. A opção pela abordagem quali-quantitativa surgiu da necessidade de aplicação de entrevistas semiestruturadas e questionário *on-line.*

Esta pesquisa foi motivada, em parte, pelo cenário atual de pesquisas incipientes sobre a temática comportamento humano em segurança da informação no âmbito da ciência da informação. De acordo com o levantamento elaborado por Araújo (2016), no período de 2007 a 2015, do total de trabalhos publicados nos anais do evento de referência dessa área no Brasil – Encontro Nacional de Pesquisa em Ciência da Informação (Enancib) – foram identificadas dez pesquisas que abordaram a temática 'segurança da informação'. A partir da pesquisa de Araújo (2016), realizamos uma atualização, ampliando o período para os anos de 2007 a 2022, o que possibilitou a identificação de mais oito publicações que abordaram a temática, conforme Quadro 2

Quadro 2 - Publicações sobre segurança da informação identificadas no Enancib

Título da publicação	Ano	Instituição	Autores
Percepções de segurança e ameaças em ambientes de tecnologias da informação	2007	UNESP UFPB	Miguel Maurício Isoni e Silvana Aparecida B. G. Vidotti
Segurança da informação: nova disciplina na ciência da informação?	2010	UNB	Jorge Henrique Cabral Fernandes
A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento.	2010	UFPB UNB	Wagner Junqueira Araújo e Suely Angélica do Amaral
O Blood Project: uma iniciativa para organização da informação em biomedicina.	2011	UFMG	Maurício Barcellos Almeida, Kátia Cardoso Coelho, André Queiroz Andrade, Luciana Emirena Santos Carneiro, Joel Augusto Oliveira, Fabrício Martins Mendonça e Renato Rocha Souza
Brasil informacional: a segurança cibernética como desafio à segurança nacional	2011	UFMG	Rafael Oliveira de Ávila e Rafael Pinto da Silva

Título da publicação	Ano	Instituição	Autores
Análise de informações pessoais na web: métrica para identificar o grau de exposição da informação	2013	UFPB	Narjara Bárbara Xavier da Silva, Wagner Junqueira de Araújo e Patrícia Morais de Azevedo
Análise de risco no sistema de concessão de diárias e passagens (SCDP): estudo de caso sob a ótica da segurança da informação no departamento contábil da UFPB	2013	UFPB	Josivan de Oliveira Ferreira e Wagner Junqueira de Araújo
Escola politécnica da UFBA e a assessoria de segurança e informação	2014	UFBA	Louise Anunciação Fonseca de Oliveira, Anne Alves da Silveira e Jussara Borges.
Modelo para o descarte seguro da informação em suporte digital	2014	UFPB	Silvio Lucas da Silva e Wagner Junqueira de Araújo
Aspectos humanos da segurança da informação	2015	UFPB	Sueny Gomes Léda Araújo, Rafaela Romaniuc Batista e Wagner Junqueira de Araújo
Análise da dimensão humana no processo de gestão de segurança da informação	2016	UFPB	Sueny Gomes Léda Araújo e Wagner Junqueira de Araújo
Privacidade: perspectivas da ciência da informação sobre o contexto acadêmico.	2017	UFSC	Andressa Stival Cordeiro e Enrique Muriel-Torrado
A proteção da informação em ambientes digitais – tendências e perspectivas	2018	UnB	Eduardo Wallier Vianna e Renato Tarciso Barbosa Sousa
Internet das coisas e privacidade: uma revisão sistemática da literatura.	2018	FUMEC	Jeferson Gonçalves de Oliveira, Paulo Augusto Isnard Santos, Cristiana Fernandes de Muyder, Rodrigo Moreno Marques
A efetividade dos sistemas de informação nas organizações sob o foco da qualidade, sistemas, segurança e gestão da informação	2018	FUMEC[4] UEMG	Cláudia Reis de Paula Kleinsorge, Renata de Souza França, Eric de Paula Ferreira, Paulo Augusto Isnard e Fabricio Ziviani
Ciber terrorismo na Paraíba	2019	UFPB	Wagner Junqueira de Araújo e José Roberto Cavalcante da Silva
Contribuições da ciência da informação para a segurança da informação: uma abordagem teórica	2019	UFMG	Rafael dos Santos Nonato e Elisangela Cristina Aganette
Gestão da informação e sistemas de gestão de segurança da informação: modelo para a garantia de	2022	UFMG	Rafael dos Santos Nonato e Elisângela Cristina Aganette

[44] Fundação Mineira de Educação e Cultura

Título da publicação	Ano	Instituição	Autores
disponibilidade em processos de contratação			

Fonte: Elaborado pela autora (2023).

Os resultados indicam que dos 16 anos pesquisados, foram identificadas 18 publicações abordando a temática ‘segurança da informação’. Essa recorrência demonstra que a temática continua emergindo na ciência da informação em contexto nacional. Entretanto, das 18 publicações identificadas, apenas as pesquisas de Araújo, Batista e Araújo (2015) e a de Araújo e Araújo (2016) abordaram o comportamento humano em segurança da informação.

Devido à relevância da segurança da informação para as organizações, bem como por ser uma temática recorrente em outras áreas como informática, psicologia e administração, torna-se salutar que a ciência da informação aborde de forma mais contundente a referida temática de modo a contribuir com o esclarecimento de problemáticas em contexto social, ainda carente de estudos que direcionem a possíveis soluções. Santana (2021) alerta para necessidade do profissional da área de ciência da informação, seja gestor, técnico e/ou cientista, adquirir conhecimentos para entender e poder atuar competentemente em equipes multidisciplinares no âmbito dos desafios associados à segurança da informação. Ainda nesse sentido, Araújo (2009) destaca que a segurança da informação era pouco pesquisada na ciência da informação, mantendo-se, todavia, objeto de estudo em outras áreas do conhecimento.

Outro importante motivador para o desenvolvimento da pesquisa, refere-se ao contexto das universidades públicas, ambiente profissional da pesquisadora, deste estudo, que convive com a complexidade de uma instituição produtora de conhecimento contínuo que produz, manuseia e armazena, constantemente, informações para o seu funcionamento organizacional, que depende de recursos humanos, formado por servidores (técnico-administrativos e docentes) para movimentar a sua dinâmica informacional. Além disso, o desejo da pesquisadora em continuar estudando a temática comportamento humano em segurança da informação, iniciado durante o mestrado.

Diante da apresentação desses aspectos motivacionais, a justificativa fundamenta-se pelo potencial contribuição teórica, prática e social da pesquisa. A contribuição teórica encontra-se associada à ampliação do modelo da TMP, a partir da inclusão das variáveis gravidade percebida das sanções, normas injuntivas, normas descritivas, fortalecimento da política de segurança da informação, capacitação e conscientização. A contribuição prática dá-se pelo desenvolvimento de um modelo de comportamento preventivo para universidades federais, baseado na TMP. Para a contribuição social da pesquisa, pode-se referenciar ao fato

de que as constatações do estudo podem ser determinantes para que os profissionais de segurança, não apenas das universidades, mas dos diversos segmentos, desenvolvam estratégias de segurança da informação que contribuam, efetivamente, no desenvolvimento de um comportamento preventivo dos funcionários de distintas organizações.

Para uma melhor compreensão, esta tese divide-se em seis seções: primeiro com essa seção introdutória, seguido pelo referencial teórico, procedimentos metodológicos, apresentação e análise dos dados, considerações finais e, por fim, as referências da pesquisa.

2 REFERENCIAL TEÓRICO

O referencial teórico encontra-se constituído em duas partes. A primeira apresenta um estudo exploratório e quanti-qualitativo das produções científicas sobre a temática comportamento humano em segurança da informação, para tanto, foi realizada uma Revisão Sistemática de Literatura (RSL). A segunda parte é composta da revisão dissertativa sobre o Comportamento Humano em Segurança da Informação e a Teoria da Motivação de Proteção.

2.1 REVISÃO SISTEMÁTICA DE LITERATURA SOBRE COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO

Esta subseção foi realiza no intuito de cumprir o primeiro objetivo específico desta pesquisa que foi o de realizar uma RSL sobre comportamento humano em segurança da informação. Nesse sentido, para uma melhor compreensão de como as pesquisas nessa temática foram desenvolvidas, realizamos as análises bibliométrica e lexicométrica das principais características dessas produções. Para Samapio e Mancini (2007) a importância da RSL dá-se principalmente pela acumulação de resultados de pesquisas científicas. Kitchenham *et al.*, (2009) acrescentam que a RSL agrega evidências existentes sobre uma questão de pesquisa, norteia o desenvolvimento de projetos, indica novos rumos para futuras investigações, identifica quais métodos de pesquisa foram utilizados em determinada área e, destina-se também a apoiar os profissionais no desenvolvimento de diretrizes baseadas em evidências. Além disso, é um processo metodologicamente rigoroso para revisão de resultados de pesquisas, sendo passível de reprodução (KITCHENHAM *et al*., 2009; SAMPAIO; MANCINI, 2007).

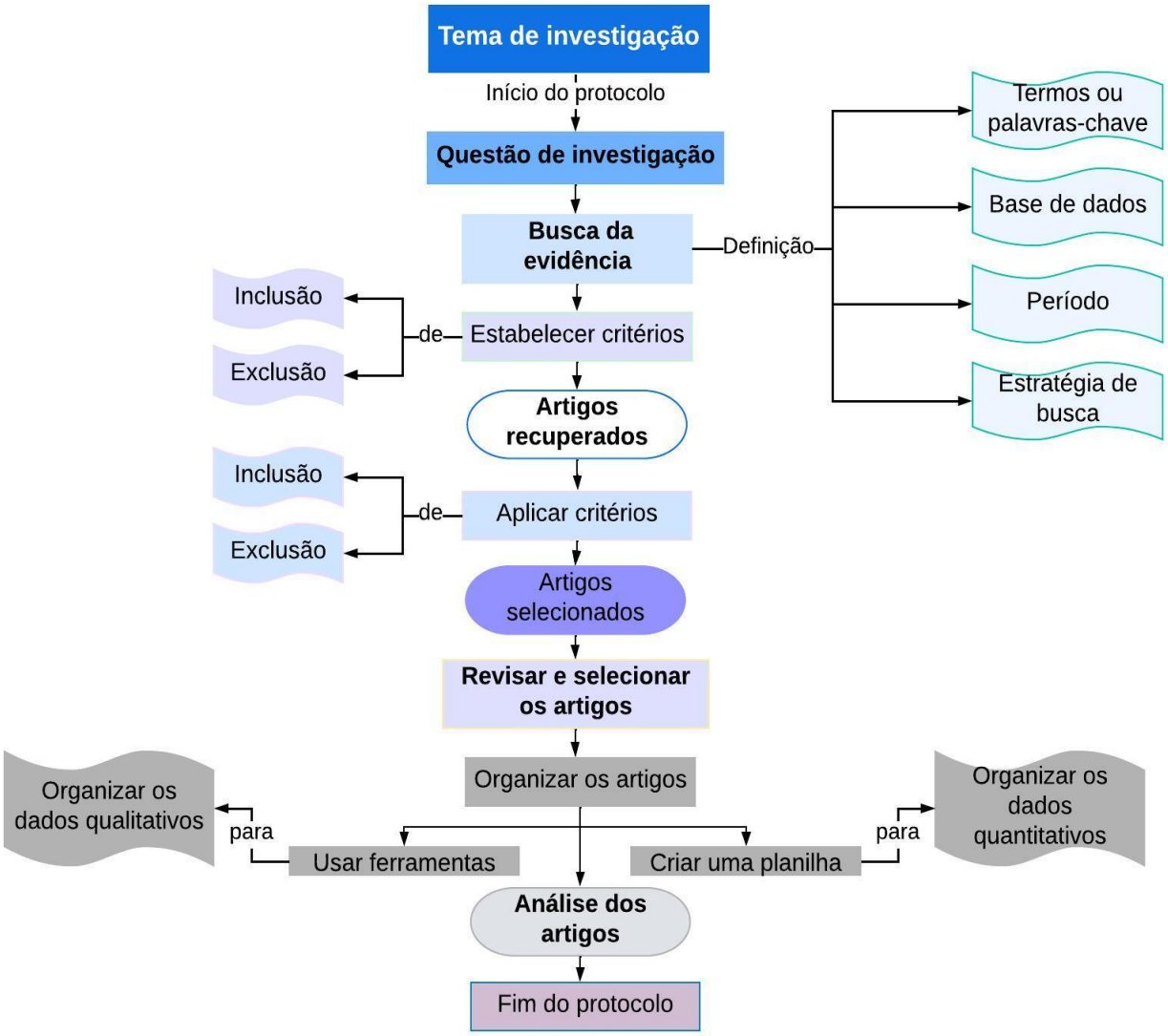
A análise bibliometria é uma abordagem metodológica quantitativa, com raízes na Ciência da Informação, que aplica métodos estatístico e matemáticos, comumente voltados para a análise, identificação de padrões e avaliação da produção científica (CAMARGO; BARBOSA, 2018).

Quanto a análise lexicométrica, esta pode ser caracterizada como uma estratégia que aplica métodos quantitativos, estatística descritiva e inferencial a dados qualitativos, textos, com o objetivo de realizar observações sobre as características de um conjunto de comunicações (SOUSA, 2021). Para Bardin (2010), a lexicometria pode ser útil nos seguintes casos: quando a unidade de registro é a palavra e o indicador principal é a sua frequência; quando a análise é complexa e multivariada, o que exige um tratamento simultâneo de categorias e unidades de

registro; quando se deseja analisar a concorrência de palavras em unidades de contexto; quando a investigação possui etapas sucessivas e a análise demanda tratamentos estatísticos complexos. Da mesma forma que a RSL, a lexicometria exige a adoção de procedimentos sistemáticos e objetivos, no sentido de garantir que as etapas envolvidas no processo de análise possam ser explicitadas e replicadas (SOUSA, 2021).

O desenvolvimento dessa RSL toma como referência as estruturas propostas por Yupanqui e Oré (2018), Kitchenham *et al.* (2009) e Sampaio e Mancini (2007). Para esses autores, é necessário elaborar um protocolo de pesquisa que contemple quatro passos: 1 - preparação de uma questão de pesquisa bem formulada e clara; 2 - busca das evidências, a partir da definição de termos ou palavras-chave, seguida das estratégias de busca, definição das bases de dados e de outras fontes de informação a serem pesquisadas; 3 – estabelecimento de critérios de inclusão e exclusão dos artigos; e 4 - revisão e seleção dos artigos. O protocolo dessa RSL está ilustrado na Figura 2, na qual estão indicados a sequência de execução e os processos envolvidos. Com base no protocolo da pesquisa desenvolvido para esta RSL, foi elaborada a seguinte questão de pesquisa: quais as principais características das produções científicas relacionadas ao comportamento humano em segurança da informação?

Figura 2- Protocolo de pesquisa



Fonte: Elaborado pela autora (2022) a partir de Sampaio e Mancini (2007); Yupanqui e Oré (2018); Kitchenham *et al.* (2009).

A partir da definição da questão e do protocolo de pesquisa, considerou-se como fonte de informação a base Scopus (Elsevier). A escolha pela base Scopus deu-se por ela oferecer a maior cobertura de banco de dados interdisciplinar[5] de resumos e citações de literatura *peer-reviewed* e por possuir mais de 7.000 editores, 26 mil títulos de série ativos, 243 mil livros, 87 milhões de itens, sendo 17,5 milhões de acesso aberto, 17,6 milhões de perfis de autores e 1,8 bilhões de referências citadas desde 1970. Os tipos de conteúdo incluídos na Scopus são publicações seriadas que possuem um *International Standard Serial Number* (ISSN), como periódicos, séries de livros e séries de conferências, ou publicações não seriais que possuem um *International Standard Book Number* (ISBN), como monografias. Além disso, a Scopus oferece

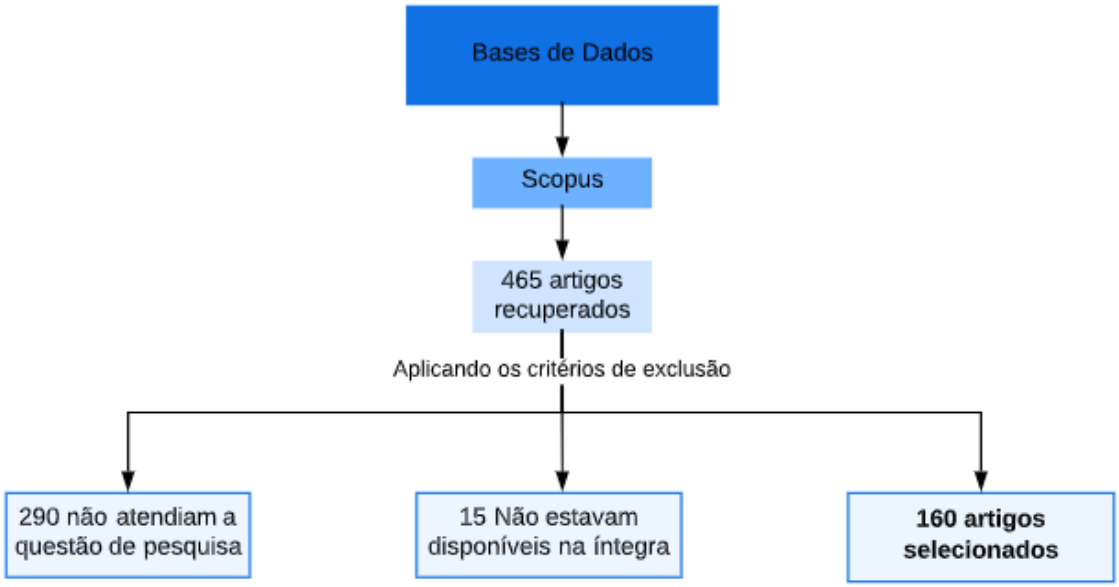
5 Dados disponibilizados no site da Elsevier, disponível em https://www.elsevier.com/pt-br/solutions/scopus . Acesso em 10 de outubro de 2022.

uma visão abrangente da produção científica nas áreas de tecnologia e ciências sociais (SCOPUS, 2017).

A pesquisa foi realizada no período de 2017 a 15 de dezembro de 2021 e para isso foram utilizados os operadores booleanos (delimitadores) representados pelos termos conectores AND e OR. Quatro descritores de busca foram definidos: a) "*information security" and people or*; b) "*information security" and human or*; c) "*information security" and process or;* e d) *"information security" and behavior*. A opção de pesquisa avançada foi utilizada e a busca foi realizada no título, resumo e palavras-chave dos artigos. Todos os descritores foram considerados na língua inglesa, uma vez que a base de dados Scopus utiliza as informações nessa língua para indexar as publicações em sua plataforma.

Nessa RSL, utilizou-se como critério de inclusão artigos que responderam à pergunta de pesquisa, publicados entre 2017-2021 nas áreas de: *computer science, social sciences, business, management and accouting, psychology* e *arts and humanities*. Os critérios de exclusão considerados nesta pesquisa foram: artigos duplicados ou publicados sobre a mesma pesquisa em diferentes periódicos, os que não permitem acesso ao texto completo e os que não atendiam à pergunta de pesquisa, abordando assuntos como: internet das coisas, segurança em *smartphones*, computação em nuvens e comportamento de sistemas. Inicialmente, foram recuperados 465 artigos, conforme demonstrado na Figura 3.

Figura 3- Processo de seleção dos artigos



Fonte: Elaborado pela autora (2022).

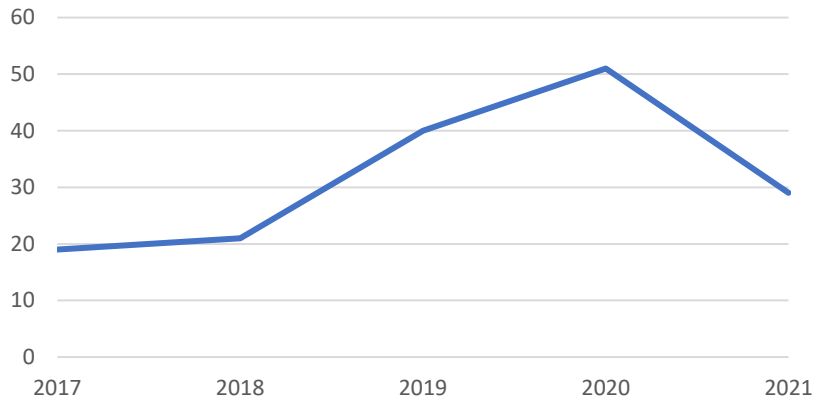
No primeiro momento, foram identificados 22 artigos indisponíveis na íntegra. Entretanto, esse número foi reduzido para 15, a partir de contato com os autores dos referidos artigos e buscas em outras plataformas como *ResearchGate*. A partir da Figura 3, observa-se que foram selecionados 160 artigos que respondem à questão de pesquisa. Os procedimentos seguintes foram: importação dos artigos para o *Mendeley* – programa de gestão de referências bibliográficas; em seguida, para o NVivo 12 Plus, software para análise qualitativa dos dados, cujos artigos primários foram lidos na íntegra e seu conteúdo categorizado; criação de uma planilha no Microsoft Office Excel preenchida com as seguintes variáveis: título do artigo, autores, ano, periódicos, resumo, palavras-chave, objetivo, teoria de suporte, país onde a pesquisa foi realizada, instituição, público ao qual a pesquisa foi aplicada, tipo de estudo (teórico ou empírico), abordagem (quantitativa, qualitativa ou quali-quantitativa), instrumento de coleta, variáveis mensuradas e temáticas.

Após o preenchimento da planilha, foi realizada uma análise bibliométrica das seguintes variáveis: ano, tipo de estudo, abordagem, instrumento de coleta, país, instituição, público, teoria de suporte, autores, periódicos e palavras-chave. A variável 'objetivo' foi trabalhada com auxílio do software *Iramuteq*, que possibilitou uma análise lexicométrica dos objetivos dos artigos. Na próxima subseção apresentaremos a análise bibliométrica dos artigos que compõem a RSL.

2.2 ANÁLISE BIBLIOMÉTRICA DOS ARTIGOS IDENTIFICADOS NA RSL

Em relação ao ano de publicação dos 160 artigos recuperados nessa RSL, conforme o Gráfico 1, percebeu-se um crescimento contínuo e expressivo dos artigos que abordaram a temática de comportamento humano em segurança da informação, no período de 2017-2021, com seu pico de publicação em 2020. Entretanto, em 2021 houve um declínio dessas publicações, o que pode ser justificado por duas possíveis motivações: a primeira diz respeito a limitação temporal da pesquisa, até 15 de dezembro de 2021, e por muitas periódicos permanecerem publicando suas edições do ano anterior no início do ano subsequente; a segunda motivação pode estar relacionada à pandemia da Covid-19 que inviabilizou muitas pesquisas empíricas, seja por questões emocionais, burocráticas ou pela dificuldade de acesso aos sujeitos a serem pesquisados. Isso justifica o ano de 2021 apresentar, proporcionalmente, o maior número de pesquisas teóricas, no período de 2017-2021.

Gráfico 1 - Ano de publicação dos artigos identificados na RSL



Fonte: Elaborado pela autora (2023).

Os resultados das variáveis ‘tipo de pesquisa’, ‘abordagem da pesquisa’ e ‘instrumento de coleta’ estão apresentados no Quadro 3, onde podemos verificar uma predominância por pesquisas empíricas, em detrimento da teórica, o que demonstra uma preferência dos autores por pesquisas baseadas em experiências e análise de fatos, com abordagens quantitativas e, por consequência, pelo uso do questionário *on-line* como principal instrumento de coleta de dados. Observa-se que foi indicada uma frequência de instrumentos de coleta superior a 140 (número de pesquisas empíricas), fato que se justifica por alguns autores utilizarem mais de um instrumento de coleta de dados em suas pesquisas. Destaca-se ainda, que a opção dos pesquisadores pelo questionário impresso decorreu-se da intenção de complementar a aplicação de questionário *on-line.*

Quadro 3 – Metodologia de pesquisa identificada nos artigos

Tipo de pesquisa	Ocorrência	Abordagem	Ocorrência	Instrumentos coleta	Ocorrência
Empírica	140	Quantitativa	115	Questionário on-line	120
Teórica	20	Qualitativa	16	Entrevista	22
		Mista	9	Experimento	6
				Cenários	5
				Grupo focal	4
				Pesquisa documental	3
				Observação	3
				Questionário impresso	3

Fonte: Elaborado pela autora (2023).

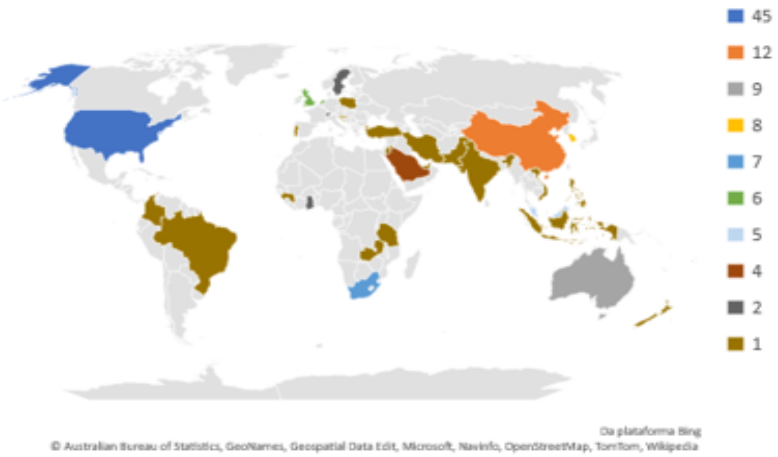
Dentre as 140 pesquisas empíricas recuperadas, 124 indicaram o(s) país(es) onde essas pesquisas foram aplicadas, Figura 4. No entanto, elas ficaram restritas a apenas 36 países, com maior destaque aos Estados Unidos, seguido timidamente pela China, Austrália, Coréia, África do Sul, Holanda e Reino Unido. Ressalta-se que nove pesquisas foram realizadas em mais de um país (CHOI; MARTINS; BERNIK, 2018; CONNOLLY *et al*., 2017; CONNOLLY; LANG; WALL, 2019; JANSEN; VAN SCHAIK, 2017; KARJALAINEN; SIPONEN; SARKER, 2020; KI-ARIES; FAILY, 2017; MENARD; WARKENTIN; LOWRY, 2018; VAN SCHAIK *et al*., 2017; ZWILLING *et al*., 2020).

Foram identificados ainda, 23 países que tiveram apenas uma fração de sua população estudada, como é o caso do Brasil, onde Santos e Silva (2021) aplicaram sua pesquisa em servidores de uma instituição pública com o objetivo de identificar os principais fatores que levam o sujeito a assumir comportamentos que colocam em risco a segurança da informação da instituição ao desempenhar suas atividades cotidianas de trabalho.

Uma quantidade de 14 pesquisas, o que corresponde a 10% das pesquisas empíricas, não declararam os países onde foram aplicadas, inclusive duas delas foram realizadas no continente Europeu, sem a nomeação do referido país. Algumas justificativas possíveis para autores não especificarem o(s) país(es) onde aplicaram suas pesquisas podem ser decorrentes de algumas delas terem sido realizadas em empresas multinacionais com filiais em vários países e, nesses casos, os autores não especificam o país onde a pesquisa foi aplicada. Outra justificativa seria a utilização de painéis de pesquisa pagos como ferramenta para atingir o maior número de respondentes de determinado perfil, independentemente desses respondentes pertencerem a outros países. Nesses estudos, o mais importante é uma amostra robusta e válida.

Figura 4 - Países onde as pesquisas foram realizadas e Mapa coroplético

Países	Freq.
Estados Unidos	45
China	12
Austrália	9
Coréia	8
África do Sul	7
Holanda	6
Reino Unido	6
Malásia	5
Arábia Saudita	4
Gana	2
Iranda	2
Israel	2
Suécia	2
Suiça	2
Alemanha, Brasil, Brunei Darussalam, Colômbia, Croácia, Dubai, Emirados Árabes Unidos, Eslovênia, Filipinas, Guiné, Índia, Indonésia, Irã, Jordânia Nova Zelândia, Paquistão, Polônia, Portugal, Tanzânia, Turquia, Vietnã e Zâmbia	1



Fonte: Elaborado pela autora (2023).

Referente ao tipo de instituição onde as pesquisas foram realizadas, houve uma tendência dos autores em generalizar essa informação, 40 pesquisas, referindo-se, muitas vezes, apenas como uma organização/empresa estudada ou simplesmente ocultando qualquer tipo de informação relacionada ao objeto de pesquisa, 25 pesquisas, conforme Quadro 4. A opção dos autores por omitir detalhes do local da pesquisa pode se dar por exigência da instituição pesquisada, uma vez que o resultado das pesquisas em segurança da informação pode evidenciar vulnerabilidades que se forem publicizadas, implicaria em prejuízos para instituição.

Quadro 4 - Instituição e público pesquisado identificado nos artigos da RSL

Tipo de instituição pesquisada	Ocorrência	Público	Ocorrência
Organização/Empresas	40	Funcionários	35
		Especialistas de SI	3
		Funcionários de TI	2
		Gerentes de SI	1
Universidades	31	Discentes	18
		Funcionários	13

Tipo de instituição pesquisada	Ocorrência	Público	Ocorrência
		Docentes	6
Não identificada	25	Funcionários	10
		Internautas	5
		População	4
		Usuário de PC	3
		Gerentes de ISA	1
		Estudantes	1
		Contadores	1
Bancos	8	Funcionários	7
		Gerentes de SI	1
		Usuários	1
		Gerentes de ISA	1
Indústria	7	Funcionários	6
		Especialistas em SI	1
Telecomunicação	5	Funcionários	5
Multinacional	4	Funcionários	3
Comércio eletrônico	3	Funcionários	3
Departamento de Defesa	3	Funcionários	3
Governo	3	Funcionários	3
		Especialista ISA	1
Hospitais	3	Enfermeiros	2
		Médicos	1
		Equipes de apoio	1
		Funcionários	1
Empresa de Seguro	4	Funcionários	3
		Especialista ISA	1
Empresa de Energia, Empreiteira de interiores, Hoteleiras, Educação, Pequenas e Médias Empresas.	2	Funcionários	8
		CEOs	1
Bibliotecas, Centro de Análise e Compartilhamento de Informações (ISAC), Consultoria de TI, Empresa de desenvolvimento de software, Empresa pública, Escolas secundárias, Imobiliárias, Instituição Pública Federal, Instituição de ensino, Ministérios, Empresa de pesquisa de marketing, Financeira, Empresas de Mídia, Saúde pública, Serviços sociais, Exército.	1	Funcionários	9
		Estudantes	2
		Gerentes	1
		Direção	1
		Servidores	1
		Bibliotecários	1
		Legisladores	1
		Especialista em SI	1

Fonte: Elaborado pela autora (2023).

A partir do Quadro 4, observa-se ainda que houve significativa representatividade das universidades como objetos de pesquisa, tendo no público discente a maior concentração delas. Desse modo, das 31 pesquisas que objetivaram estudar o comportamento humano em segurança da informação nas universidades, 15 foram aplicadas em universidades dos Estados Unidos. As demais pesquisas foram distribuídas entre a Austrália, África do Sul, Índia, Malásia, Dubai, Gana, Paquistão, Israel, Reino Unido, China, Suécia, Eslovênia, Polônia e Turquia.

Essa informação nos possibilita inferir que as universidades americanas são as mais estudadas no mundo em relação ao comportamento em segurança da informação e, consequentemente, remete-nos à ideia de que esse tipo de instituição quando localizada em outros países possuem poucos ou nenhum estudo que busque compreender esse comportamento, como é o caso das universidades localizadas na América do Sul e América Central, onde não foi identificado nenhuma pesquisa direcionada a essas instituições. Esse resultado é semelhante ao já apresentado na pesquisa de Yupanqui e Oré (2017) em que os autores não identificaram, durante sua RSL, nenhuma pesquisa desenvolvida nesses dois continentes.

Apesar de as pesquisas em segurança da informação nas universidades ainda se apresentarem incipientes, com exceção das universidades americanas, entender o comportamento das pessoas é essencial para uma gestão eficiente. Há a necessidade de a segurança da informação ser gerenciada em todos os tipos de instituição, inclusive as instituições públicas, uma vez que, almejam permanecer no mercado a que se propuseram. Elas também oferecem retorno aos seus *stakeholders*, mas de uma forma diferente: retribuição social aos cidadãos, serviços prestados à população, melhoria de vida e ações que fortalecem a cidadania (ABNT NBR ISO/IEC 27002, 2013a; FONTES, 2016).

Os bancos e as indústrias também apresentam destaques nas pesquisas sobre segurança da informação, conforme Quadro 2. Essa tendência pode ser explicada pelo retorno financeiro que essas instituições proporcionam aos seus investidores e aos prejuízos decorrentes de um possível incidente de segurança.

A análise dos 160 estudos permitiu identificar 37 teorias que os autores dos artigos utilizaram para explicar, compreender e/ou propor modelos que explicam o comportamento humano em segurança da informação, conforme Quadro 5. As teorias são aplicadas de forma isolada, associadas a outras teorias ou expandindo a teoria original. De cordo com o Quadro 5 as teorias mais frequentemente aplicadas são nomeadamente a teoria da motivação de proteção, a teoria do comportamento planejado, teoria da dissuasão e teoria da escolha racional. Outras teorias foram testadas apenas ocasionalmente, sendo identificadas em apenas um ou dois

artigos. Do mesmo modo, esse resultado corrobora as ideias de Sommestad (2018) e a pesquisa desenvolvida por Yupanqui e Oré (2017) que realizaram uma RSL das publicações dos anos de 2000 a 2017 e identificaram as mesmas teorias como as mais recorrentes.

Quadro 5 - Teorias de suporte utilizada nas pesquisas identificadas na RSL

Teorias de suporte identificadas nos artigos	Ocorrência
Teoria da Motivação de Proteção	35
Teoria do Comportamento Planejado	27
Teoria da Dissuasão	22
Teoria da Escolha Racional	8
Teoria da Ação Racional e Teoria da Autodeterminação	5
Teoria Cognitiva Social e Teoria do Vínculo Social	4
Teoria de Prevenção de Ameaças de Tecnologia e Teoria do Nível de Construção	2
Teoria do Estágio, Teoria do Equilíbrio de Controle, Teoria Analítica Fundamentada, Teoria Clássica de Gestão Organizacional, Teoria da Agência, Teoria da Aprendizagem Social, Teoria da Atividade, Teoria da Autorregulação, Teoria da Difusão da Inovação, Teoria da Identidade Social, Teoria da Influência Normativa, Teoria da Neutralização, Teoria da Prestação de Contas, Teoria da Prevenção do Crime Situacional, Teoria de Domínios, Teoria do Apelo ao Medo, Teoria do Aprendizado Organizacional, Teoria do Desenvolvimento Cognitivo Moral, Teoria do Envolvimento, Teoria do Laço Social, Teoria do Rebanho, Teoria do Relacionamento Interpessoal, Teoria dos Eventos Efetivos, Teoria dos Jogos, Teoria Organizacional, Teoria Social Cognitiva e Teoria de Ampliação e Construção.	1

Fonte: Elaborado pela autora (2023).

Apesar dessa diversidade teórica, há pontos em comum entre essas teorias. Primeiramente elas estão focadas em estudar, compreender e prever o comportamento humano (SOMMESTAD, 2018). O segundo ponto está relacionado à ligação teorizada, que aparece em muitos estudos, entre as intenções comportamentais e os comportamentos reais relacionados à segurança (ALI; DOMINIC; ALI, 2020; ALZAHRANI, 2021; CHEN; CHEN; WU, 2018; RAJAB; EYDGAHI, 2019; SAFA *et al*., 2018a). Isso significa que os funcionários, em média, agirão de acordo com suas intenções de cumprir ou não as políticas de segurança da informação das instituições (AJZEN, 2011). A compreensão do comportamento humano por meio de teorias psicológicas, que vão além da perspectiva meramente tecnológica, justifica-se pelo comportamento humano ser considerado o elo mais fraco da segurança da informação (CONNOLLY *et al*., 2017; DANG-PHAM; PITTAYACHAWAN; BRUNO, 2017a; JANSEN;

VAN SCHAIK, 2018a; PARSONS *et al*., 2017; SAMPAIO; MANCINI, 2007; SNYMAN; KRUGER, 2017a; SOHRABI SAFA; VON SOLMS; FURNELL, 2016).

Descrever todas as teorias escaparia ao objetivo deste trabalho e, nesse sentido, apenas as três mais frequentes serão abordadas.

A TMP foi desenvolvida por Rogers (1975) e ampliada para o domínio da pesquisa em saúde e segurança pública pelo mesmo autor em 1983. Essa teoria envolve dois processos cognitivos avaliação de ameaça e avaliação de enfretamento (MENARD; WARKENTIN; LOWRY, 2018).

Essa teoria tem ganhado cada vez mais atenção na pesquisa em segurança da informação (HAAG; SIPONEN; LIU, 2021; JANSEN; VAN SCHAIK, 2018a; LI *et al.*, 2019; ORAZI; JOHNSTON; WARKENTIN, 2019). Isso ocorre porque a motivação representa as razões para as ações, necessidades e desejos das pessoas. A motivação define a direção e as razões de um padrão comportamental específico. Um motivo leva a pessoa a se comportar de uma maneira específica (SAFA; VON SOLMS, 2016b). A partir do resultado desta RSL, foram identificados 35 artigos que utilizaram a TMP, seja isoladamente ou associada a outras teorias (AIGBEFO; BLOUNT; MARRONE, 2020; ALANAZI *et al*., 2020; AURIGEMMA; MATTSON, 2019; BARLETTE; JAOUEN, 2019; BAX; MCGILL; HOBBS, 2021; BURNS; POSEY; ROBERTS, 2021; CHEN; CHEN; WU, 2018; CROSSLER; BÉLANGER; ORMOND, 2019; DEBB; MCCLELLAN, 2021; GRIMES; MARQUARDSON, 2019; HAAG; SIPONEN; LIU, 2021; HINA; SELVAM; LOWRY, 2019; HOOPER; BLUNT, 2020; JAEGER; ECKHARDT, 2020; JANSEN; VAN SCHAIK, 2017, 2018b, 2019; KHAN; ALSHARE, 2019; KOOHANG *et al*., 2020; LANKTON; STIVASON; GURUNG, 2019; LEMAY; BASNET; DOLECK, 2020; LI *et al*., 2019; MAMONOV; BENBUNAN-FICH, 2018; MCGILL; THOMPSON, 2021; MENARD; BOTT; CROSSLER, 2017; MENARD; WARKENTIN; LOWRY, 2018; ORAZI; JOHNSTON; WARKENTIN, 2019; PARK; CHAI, 2020; QAZI; RAZA; KHAN, 2020; RAJAB; EYDGAHI, 2019; SCHUETZ *et al*., 2020; VAN SLYKE; BELANGER, 2020; VEDADI; WARKENTIN; DENNIS, 2021; WIAFE *et al*., 2020; ZHEN; XIE; DONG, 2020a).

A Teoria do Comportamento Planejado também tem sido amplamente utilizada no domínio da segurança da informação, conforme Quadro 5. Desenvolvida a partir da Teoria da Ação Racional, descreve as mudanças no comportamento humano com base na perspectiva da influência social. Essa teoria postula três construtos: atitude, norma subjetiva e controle comportamental percebido. Atitude é definida como os sentimentos positivos ou negativos do indivíduo em relação à participação em um comportamento específico. As normas subjetivas descrevem a percepção de um indivíduo sobre o que as pessoas importantes pensam sobre

determinado comportamento, já o controle comportamental percebido é definido como as crenças do indivíduo em relação à eficácia e aos recursos necessários para facilitar um comportamento (YUPANQUI; ORÉ, 2017). Este estudo identificou 27 artigos que abordam essa teoria isoladamente ou associada a outras (AIGBEFO; BLOUNT; MARRONE, 2020; AJZEN, 2011; ALANAZI *et al.*, 2020; ALEROUD *et al.*, 2020; AURIGEMMA; MATTSON, 2017a, 2019; BÉLANGER *et al.*, 2017; CANO; ALMANZA, 2020; CHEN *et al.*, 2020b; CHINYEMBA; PHIRI, 2018; D'ARCY; LOWRY, 2019; GRIMES; MARQUARDSON, 2019; HINA; SELVAM; LOWRY, 2019; HONG; FURNELL, 2019; KHAN; ALSHARE, 2019; KIM; KIM, 2017; KOOHANG *et al.*, 2020; LEERING; VAN DE WIJNGAERT; NIKOU, 2020; MAKERI, 2020; MERHI; AHLUWALIA, 2019; RAJAB; EYDGAHI, 2019; SAFA *et al.*, 2018a, 2019; SNYMAN; KRUGER; KEARNEY, 2018; SOLOMON; BROWN, 2020; VAN SLYKE; BELANGER, 2020; ZWILLING *et al.*, 2020).

A última teoria de significativa recorrência é a Teoria da Dissuasão. Cannolly *et al.* (2017) esclarecem que essa teoria depende de três componentes individuais: gravidade, certeza e celeridade das sanções. Baseia-se na proposição central de que o comportamento ilícito pode ser controlado pela ameaça de sanções. A teoria da dissuasão, tal como a teoria da motivação de proteção e a teoria do comportamento planejado, foi estudada tanto isoladamente como associada a outras teorias, conforme os 22 artigos recuperados na RSL (ALANAZI *et al.*, 2020; ALSHARE; LANE; LANE, 2018; AURIGEMMA; MATTSON, 2017b, 2019; BERNDTSSON; JOHANSSON; KARLSSON, 2018; CHEN *et al.*, 2020b; CHEN; CHEN; WU, 2018; CHOI, 2019; CONNOLLY *et al.*, 2017; GUAN; HSU, 2020; HAMID; YUSOF; DALI, 2019; HOOPER; BLUNT, 2020; KHAN; ALSHARE, 2019; KIM; LEE; KIM, 2020; KOOHANG *et al.*, 2020; LANKTON; STIVASON; GURUNG, 2019; MERHI; AHLUWALIA, 2019; RAJAB; EYDGAHI, 2019; SAFA *et al.*, 2019; SARKAR *et al.*, 2020; VAN SLYKE; BELANGER, 2020; WIAFE *et al.*, 2020).

No que concerne às autorias, verificou-se que, para a temática 'comportamento humano em segurança da informação', as pesquisas colaborativas são mais frequentes do que as de autoria isolada. Dos 160 artigos recuperados, 147 (91,9%) dos pesquisadores desenvolveram sua pesquisa com pelo menos um co-autor e apenas 13 (8,1%) dos autores publicaram de forma isolada (ALSHAIKH, 2020; ALZAHRANI, 2021; CHOI, 2019; CHULKOV, 2017; HADLINGTON, 2018; LETICA, 2019; MAKERI, 2020; MUTCHLER, 2019; NOOR, 2020; OGBANUFE, 2021; SOMMESTAD, 2018; STEFANIUK, 2020; VEIGA, 2018). Diante disso, percebe-se uma preferência significativa dos autores por pesquisas colaborativas, o que pode

ser reflexo da interdisciplinaridade da temática e pela predominância de pesquisas empíricas que demandam, em sua maioria, mais esforço prático dos pesquisadores.

A partir dos artigos recuperados na RSL, identificamos os dez mais citados, Quadro 6, (BAUER; BERNROIDER; CHUDZIKOWSKI, 2017; BRUIJN; JANSSEN, 2017; D'ARCY; LOWRY, 2019; LI *et al.*, 2019; MAMONOV; BENBUNAN-FICH, 2018; MCCORMAC *et al.*, 2017a; MENARD; BOTT; CROSSLER, 2017; MENARD; WARKENTIN; LOWRY, 2018; PARSONS *et al.*, 2017; VAN SCHAIK *et al.*, 2017). Os dois primeiros artigos são dos mesmos autores: Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. e Zwaans, T., assim como Menard, P. e Lowry, P. B. também se repetem como autores em dois artigos.

Quadro 6 - Artigos mais citados da RSL

Título dos artigos	Citações	Referências	Ano
Individual differences and Information Security Awareness	132	McCormac A., Zwaans T., Parsons K., Calic D., Butavicius M., Pattinson M.	2017
The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies	120	Parsons, K.; Calic, D.; Pattinson, M.; Butavicius, M.; McCormac, A.; Zwaans, T.	2017
User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory	107	Menard, P.; Bott, G. J.; Crossler, R. E.	2017
Building Cybersecurity Awareness: The need for evidence-based framing strategies	93	Bruijn, H.; Janssen, M.	2017
Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior	88	Li, L.; He, W.; Xu, L.; Ash, I.; Anwar, M.; Yuan, X.	2019
Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study	77	D'Arcy, J.; Lowry, P. B.	2019
Risk perceptions of cyber-security and precautionary behaviour	66	van Schaik, P.; Jeske, D.; Onibokun, J.; Coventry, L.; Jansen, J.; Kusev, P.	2017
The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination	58	Menard, P.; Warkentin, M.; Lowry, P. B.	2018

Título dos artigos	Citações	Referências	Ano
Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks	57	Bauer, S.; Bernroider, E. W. N.; Chudzikowski, K.	2017
The impact of information security threat awareness on privacy-protective behaviors	55	Mamonov, S.; Benbunan-Fich, R.	2018

Fonte: Elaborado pela autora (2023).

O Quadro 7 apresenta os periódicos que obtiveram uma frequência mínima de três artigos publicados, onde a *Information and Computer Security*, da *Emerald*, periódico diretamente relacionado à teoria e prática do gerenciamento em segurança dos sistemas de informação apresentou maior número de publicações, seguido da *Computers and Security*, da *Elsevier*, periódico técnico na área de segurança em tecnologia da informação. Conforme exposto, ambos possuem, como essência, o foco em segurança da informação na dimensão tecnológica. O periódico brasileiro identificado, a Revista Digital de Biblioteconomia e Ciência da Informação, da UNICAMP, teve um artigo publicado.

Quadro 7 – Periódicos com maior frequência de publicação

Periódicos	Frequência
Information and Computer Security	27
Computers and Security	26
Information Technology and People	6
Journal of Computer Information Systems	6
Behaviour and Information Technology	5
Computers in Human Behavior	5
Information Systems Journal	4
Information and Management	3
Information Systems Frontiers	3
Journal of Enterprise Information Management	3
Journal of Information Security and Applications	3
Journal of the Association for Information Systems	3

Fonte: Elaborado pela autora (2023).

A subseção seguinte, apresentará a análise lexicométrica para uma melhor compreensão dos objetivos dos artigos que compõem essa RSL.

2.3 ANÁLISE LEXICOMÉTRICA DO OBJETIVO DOS ARTIGOS

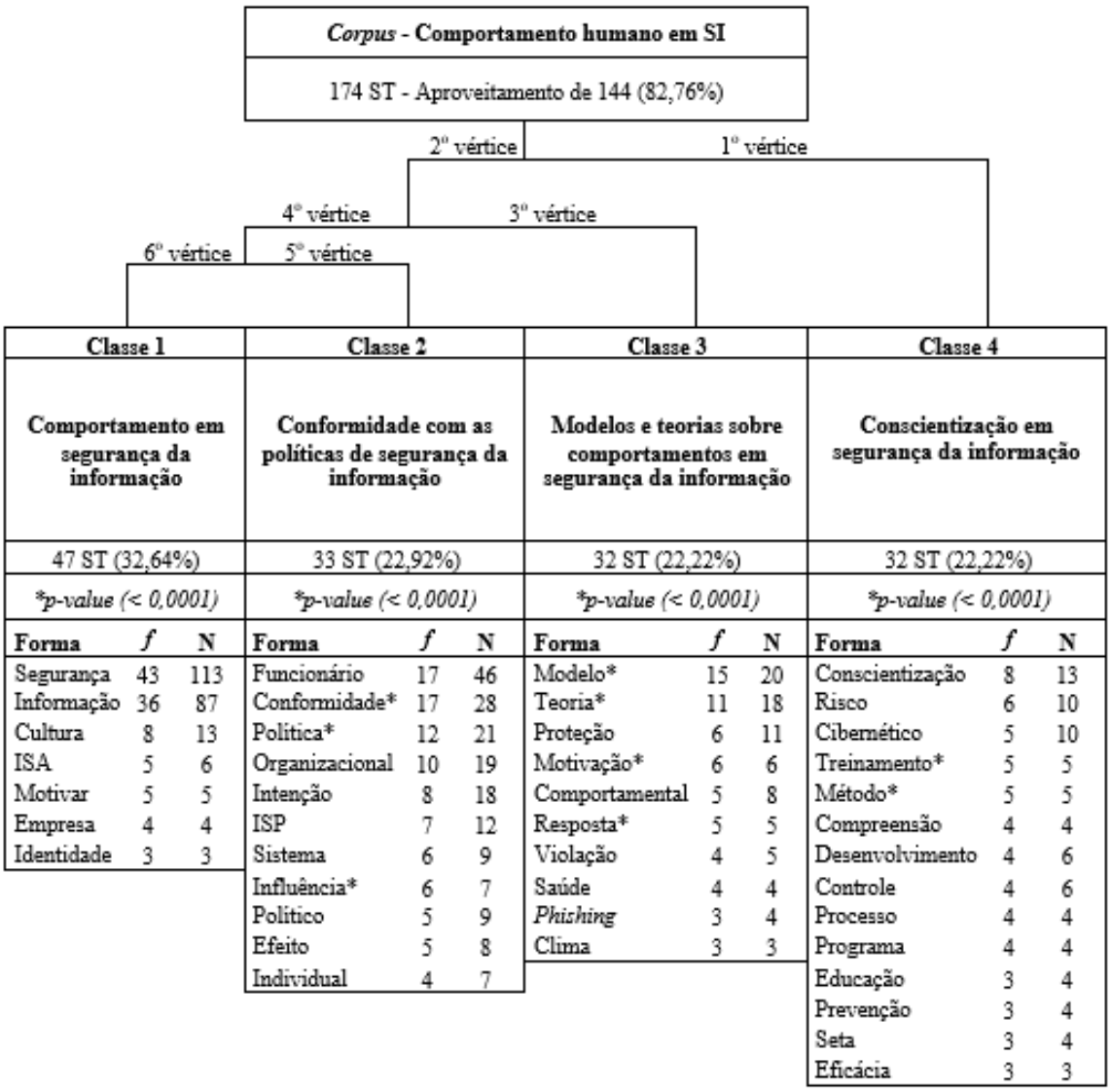
A análise lexicométrica foi realizada com o auxílio do *Iramuteq*, software gratuito que auxilia o tratamento de dados textuais por meio de diferentes possibilidades de análise baseadas na estatística de texto ou lexicometria, tais como: Estatísticas Textuais Clássicas, Análise de Especificidades, Análise de Similitude (AS), Análise Fatorial por Correspondência, Classificação Hierárquica Descendente (CHD) (método Reinert), Nuvem de Palavras e Análise Prototípica de evocações livres (SOUSA, 2021). Nesta pesquisa utilizamos a Classificação Hierárquica Descendente e Análise de Similitude.

O estudo de Marchand e Ratinaud (2012) foi o alicerce para a análise léxica dos objetivos dos 160 artigos utilizados na amostra para a formação do *corpus* gerando 4.395 ocorrências, palavras dentro do *corpus*, das quais apresentaram 998 palavras distintas, sendo 806 formas lematizadas (palavras distintas com mais de uma ocorrência) e 450 *hapax* (palavras com apenas uma ocorrência no *corpus*). Foram identificados 174 segmentos de textos, 711 formas de palavras ativas, 90 formas suplementares, representando uma retenção de 82,76% na Classificação Hierárquica Descendente pelo método de Reinert, o que é adequado para a análise a ser realizada por Reinert (1990), pré-selecionando 132 dos 160 estudos da amostra. Os demais 28 estudos não selecionados para a formação das classes foram eliminados das análises sem prejuízo para o entendimento da revisão de literatura analisada, uma vez que as temáticas abordadas por esses artigos, a saber: apelo ao medo, comportamento em segurança da informação, conscientização em segurança da informação, cultura de segurança cibernética, *phishing* e treinamento em segurança da informação são temáticas já contempladas nos 132 artigos que compõem essa análise.

Posteriormente ao processamento da Classificação Hierárquica Descendente pelo método de *Reinert*, foi elaborado o dendrograma das classes, Figura 5, que obteve quatro classes distintas, onde o primeiro vértice foi responsável pela criação da Classe 4, com 32 segmentos de textos dos 144 segmentos contidos na CHD, sendo responsável por 22,22% dos segmentos de todas as classes. O segundo vértice foi subdividido gerando o terceiro e quarto vértices. O terceiro vértice foi responsável pela geração da Classe 3, também com 32 segmentos de texto, representando 22,22% dos segmentos totais. O quarto vértice foi subdividido, dando origem às Classes 1 e 2. A Classe 2, representa 33 segmentos de textos, sendo 22,92% dos segmentos totais e a Classe 1, maior classe evidenciada, com 47 dos 144 segmentos da CHD, sendo responsável por 32,64% dos segmentos totais.

Conforme ilustrado na Figura 5, o símbolo (f) representa a frequência individual de cada termo ao longo de uma única classe, e o símbolo (N) a frequência global de cada termo dentro do *corpus*. Os dados estão apresentados na ordem decrescente das formas ativas de cada classe. Com este resultado, foi possível eliminar aproximadamente 17% de termos considerados não relevantes para essa análise. Salienta-se que a seleção apenas das formas ativas deu-se pelo fato de serem mais fidedignas na composição das palavras que compõem os temas centrais dos objetivos dos estudos.

Figura 5 - Dendrograma das classes



Classe 1			Classe 2			Classe 3			Classe 4		
Comportamento em segurança da informação			**Conformidade com as políticas de segurança da informação**			**Modelos e teorias sobre comportamentos em segurança da informação**			**Conscientização em segurança da informação**		
47 ST (32,64%)			33 ST (22,92%)			32 ST (22,22%)			32 ST (22,22%)		
**p-value (< 0,0001)*			**p-value (< 0,0001)*			**p-value (< 0,0001)*			**p-value (< 0,0001)*		
Forma	***f***	**N**	**Forma**	***f***	**N**	**Forma**	***f***	**N**	**Forma**	***f***	**N**
Segurança	43	113	Funcionário	17	46	Modelo*	15	20	Conscientização	8	13
Informação	36	87	Conformidade*	17	28	Teoria*	11	18	Risco	6	10
Cultura	8	13	Politica*	12	21	Proteção	6	11	Cibernético	5	10
ISA	5	6	Organizacional	10	19	Motivação*	6	6	Treinamento*	5	5
Motivar	5	5	Intenção	8	18	Comportamental	5	8	Método*	5	5
Empresa	4	4	ISP	7	12	Resposta*	5	5	Compreensão	4	4
Identidade	3	3	Sistema	6	9	Violação	4	5	Desenvolvimento	4	6
			Influência*	6	7	Saúde	4	4	Controle	4	6
			Politico	5	9	*Phishing*	3	4	Processo	4	4
			Efeito	5	8	Clima	3	3	Programa	4	4
			Individual	4	7				Educação	3	4
									Prevenção	3	4
									Seta	3	4
									Eficácia	3	3

Fonte: Elaboração própria (2023).

As classes identificadas no dendrograma propõem campos semânticos que irão nortear a organização e análise dos estudos da amostra. Esse procedimento nos ajuda a compreender como a temática "comportamento humano em segurança da informação" vem sendo estudada

a partir dos objetivos dos artigos que compõem o *corpus* da pesquisa. Essa metodologia foi alicerçada no estudo de Porte, Saur-Amaral e Pinho (2018) que pesquisaram os temas publicados em auditoria a partir dos objetivos dos artigos. Do mesmo modo, quanto à geração de classes, foi referência a pesquisa de Porte e Trindade (2019) sobre barreiras tecnológicas.

Nas próximas subseções será apresentada a literatura existente sobre o comportamento humano em segurança da informação por meio da análise de similitude e de estatísticas textuais. De acordo com Marchand e Ratinaud (2012), a análise de similitude utiliza a coocorrência e relações de formas lexicais em textos ou segmentos de texto para construir representações gráficas sobre a estrutura do conteúdo de um *corpus*. Os resultados são apresentados na forma de grafos, onde as palavras constituem os vértices e as arestas representam a relação entre eles. Ressalta-se que as apresentações das subseções seguiram a ordem do primeiro ao último vértice gerados a partir do dendrograma, Figura 5.

2.3.1 Classe 4 – Conscientização em segurança da informação

A Classe 4 ‘Conscientização em segurança da informação’ obteve a representatividade de 22,22% do *corpus,* apresentando os termos ‘conscientização’, ‘risco’, ‘cibernético’, ‘treinamento’ e ‘método’ como os mais significativos entre os 32 segmentos de textos da classe, conforme o dendrograma apresentado na Figura 5.

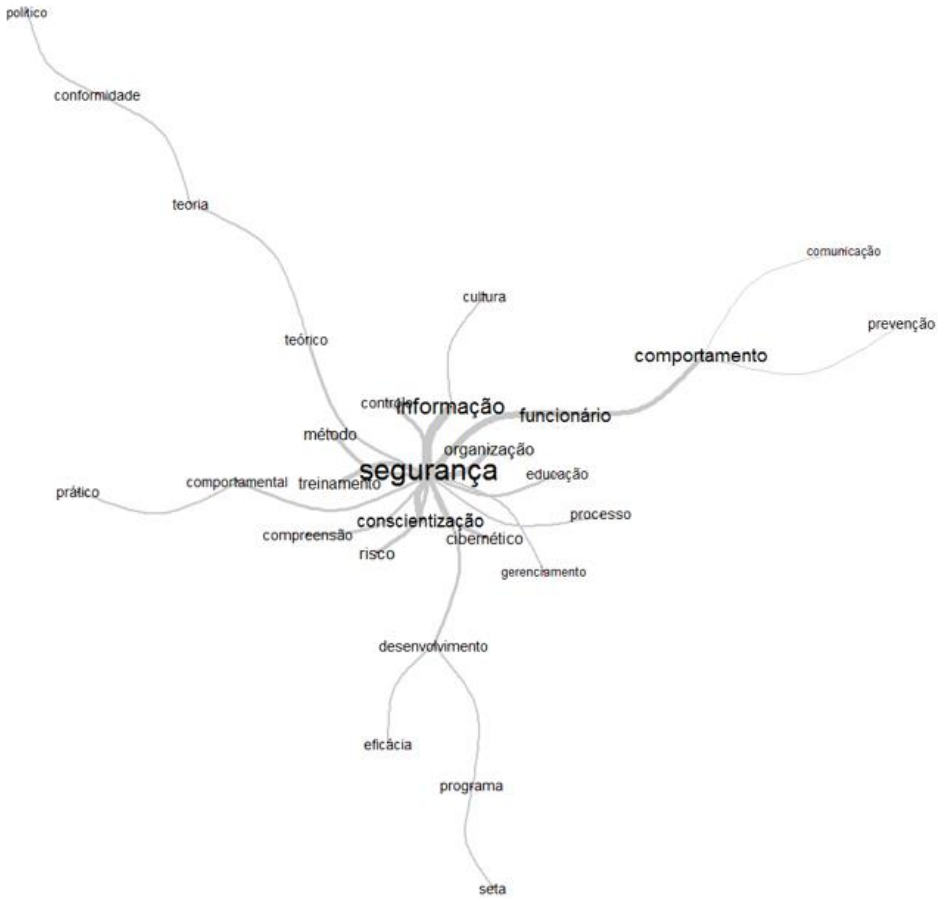
Percebe-se que o resultado da análise de similitude, Figura 6, fornece um destaque para 28 palavras, sendo 14 anteriormente destacadas no dendrograma das classes, Figura 5, com a inserção dos termos ‘segurança’, ‘teoria’, ‘teórico’, ‘conformidade’, ‘político’, ‘cultura’, ‘informação’, ‘organização’, ‘funcionário’, ‘comportamento’, ‘comunicação’, ‘comportamental’, ‘prático’ e ‘gerenciamento’. A partir da análise de similitude, é possível identificar uma forte relação do termo ‘segurança’ com os termos ‘informação’, ‘conscientização’ e ‘funcionário’, o que justifica a denominação da referida classe. Os termos presentes na análise de similitude, Figura 6 possuíram uma frequência mínima de três aparições nos objetivos dos 22 artigos que compõem a Classe 4.

Os resultados indicaram nove estudos direcionados às temáticas que envolvem os programas de Educação, Treinamento e Conscientização em Segurança (SETA[6]) (ALMINDEEL; MARTINS, 2020; ALSHAIKH; MAYNARD; AHMAD, 2021; BARLOW *et al.*, 2018; BAUER; BERNROIDER; CHUDZIKOWSKI, 2017; HAMID; YUSOF; DALI,

6 SETA, sigla muito utilizada em segurança da informação, tem sua origem na língua inglesa, refere-se a Security Education, Training, and Awareness (SETA).

2019; HE *et al.*, 2019; KI-ARIES; FAILY, 2017; PATTINSON *et al.*, 2019; SNYMAN; KRUGER, 2017b).

Figura 6 - Análise de similitude da Classe 4



Fonte: Elaborado pela autora (2023).

Os Programas SETA podem ser definidos como programas de educação projetados para reduzir as violações de segurança que ocorrem por meio da falta de conscientização em segurança da informação dos funcionários, apresentando-se como uma ferramenta vital para inculcar a consciência de segurança e mitigar possíveis ameaças decorrentes de um comportamento não conforme. Sem programas adequados de SETA, os funcionários, muitas vezes, não conseguem discernir se cometeram ou não uma violação à segurança (ABDALLAH *et al.*, 2020).

As pesquisas de Alshaikh, Maynard e Ahmad (2021) e Barlow *et al.* (2018) abordaram formas de tornar os programas SETA mais eficientes. Nesse sentido, Alshaikh, Maynard e Ahmad (2021) utilizaram abordagens de marketing social para avaliar a eficácia do processo de desenvolvimento de programas SETA existentes em organizações de seguros, bancos, setor automotivo e serviços de tecnologia da informação. O estudo de Barlow *et al.* (2018) investigou

três abordagens de comunicação baseadas em teorias que podem ser incorporadas aos programas SETA para ajudar a aumentar o comportamento de prevenção: comunicação informativa projetada para explicar por que as políticas são importantes; comunicação normativa projetada para explicar que outros funcionários não violariam políticas; e comunicação anti-neutralização projetada para inibir a racionalização. A pesquisa de Hamid, Yusof e Dali (2019), apesar de não abordar a nomenclatura SETA em seu objetivo, analisou a gestão do controle de segurança da informação, incluindo a conscientização da segurança da informação, o treinamento e a educação como fatores de impacto no comportamento de prevenção dos funcionários na organização.

Quatro estudos abordaram a conscientização em segurança da informação (ALMINDEEL; MARTINS, 2021; BAUER; BERNROIDER; CHUDZIKOWSKI, 2017; KI-ARIES; FAILY, 2017; SNYMAN; KRUGER, 2017a). Entretanto, serão apresentados ainda, na presente classe, seis artigos, vinculados à Classe 1, mas que abordam a 'conscientização em segurança da informação' como principal temática (HADLINGTON *et al.*, 2019; HADLINGTON; BINDER; STANULEWICZ, 2020; HWANG *et al.*, 2021; MCCORMAC *et al.*, 2018; PARSONS *et al.*, 2017; WILEY; MCCORMAC; CALIC, 2020). A inserção desses artigos na Classe 1 pode ser em decorrência do uso, por alguns autores, apenas da sigla ISA[7] nos objetivos dos artigos ou pela forte ligação entre conscientização e o comportamento em segurança da informação.

De acordo com Parsons *et al*. (2017), as definições associadas ao conceito de conscientização em segurança da informação possuem dois componentes essenciais: o primeiro está relacionado ao nível de compreensão que o indivíduo possui sobre a política de segurança da informação organizacional, pois muitas vezes as políticas e protocolos de segurança da informação podem não ser muito compreensíveis, o que impossibilita que o funcionário possua um comportamento seguro. O segundo componente analisa até que ponto o indivíduo se compromete com os princípios fundamentais da segurança da informação dentro de sua organização e quanto de seu comportamento atende aos requisitos de melhores práticas. Nessa perspectiva, a pesquisa de Almindeel e Martins (2021) buscou aumentar a compreensão da consciência de segurança da informação dos funcionários em uma agência governamental na Arábia Saudita e evidenciar os problemas que as organizações do setor público enfrentam quando procuram estabelecer um programa de conscientização em segurança da informação. Com o auxílio de um estudo semelhante, Hwang *et al.* (2021) exploraram como experiências

7 *Information Security Awareness* (ISA), ou seja, Conscientização em Segurança da Informação.

e observações típicas relacionadas à segurança da informação no local de trabalho motivam a conscientização acerca da segurança.

Seguindo a linha das pesquisas sobre conscientização em segurança da informação, quatro pesquisas analisaram a relação entre conscientização em segurança da informação e outros fatores como o medo de perder, análise de limiares comportamentais, cultura organizacional, resiliência e estresse no trabalho (HADLINGTON; BINDER; STANULEWICZ, 2020; MCCORMAC *et al.*, 2018; SNYMAN; KRUGER, 2017b; WILEY; MCCORMAC; CALIC, 2020).

Hadlington *et al.* (2019) exploraram se o *locus* de controle do trabalho de um indivíduo poderia prever o nível em que os funcionários se engajam em uma conscientização eficaz. Os autores Ki-Aries e Faily (2017) apresentaram em sua pesquisa uma abordagem para identificar fatores humanos relacionados à segurança, incorporando as pessoas ao projeto de implementação da conscientização em segurança da informação. Parsons *et al* (PARSONS *et al.*, 2017) estabeleceram ainda mais a validade do Questionário de Aspectos Humanos de Segurança da Informação (HAIS-Q) como um instrumento eficaz para medir a conscientização em segurança da informação. Bauer, Bernroider e Chudzikowski (2017) analisaram os esforços dos gerentes de segurança da informação para projetar programas de conscientização em segurança da informação eficazes, comparando as recomendações de projeto atuais sugeridas pela literatura científica com as práticas reais de um projeto de programas de conscientização em três bancos europeus. Snyman e Kruger (2017) realizaram uma investigação exploratória sobre a viabilidade da análise de limiares comportamentais como um possível auxílio em campanhas de conscientização de segurança.

Ainda com relação às temáticas envolvidas nos programas SETA, foram identificados, nesta classe, dois estudos que possuem como principal foco o treinamento em segurança (HE *et al.*, 2019; PATTINSON *et al.*, 2019). Para Van Schaik *et al.* (2017), os programas regulares de treinamento e conscientização são executados para garantir que todos os funcionários saibam como responder às ameaças, entendam os termos básicos de segurança e passem a usar os dispositivos de forma segura.

O estudo de Pattinson *et al* (2019) direcionaram sua pesquisa para apresentar o conceito de uma estrutura de controles de segurança cibernética que são adaptáveis a diferentes tipos de organizações e diferentes tipos de funcionários. Nesse sentido, um desses controles adaptativos, a saber, o modo de treinamento fornecido, foi testado empiricamente quanto à sua eficácia. He *et al.* (2019) investigaram o efeito de diferentes métodos de treinamento de segurança cibernética baseados em evidências na percepção de risco e no comportamento relatado pelos

funcionários.

Os programas SETA impactam na consciência e na capacidade do comportamento seguro dos funcionários (CHEN; CHEN; WU, 2018). A estreita relação entre os programas SETA e o comportamento dos funcionários pode justificar a presença de cinco estudos que abrangem a referida temática, na presente classe (ALZAHRANI; JOHNSON, 2019; DANG-PHAM; PITTAYACHAWAN; BRUNO, 2017a; GANGIRE; VEIGA; HERSELMAN, 2021; SNYMAN; KRUGER, 2021; WALL; PALVIA; D'ARCY, 2021). Entretanto, esses estudos serão apresentados na Classe 1.

Apesar de a presente Classe possuir uma maior tendência em abordar assuntos relacionados aos programas SETA, também fazem parte da Classe 4, dois estudos apresentados como RSL (AL-HARTHY *et al.*, 2020; HWANG; KIM; REBMAN, 2021); dois artigos que possuem a cultura de segurança como principal temática e os quatro artigos restantes apresentam estudos distribuídos em temáticas que envolvem ameaças à segurança da informação, estresse tecnológico e mensagens de apelo ao medo (CHINYEMBA; PHIRI, 2018; HWANG; KIM; REBMAN, 2021; JOHNSTON *et al.*, 2019; SAFA *et al.*, 2019).

2.3.2 Classe 3 – Modelos e teorias sobre comportamento em segurança da informação

A presente Classe, 'Modelos e teorias sobre comportamento em segurança da informação' obteve a representatividade de 22,22% do *corpus,* apresentando os termos 'modelo', 'teoria', 'proteção', 'motivação', 'comportamental' e 'resposta' como os mais significativos entre os 32 segmentos de textos da classe, de acordo com a Figura 5, que apresenta o dendrograma.

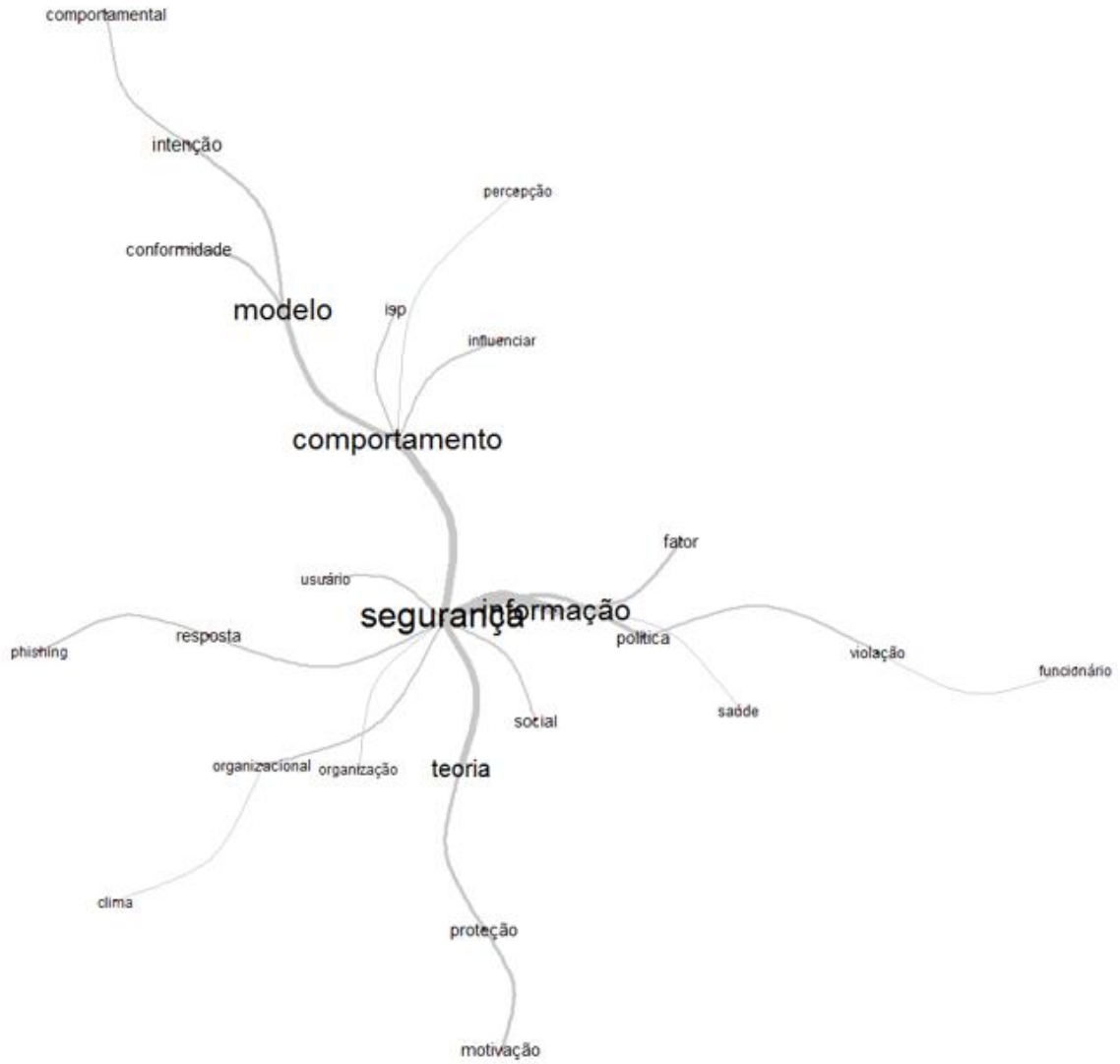
A Figura 7 apresenta a análise de similitude da Classe 3 dos termos que melhor integram a descrição da Classe. Observa-se que a Figura 7, fornece um realce para 25 palavras, sendo que dez foram ilustradas na Classe 3 do dendrograma, Figura 5, com o acréscimo dos termos 'segurança', 'informação', 'comportamento', 'fator', 'funcionário', 'política', 'social', 'organização', 'organizacional' 'usuário', 'ISP'[8], influenciar', 'percepção', 'conformidade' e 'intenção'. Esses termos possuíram uma frequência mínima de três aparições nos objetivos dos 32 artigos que compõem a Classe 3.

Os resultados apontam para 16 estudos que apresentam, desenvolvem, constroem, comparam ou propõem 'modelos', baseados ou não em teorias para melhor compreender o

8 Sigla do termo em língua inglesa, *Information Security Policy (ISP)*, traduzido para Política de Segurança da Informação (PSI).

comportamento humano em segurança da informação (ALANAZI *et al.*, 2020; ALOTAIBI; FURNELL; CLARKE, 2019; ALSHARE; LANE; LANE, 2018; BÉLANGER *et al.*, 2017; CHEN; CHAU; LI, 2019; CHEN *et al.*, 2020b; CHEN; CHEN; WU, 2018; D'ARCY; LOWRY, 2019; DAVIS; AGRAWAL; GUO, 2021; GRIMES; MARQUARDSON, 2019; GWEBU; WANG; HU, 2020; HONG; FURNELL, 2019; JANSEN; VAN SCHAIK, 2017; MENARD; BOTT; CROSSLER, 2017; MERMOUD *et al.*, 2019; YENG *et al.*, 2021).(VAN SLYKE; BELANGER, 2020).

Figura 7 - Análise de similitude da Classe 3



Fonte: Elaborado pela autora (2023).

O estudo de Davis, Agrawal e Guo (2021) apresentou um modelo de pesquisa que destaca os fatores do local de trabalho que impulsionam o compromisso internalizado dos usuários com a segurança da informação organizacional. Chen *et al.* (2020) constroem um

modelo com base nas teorias sobre escolha racional e dissuasão geral, e o aplica para explicar os efeitos da sanção de violação da política de segurança da informação por funcionários. No mesmo ano, Gwebu, Wang e Hu (2020) desenvolveram um modelo integrativo que investiga como o clima de trabalho ético, as crenças e a neutralização interagem para explicar conjuntamente o descumprimento da política de segurança da informação.

No ano anterior, Chen, Chau e Li (2019) desenvolveram um modelo que integra o desengajamento moral e o clima ético organizacional para entender o comportamento de violação da política de segurança da informação no local de trabalho. Foram identificados nessa classe, dois estudos que se utilizaram do modelo da teoria do comportamento planejado para explicar a formação da intenção do comportamento de conformidade com a política de segurança da informação (BÉLANGER *et al.*, 2017; HONG; FURNELL, 2019). No modelo desenvolvido e testado por Grimes e Marquardson (2019) também foi utilizada a teoria do comportamento planejado integrada a teoria da motivação de proteção para descrever como a qualidade do sistema evoca normas sociais positivas, reduz a avaliação de ameaças e aumenta a avaliação de enfrentamento para influenciar as intenções de comportamento seguro. Ainda nesse sentido, a pesquisa de Menard, Bott e Crossler (2017) trouxe os modelos da teoria da motivação de proteção integrado à teoria da autodeterminação e compararam aos modelos nativos no contexto de comportamentos de segurança.

Duas pesquisas desenvolveram modelos para elevar o nível de conformidade dos usuários com as políticas de segurança da informação (ALOTAIBI; FURNELL; CLARKE, 2019; D'ARCY; LOWRY, 2019). Entretanto, no modelo proposto por D'Arcy e Lowry (2019) foram inseridos os elementos cognitivos e afetivos. Conforme já havia sido realizado na pesquisa de Jansen e Van Schaik (2017) que comparou três modelos cognitivos sociais em sua capacidade de explicar intenções de comportamento de prevenção. No modelo comportamental proposto por Mermoud *et al.* (2019), os autores teorizam como e por que o comportamento humano e o comportamento de compartilhamento de segurança podem estar associados.

Alshare, Lane e Lane (2018) examinaram os fatores que afetam as violações da política de segurança da informação por funcionários do ensino superior, desenvolvendo um modelo de pesquisa baseado em teorias fundamentadas, como a teoria da dissuasão, a teoria da neutralização e a teoria da justiça. Chen, Chen e Wu (2018) propuseram um modelo de pesquisa baseado no *framework* da consciência-motivação-capacidade, com o objetivo de unificar os fatores para predizer a intenção de conformidade com a política de segurança da informação do funcionário.

Para finalizar os estudos que apresentaram ‘modelos’, foram identificados dois estudos aplicados a área de saúde (ALANAZI *et al.*, 2020; YENG *et al.*, 2021). Os autores Yeng *et al.* (2021) desenvolveram por meio de uma RSL uma estrutura para modelar e analisar as práticas de segurança da informação dos profissionais de saúde relacionadas às suas características individuais, como seus traços psicológicos, sociais e culturais. Alanzi *et al.* (2020) investigaram a utilidade de um modelo baseado em teoria que determinasse os preditores do comportamento de prevenção dos trabalhadores de saúde em hospitais públicos no Reino da Arábia Saudita.

Nessa classe, foram identificados ainda outros três estudos aplicados ao setor da saúde (DONG *et al.*, 2021; PARK *et al.*, 2019; SARKAR *et al.*, 2020). Dong *et al.* (2021) examinaram uma estrutura de pesquisa que se baseia nos fatores do clima organizacional de segurança da informação e na teoria do vínculo social para aprimorar o comportamento de segurança da informação entre os enfermeiros. Sarkar *et al.* (2020) analisaram as diferenças no comportamento de violação da política de segurança da informação entre diferentes subculturas profissionais em uma organização de saúde. Park *et al.* (2019) explicaram teoricamente as intenções de estudantes de enfermagem em divulgar informações protegidas da saúde de pacientes.

Foram destacados, quatro estudos que abordaram a temática ataques de *phishing*[9] (BAX; MCGILL; HOBBS, 2021; HOUSE; RAJA, 2020; LEMAY; BASNET; DOLECK, 2020; MCGILL; THOMPSON, 2021). Dois desses estudos investigaram como os custos de resposta e recompensas influenciam os comportamentos de segurança de proteção e desadaptação dos usuários no domínio do *phishing*. Ambos testaram um modelo que estende a teoria da motivação de proteção (BAX; MCGILL; HOBBS, 2021; MCGILL; THOMPSON, 2021). A pesquisa de House e Raja (2020) exploraram o medo e a autoconfiança em pessoas que enfrentam ataques de *phishing*. Lemay, Basnet e Doleck (2020) propuseram um modelo da relação entre as percepções de ameaças de estudantes universitários, seu nível de ansiedade e uma intenção comportamental de aprender sobre *phishing*.

Quatro estudos objetivaram desenvolver, estender, explicar ou integrar teorias para melhor entender o comportamento em segurança da informação (AHMAD *et al.*, 2020; CHOI; MARTINS; BERNIK, 2018; ORAZI; JOHNSTON; WARKENTIN, 2019; RAJAB; EYDGAHI, 2019). Ahmad *et al.* (2020) desenvolveram uma estrutura conceitual que explica

9 É uma tentativa de adquirir informações confidenciais ou pessoais e geralmente é realizado por e-mail, em que o remetente se disfarça como legítimo e solicita que o destinatário execute uma ação, como clicar em um *link* fornecido (PARSONS *et al.*, 2017)(PARSONS *et al.*, 2017).

como as funções de gerenciamento de segurança da informação e resposta de incidente podem ser melhor integradas. A pesquisa de Rajab e Eydgahi (2019) determinaram a relação entre os fatores atitudinais, comportamentais e organizacionais com o cumprimento da política de segurança da informação com base em quatro teorias, a saber: teoria do comportamento planejado, teoria da motivação de proteção, teoria geral da dissuasão e teoria organizacional. Orazi, Johnston e Warkentin, (2019) discutiram como os pesquisadores podem integrar perfeitamente a teoria de nível de construção em estudos de segurança da informação com base na teoria de motivação de proteção. Choi, Martins e Bernik (2018) estenderam a teoria da segurança da informação, explorando os componentes percebidos de práticas eficazes de segurança da informação de dentro da organização.

Dois artigos abordaram o comportamento em segurança da informação (MUTCHLER, 2019; NASIRPOURI SHADBAD; BIROS, 2021). Os autores Nasirpouri Shadbad e Biros (2021) buscaram entender como diferentes tipos de estresse contribuem para o comportamento de prevenção. Ainda nesse sentido, Mutcher (2019) examinou a influência da percepção da resposta na intenção comportamental.

Para finalizar a Classe 3, as duas pesquisas restantes abordam temáticas distintas (SAFA *et al.*, 2018b; TOPA; KARYDA, 2019). Topa e Karyda (2019) buscaram identificar as implicações dos determinantes do comportamento de segurança para a gestão da segurança com a finalidade de propor as respectivas diretrizes que podem ser integradas as práticas atuais de gestão da segurança, incluindo aquelas que seguem as normas de segurança da informação amplamente adotadas ISO 27001, 27002, 27003 e 27005. Safa *et al.* (2018) mostraram como a colaboração em segurança da informação se forma e se desenvolve no contexto de uma organização com base em fatores de vínculo social.

2.3.3 Classe 2 – Conformidade com as políticas de segurança da informação

A Classe 2 obteve a representatividade de (22,92%) do *corpus*, a segunda maior entre as quatro Classes, apresentando os termos ‘funcionário’, ‘conformidade’, ‘política’, ‘organizacional’, ‘intenção’, ‘ISP’[10], ‘sistema’, ‘influência’, ‘político’ e ‘efeito’ como os mais significativos entre os 33 segmentos de textos, conforme o dendrograma, Figura 5.

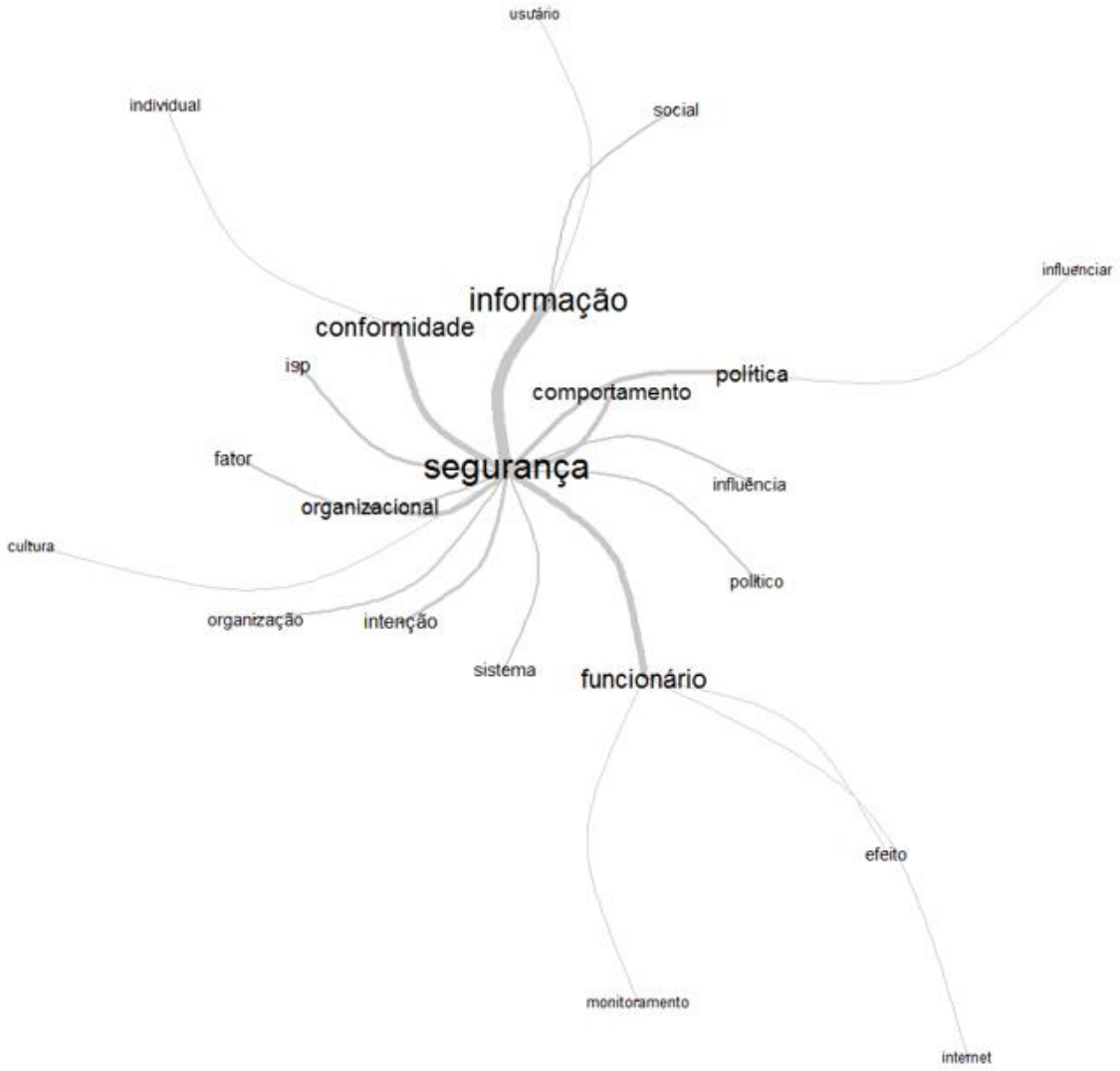
O resultado da análise de similitude, Figura 8, destaca 22 palavras, com 11 delas ilustradas na Classe 2 do dendrograma, Figura 5, com o acréscimo dos termos ‘segurança’,

10 Sigla em inglês para *Information Security Policy (ISP)*, utilizada, por muitos autores, para referenciar as Políticas de Segurança da Informação das instituições.

‘informação’, ‘comportamento’, ‘social’, ‘usuário’, ‘influenciar’, ‘internet’, ‘monitoramento’, ‘organização’, ‘fator’ e ‘cultura’. Observa-se ainda a partir da análise de similitude, Figura 8, uma forte relação do termo ‘segurança’ com os termos ‘informação’, ‘conformidade’, ‘funcionários’, ‘comportamento’ e política, o que ilustra a articulação dos termos para compor a temática de comportamento de conformidade dos funcionários com as políticas de segurança da informação. Esses termos possuíram uma frequência mínima de três aparições nos objetivos dos 32 artigos pertencentes a presente Classe.

É importante destacar que uma política de segurança da informação pode ser compreendida como conjunto de regras que descrevem como tornar os ativos informacionais seguros e como protegê-los de possíveis ameaças, bem como informar aos usuários dessa política, quais são suas responsabilidades, ou seja, o que eles devem ou não fazer para salvaguardar esses ativos. Há um consenso crescente na literatura de que a política de segurança da informação é um documento de negócio cada vez mais importante, que está excepcionalmente bem posicionado para proteger de forma proativa a disponibilidade, a confidencialidade e integridade de todos os recursos de informação corporativo (DOHERTY; TAJUDDIN, 2018). No entanto, ter essa política em vigor não é garantia de que os usuários adotem o comportamento de conformidade, eles podem não se comportar como esperado, seja por comportamento intencional de violação da política, ou mesmo por falta de compreensão de seu conteúdo (ALOTAIBI; FURNELL; CLARKE, 2019).

Figura 8 - Análise de similitude da Classe 2



Fonte: Elaborado pela autora (2023).

Assim, diante da importância do cumprimento das políticas de segurança para as instituições, na Classe 2 foram identificados 23 pesquisas, que abordaram a temática 'comportamento de conformidade ou não conformidade com as políticas de segurança da informação', o que nos proporciona uma compreensão de como esses comportamentos vêm sendo abordados pelos pesquisadores (ALI; DOMINIC; ALI, 2020; ALSHAIKH; ADAMSON, 2021; ALZAHRANI, 2021; AMANKWA; LOOCK; KRITZINGER, 2018; AURIGEMMA; MATTSON, 2017b, 2017c; BURNS *et al.*, 2018; DOHERTY; TAJUDDIN, 2018; FENG *et al.*, 2019; GUAN; HSU, 2020; HWANG *et al.*, 2017a; KHATIB; BARKI, 2021; KIM; HAN, 2019; KOOHANG *et al.*, 2021; LEERING; VAN DE WIJNGAERT; NIKOU, 2020; LI *et al.*, 2019; MAKERI, 2020; SHADBAD; BIROS, 2020; SOLOMON; BROWN, 2020;

SOMMESTAD, 2018; STAFFORD; DEITZ; LI, 2018; TRANG; NASTJUK, 2021; WIAFE *et al.*, 2020)

Dentre os 23 artigos que abordaram o 'comportamento de prevenção', 21 deles mensuram ou analisaram a relação, em maior ou menor intensidade, de algumas variáveis, representadas por valores, conceitos, hábitos ou situações, nas variáveis comportamento de prevenção[11] ou 'comportamento não preventivo' dos funcionários Quadro 8.

Quadro 8 - Variáveis relacionadas ao comportamento de prevenção

VARIÁVEIS	REFERÊNCIAS
*Ansiedade do sistema de segurança, comportamentos não conformes dos colegas e visibilidade da segurança	(ALZAHRANI, 2021)
*Ansiedade do sistema de segurança, impedimento no trabalho e sistemas de segurança.	(HWANG *et al.*, 2017a)
Atitude, autoeficácia, controle comportamental percebido, normas subjetiva e status.	(AURIGEMMA; MATTSON, 2017c)
Atitude, controle comportamental percebido, certeza das sanções, norma subjetivas e gravidade das sanções.	(AURIGEMMA; MATTSON, 2017b)
Atribuição do valor a informação, percepção do valor da informação, percepção do valor da informação pelo grupo de trabalho e percepção do valor da informação estabelecido.	(DOHERTY; TAJUDDIN, 2018)
Autoeficácia, barreira percebida, eficácia de resposta, severidade percebida e vulnerabilidade percebida,	(LI *et al.*, 2019)
Benefícios da segurança, normas sociais e pressões normativas.	(MAKERI, 2020)
Benefícios percebidos de conformidade, custo percebido de conformidade, custos percebidos de não conformidade e responsabilidade social corporativa,	(KIM; HAN, 2019)
*Comportamento habitual não conforme, falta de autoeficácia, pressão do tempo e sensibilidade da informação.	(LEERING; VAN DE WIJNGAERT; NIKOU, 2020)
Comportamento rotineiro não relacionado a tecnologia da informação dos líderes e liderança paternalista.	(FENG *et al.*, 2019)
*Comprometimento organizacional (compromisso afetivo, compromisso de continuidade e compromisso normativo) e supervisão abusiva.	(GUAN; HSU, 2020)

11 Alguns desses estudos optaram por utilizar outras terminologias para referenciar o termo 'comportamento preventivo', tais como: 'comportamento de conformidade', 'comportamento de segurança' ou 'comportamento esperado'. Quanto ao termo 'comportamento não preventivo, alguns autores preferiram utilizar o termo comportamento de não conformidade, comportamento inseguro ou comportamento de violação ou comportamento não preventivo. Entendemos que unificar esses termos em 'comportamento de prevenção' e 'comportamento não preventivo, não alteram a semântico dos termos.

VARIÁVEIS	REFERÊNCIAS
Conscientização em segurança da informação, expectativa de segurança e valência de segurança	(BURNS *et al.*, 2018)
Controle comportamental percebido e Normas percebidas.	(SOMMESTAD, 2018)
Cultura organizacional de suporte, envolvimento do usuário final e liderança de conformidade com as políticas.	(AMANKWA; LOOCK; KRITZINGER, 2018)
Cultura organizacional e cultura de segurança da informação.	(SOLOMON; BROWN, 2020)
*Custos percebidos e recompensas	(KHATIB; BARKI, 2021)
Estresse ocupacional, projetos de política de segurança da informação	(TRANG; NASTJUK, 2021)
Intenção de atitude de conformidade, normas descritivas, normas pessoais e normas subjetivas.	(WIAFE *et al.*, 2020)
Medo e Valores de função	(KOOHANG *et al.*, 2021)
*Tecnoestresse (tecnosobrecarga, tecnoinsegurança, tecnocomplexidade, tecnoincerteza e tecnoinvasão).	(SHADBAD; BIROS, 2020)
Vínculo social (apego, comprometimento, envolvimento e normas pessoais dos funcionários em relação às tarefas relacionados à segurança da informação).	(ALI; DOMINIC; ALI, 2020)

Fonte: Elaborado pela autora (2023).
Nota: * Pesquisas que fizeram relação com o comportamento não preventivo.

As pesquisas de Alshaikh e Adamson (2021) e de Stafford, Deitz e Li (2018) também abordaram a mesma temática, mas não mensuraram a relação de variáveis ao comportamento de prevenção. Alshaikh e Adamson (2021) tiveram como objetivo explicar como as organizações podem mudar as atitudes dos funcionários em relação ao comportamento de prevenção; e Stafford, Deitz e Li (2018) investigaram o papel da conformidade da política de segurança da informação e o papel da auditoria de sistemas de informação na identificação de não conformidade no local de trabalho, com foco específico no comportamento não malicioso dos funcionários.

Os nove artigos restantes, inseridos na Classe 2, apresentam abordagens diversificadas. As pesquisas de Jiang *et al.* (2020) e Ahmad *et al.* (2019) abordaram a influência e os efeitos do monitoramento na segurança da informação; Qazi, Raza e Khan (2020) analisaram o comportamento de compartilhamento do conhecimento na consciência de segurança da informação; Karjalainen, Siponen e Sarker (2020) explicaram as razões das mudanças de comportamento em segurança da informação dos funcionários; Chu e So (2020) desenvolveram

instrumentos de autorrelato para uma avaliação de comportamento antiético de segurança da informação; Merhi e Ahluwalia (2019) examinaram o papel da punição organizacional e das normas organizacionais no impacto da resistência dos funcionários às políticas do sistema de segurança da informação; Choi (2019) examinou o efeito moderador da orientação à distância do poder, uma espécie de valor cultural, sobre a relação entre controle organizacional e comportamentos desviantes da segurança da informação dos funcionários; Snyman, Kruger e Kearney (2018) investigaram o paradoxo da privacidade na segurança da informação; e Dang-Pham, Pittayachawan e Bruno (2017b) que utilizaram a análise de redes sociais para investigar a influência interpessoal dos comportamentos de segurança da informação no local de trabalho.

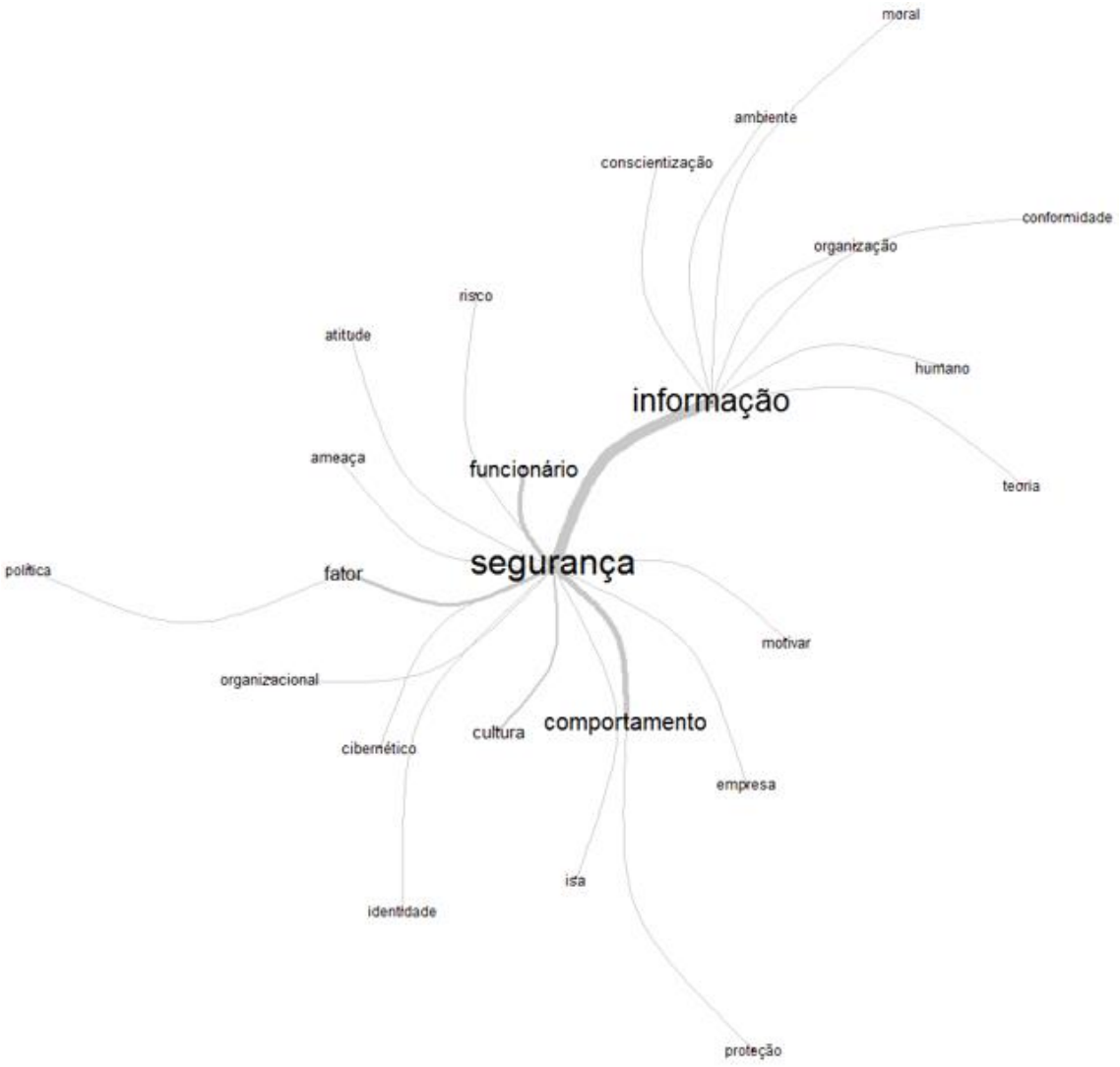
2.3.4 Classe 1 – Comportamento em segurança da informação

A Classe 1 denominada, 'Comportamento em segurança da informação' obteve a maior representatividade, 32,64% do *corpus,* apresentando os termos 'segurança', 'informação', 'cultura', 'ISA' e o verbo 'motivar' como os mais significativos entre os 47 segmentos de textos da classe, de acordo com a Figura 5, que ilustra o dendrograma.

Observa-se que o resultado da análise de similitude, Figura 9, destaca 24 palavras, com sete delas ilustradas na Classe 1 do dendrograma, Figura 5, com o acréscimo dos termos 'conscientização', 'ambiente', 'moral', 'organização', 'conformidade', 'humano', 'teoria', 'funcionário', 'risco', 'atitude', 'ameaça', 'fator', 'organizacional' 'cibernética, 'cultura', 'política' e 'proteção'. Observa-se ainda a partir da análise de similitude, Figura 9, uma forte relação do termo 'segurança' com os termos 'informação', 'comportamento' e 'funcionários' o que refletiu diretamente nas temáticas inseridas nessa classe. Esses termos possuíram uma frequência mínima de três aparições nos objetivos dos 46 artigos que compõem a Classe 1.

Seis artigos pertencentes a esta classe foram apresentados na Classe 4 por estarem diretamente relacionado a temática 'conscientização em segurança da informação' (HADLINGTON *et al.*, 2019; HADLINGTON; BINDER; STANULEWICZ, 2020; HWANG *et al.*, 2021; MCCORMAC *et al.*, 2018; PARSONS *et al.*, 2017; WILEY; MCCORMAC; CALIC, 2020).

Figura 9 - Análise de similitude da classe 1



Fonte: Elaborado pela autora (2023).

Os resultados indicam 21 estudos que abordam a temática ‘comportamento em segurança da informação’ como principal foco (ALMINDEEL; MARTINS, 2020; CANO; ALMANZA, 2020; CONNOLLY; LANG; WALL, 2019; CROSSLER; BÉLANGER; ORMOND, 2019; DEBB; MCCLELLAN, 2021; GUHR; LEBEK; BREITNER, 2019; HADLINGTON, 2018; HADLINGTON; BINDER; STANULEWICZ, 2021; HOOPER; BLUNT, 2020; KIM; KIM, 2017; KOLOSENI; LEE; GAN, 2019; LANKTON; STIVASON; GURUNG, 2019; MENARD; WARKENTIN; LOWRY, 2018; OGBANUFE, 2021; OGBANUFE; CROSSLER; BIROS, 2021; SAFA *et al.*, 2018b; SANTOS; SILVA, 2021; XU; WARKENTIN, 2020; XU; GUO, 2019; ZHEN; XIE; DONG, 2020a, 2020b).

Na Classe 1 serão apresentados ainda cinco pesquisas, inseridas na Classe 4, que apesar de abordar a conscientização, possuem uma ênfase maior no comportamento em segurança da

informação (ALZAHRANI; JOHNSON, 2019; DANG-PHAM; PITTAYACHAWAN; BRUNO, 2017a; GANGIRE; VEIGA; HERSELMAN, 2021; SNYMAN; KRUGER, 2021; WALL; PALVIA; D'ARCY, 2021).

Dentre os estudos que abordam a temática 'comportamento em segurança da informação', sete deles objetivaram pesquisar sobre alguns fatores relacionados ao comportamento dos funcionários em relação a segurança da informação, e dois estudos determinaram quais fatores podem influenciar esse comportamento (GUHR; LEBEK; BREITNER, 2019; HADLINGTON, 2018; HOOPER; BLUNT, 2020; LANKTON; STIVASON; GURUNG, 2019; OGBANUFE, 2021; OGBANUFE; CROSSLER; BIROS, 2021; SANTOS; SILVA, 2021; XU; WARKENTIN, 2020; ZHEN; XIE; DONG, 2020b), conforme Quadro 9.

Quadro 9 – Fatores relacionados ao comportamento em segurança da informação

FATORES	AUTORES
Ameaças à segurança, identidade de segurança da informação, política de segurança e suporte organizacional.	Ogbanufe, Crossler e Biros (2021)
Apoio percebido da instituição, conscientização das políticas de segurança, expectativas dos outros e identidade do papel de segurança da informação.	Ogbanufe (2021)
Atitude cognitiva dos indivíduos, grau de persuasão do argumento de segurança, mensagens de segurança da informação, mentalidade de rebanho e pistas de popularidade.	Xu, Warkentin (2020)
Atitudes em relação à segurança cibernética, consciência geral do crime cibernético, frequência de se envolver em comportamentos *online* de risco, idade e tamanho da empresa.	Hadlington (2018)
Comprometimento organizacional, eficácia da equipe e grau de satisfação de suas necessidades psicológicas (necessidades de autonomia, necessidades de competência e necessidades de relacionamento)	Zhen, Xie e Dong (2020b)
Dimensões da intensidade e criticidade organizacional e moral.	Lankton, Stivason e Gurung (2019)
Liderança	Guhr, Lebek e Breitner (2019)

Fonte: Elaborado pela autora (2023).

As pesquisas desenvolvidas por Santos e Silva (2021) e Hooper e Blunt (2020) determinaram quais fatores influenciam o comportamento de segurança da informação dos funcionários. Santos e Silva (2021) que realizaram sua pesquisa em uma instituição federal brasileira, não identificada por questões de proteção da informação, concluíram que um dos

fatores que mais influenciam no comportamento de segurança dos servidores está relacionado a um conflito existente na própria prescrição do trabalho. A pesquisa de Hooper e Blunt (2020) foi aplicada aos funcionários de tecnologia da informação de uma empresa na Nova Zelândia e os resultados indicaram que a autoeficácia e o impacto percebido de um evento foram os fatores que mais influenciaram no comportamento em segurança da informação dos funcionários.

Quatro estudos buscaram estabelecer relações entre comportamento e conscientização em segurança da informação (ALMINDEEL; MARTINS, 2020; CANO; ALMANZA, 2020; HADLINGTON; BINDER; STANULEWICZ, 2021; ZHEN; XIE; DONG, 2020a). Duas pesquisas objetivaram identificar quais comportamentos de segurança são executados pelos funcionários. (CROSSLER; BÉLANGER; ORMOND, 2019; KOLOSENI; LEE; GAN, 2019). Os autores Connolly, Lang e Wall (2019) e Menard, Warkentin e Lowry (2018) avaliaram a relação dos aspectos culturais com os comportamentos seguros.

Os estudos de Snyman e Kruger (2021) e Gangire e Veiga (2021) apresentaram formas de avaliar o comportamento em segurança da informação. Snyman e Kruger (2021) desenvolveram um *framework* para avaliação do comportamento de grupos na prática de segurança da informação; e Gangire e Veiga (2021) criaram um questionário para avaliar o mesmo comportamento.

Wall, Palvia e D'arcy (2021) abordaram a gestão de controles[12] de segurança para estudar o comportamento. Esses autores apresentaram uma tipologia e um modelo teórico de controles de segurança baseado em uma extensão da teoria de controle que podem influenciar no comportamento do funcionário. A pesquisa realizada por Alzahrani e Johnson (2019) examinou como o processo de hierarquia analítica é usado como orientação na tomada de decisão sobre a política de segurança da informação, identificando os fatores de influência e seus pesos para o comportamento de prevenção. Dang-Pham, Pittayachawan e Bruno (2017) propuseram a adoção de métodos de análise de redes sociais no campo da segurança da informação comportamental.

Os cincos últimos artigos que apresentaram como foco o 'comportamento em segurança da informação' são as pesquisas de Debb e Mcclellan (2021), que examinaram as atitudes e comportamentos de segurança da informação que contribuem para a vulnerabilidade percebida da segurança; Xu e Guo (2019), que investigaram como e por que os funcionários deixam de realizar as tarefas de segurança exigidas; Safa *et al.* (2018), que analisaram se o aumento do

12 Controles de segurança da informação existem para prevenir estados futuros indesejáveis, restringindo comportamentos. Os funcionários querem que algo seja feito, mas, em alguns casos, os controles de segurança atuam como obstáculos (VAN SLYKE; BELANGER, 2020).

esforço e do risco associado ao mau comportamento de segurança da informação, reduzindo recompensas e provocações, e removendo desculpas ou justificativas para o mau comportamento funcionam para mitigar ameaças internas nas organizações; e a pesquisa de Kim e Kim (2017) que buscou compreender, na perspectiva da gestão do conhecimento, como funciona o mecanismo de diferentes comportamentos de conformidade e como a tecnologia da informação é usada para a gestão da conformidade em ambientes corporativos.

Como pode ser observado no Dendrograma, Figura 5 e na Análise de Similitude, Figura 9, a temática 'cultura', que apesar de estar presente em outras classes, obteve maior representatividade na Classe 1, abrangendo cinco artigos (CONNOLLY *et al.*, 2017; MD AZMI *et al.*, 2021; NEL; DREVIN, 2019; UCHENDU *et al.*, 2021; VEIGA *et al.*, 2020). O que corrobora a ideia de Connolly *et al.* (CONNOLLY *et al.*, 2017) de que a cultura organizacional é um forte preditor do comportamento de segurança da informação do funcionário. Conforme mencionado, a presente temática também foi inserida nas Análises de Similitude das Classes 2 e 4, devido a estreita relação da 'cultura' com a 'conscientização' e com as 'políticas de segurança da informação'. Rocha Flores e Ekstedt (2016a) declararam que a cultura de segurança da informação possui uma associação direta com a conscientização, com a atitude e com as normativas de segurança.

Os autores Md Azmi *et al.* (2021) analisaram os fatores que influenciam a cultura de segurança da informação entre os funcionários. Uchendu *et al.* (2021) investigaram por meio de uma RSL quatro questões, incluindo como a cultura de segurança cibernética é definida, quais fatores são essenciais para construir e manter tal cultura, os *frameworks* propostos para cultivar uma cultura de segurança e as métricas sugeridas para avaliá-la. Veiga *et al.* (2020) determinaram em sua pesquisa o conceito de cultura de segurança da informação a partir de uma perspectiva da indústria para complementar a teoria existente. Drevin (2019) identificou os principais aspectos da cultura de segurança da informação em organizações na África do Sul. Por fim, Connolly *et al.* (CONNOLLY *et al.*, 2017) investigaram como a cultura organizacional e as contramedidas de segurança tendem a influenciar as ações de segurança dos funcionários.

Nessa classe, foram identificados ainda dois estudos que abordaram os aspectos humanos da segurança da informação (AMINI; VAKILIMOFRAD; SABERI, 2021; VAN SLYKE; BELANGER, 2020); duas revisões sistemáticas de literatura (ALYAMI *et al.*, 2021; YUPANQUI; ORÉ, 2018); e três pesquisas que abordaram os fatores que influenciam o cumprimento das medidas de segurança da informação (BARLETTE; JAOUEN, 2019; KHAN; ALSHARE, 2019; LIU; WANG; LIANG, 2020).

As sete pesquisas restantes abordam temáticas distintas: violação da segurança da informação (FARSHADKHAH; VAN SLYKE; FULLER, 2021); práticas de *Bring-Your-Own-Device*[13] (BYOD) (CHEN *et al.*, 2020a); ataques de *spear phishing* (ALEROUD *et al.*, 2020); intenção de comportamento de segurança (AIGBEFO; BLOUNT; MARRONE, 2020); conflitos e denúncia de irregularidades (BERNDTSSON; JOHANSSON; KARLSSON, 2018); escala de comprometimento em segurança da informação (CHULKOV, 2017); e formulação de políticas e comunicação da segurança cibernética (BRUIJN; JANSSEN, 2017).

2.4 CONSIDERAÇÕES SOBRE A REVISÃO SISTEMÁTICA DE LITERATURA

A partir desta RSL, primeiro objetivo específico desta tese, foi possível responder a seguinte questão de pesquisa: quais as principais características das produções científicas relacionadas ao comportamento humano em segurança da informação?

Na análise dos 160 artigos, percebemos um crescimento contínuo e expressivo dos artigos que estudam a temática de 'comportamento humano em segurança da informação', o que demonstra a importância de compreender melhor esse comportamento.

Esta RSL nos proporcionou construir um panorama de como a temática vem sendo estudada no período de 2017-2021: quais foram as principais metodologias utilizadas (tipo de pesquisa, abordagem e instrumento de coleta); onde essas pesquisas foram aplicadas (público, instituição e país); quais eram seus objetivos; quais as teorias utilizadas para suportar essas pesquisas; quais as principais temáticas abordadas; quais variáveis foram mensuradas; quais foram os autores mais citados; onde essas pesquisas foram publicadas e, por fim, como esses artigos foram organizados em *clusters*, a partir de estatística de texto.

A partir da análise bibliométrica, identificamos a preferência dos autores ao traçar a metodologia para estudar a temática "comportamento humano em segurança da informação", que incluem estudos empíricos com abordagem quantitativa e o uso de questionários *on-line* como principal instrumento de coleta. Com relação ao país que mais desenvolve essas pesquisas, os EUA se destacam como o país que mais estuda essa temática. As empresas seguidas das universidades foram as instituições mais pesquisadas, sendo os funcionários o público mais pesquisado no contexto empresarial e os estudantes no contexto das universidades.

Esta RSL nos permitiu ainda perceber uma dissonância entre as pesquisas sobre

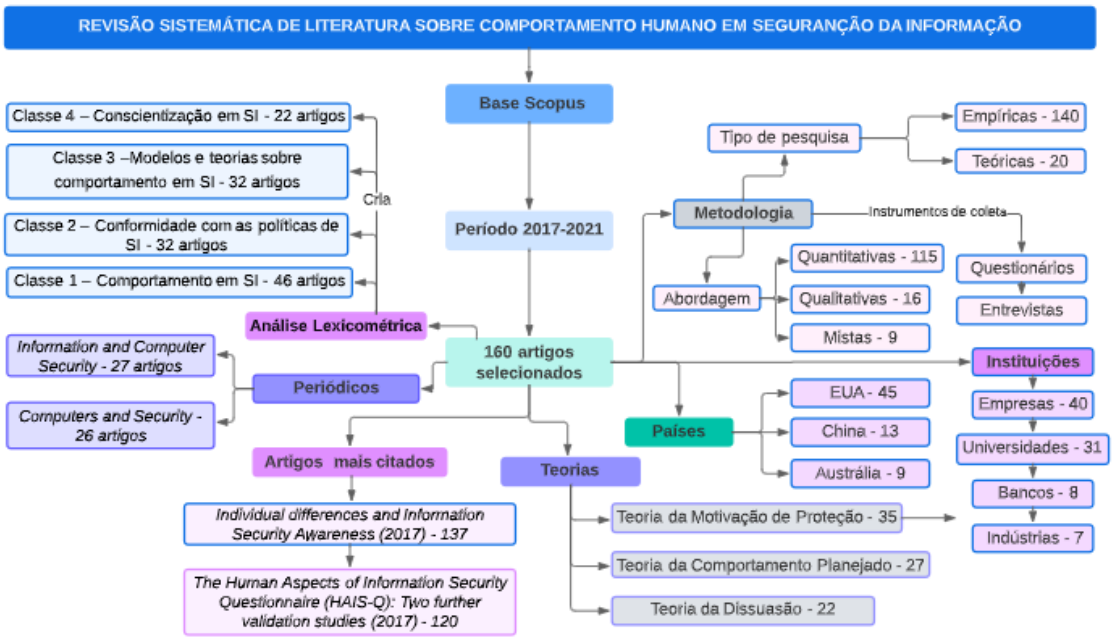
13Sigla para *Bring Your Own Device*, em português "traga seu próprio dispositivo". Os dispositivos como celulares, tablets, laptops e drives USB, de propriedade dos funcionários, são usados dentro da instituição.

comportamento humano em segurança da informação realizadas no Brasil e no mundo, o que demonstra a escassez de pesquisas direcionadas a compreender e prever o comportamento em segurança da informação dos *stakeholders* das instituições brasileiras.

A variedade de teorias identificadas para estudar o comportamento humano em segurança da informação destaca a abordagem interdisciplinar da temática, que é indiretamente evidenciada pelos autores dos artigos analisados, tornando necessária uma visão global que inclua não apenas o ponto de vista tecnológico, mas também, a perspectiva de outras disciplinas, como a social. Ressalta-se, novamente, o comportamento humano como crucial na gestão da segurança da informação, uma vez que, intencionalmente ou não, o fator humano pode colocar em risco os recursos organizacionais.

A análise lexicométrica realizada com o auxílio do *software Iramuteq* nos permitiu a analisar os objetivos dos 160 artigos recuperados na RSL. A partir da Classificação Hierárquica Descendente pelo método de Reinert, foi elaborado o dendrograma contendo quatro classes distintas, a saber: Classe 1 – Comportamento em segurança da informação; Classe 2 – Conformidade com as políticas de segurança da informação; Classe 3 – Modelos e teorias sobre comportamento em segurança da informação; e Classe 4 – Conscientização em segurança da informação. A catalogação dos artigos nas referidas classes nos trouxe a luz a forma como estudos que abordam a temática ‘comportamento humano em segurança da informação’ se relacionam com outras temáticas e como essas relações são necessárias para uma melhor compreensão desse comportamento. De outro modo, a análise de similitude nos permitiu visualizar graficamente a estrutura do conteúdo de cada classe a partir da relação entre as palavras e da força dessa relação. A Figura 10 ilustra os principais resultados da RSL.

Figura 10 - Principais resultados da RSL



Fonte: Elaborado pela autora (2023).

2.5 COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO

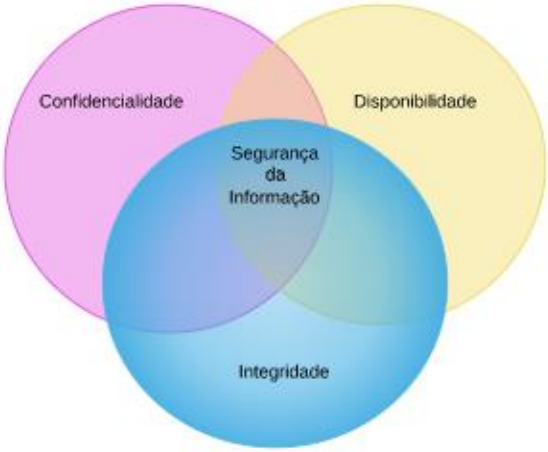
Com o avanço tecnológico e as mudanças nos mercados de bens e serviços, a informação obteve importância como ativo de grande valor. As organizações utilizam os ativos de informação para uma melhor produtividade, redução de custos, aumento de agilidade, vantagens competitivas e apoio nas decisões estratégicas (SÊMOLA, 2014). De acordo com o Glossário de Segurança da Informação, criado por meio da Portaria nº 93, de 26 de setembro de 2019, os ativos de informação são os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos a que eles têm acesso (BRASIL, 2019).

Em virtude da importância dos ativos de informação, as organizações de modo geral necessitam protegê-los contra destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada (ABNT NBR ISO/IEC 27002, 2013a), em que há a necessidade de ações continuadas alicerçadas por conceitos sólidos e amplamente reconhecidos, desenvolvidos por áreas especializadas apoiadas nas normas e padrões do campo da segurança da informação.

De acordo com Sêmola (2014) a segurança da informação é uma área do conhecimento dedicada à proteção de ativos de informação contra acesso não autorizado, alterações indevidas

ou sua indisponibilidade. Trata-se de uma área fundamentada na garantia de três propriedades básicas: **confidencialidade** – as informações são protegidas contra a divulgação para usuários não autorizados, **integridade** – proteção contra modificação indevida, e **disponibilidade** – acesso quando requerido (ISACA, 2012; SÊMOLA, 2014). Entretanto, o maior desafio configura-se no alcance do equilíbrio entre essas propriedades que se comportam de forma complementar, conforme ilustrado na Figura 11.

Figura 11- Propriedades da segurança da informação



Fonte: Elaborado pela autora (2023).

A partir das interseções dessas propriedades, consegue-se alcançar a segurança da informação, mas para isso torna-se fundamental contemplar as três dimensões que envolvem a segurança da informação: pessoas, processos e tecnologia que constituem a base das ações da gestão de segurança da informação, cuja função é determinar o encaminhamento do processo de segurança de forma sistemática, baseado em definições de estratégias e monitoramento dos controles estabelecidos pelas normas específicas e adotadas pelas organizações (SÊMOLA, 2014).

No âmbito da segurança da informação, os controles são medidas adotadas para evitar ou diminuir o risco de um ataque (BRASIL, 2019). A pesquisa desenvolvida por Malatji, Marnewick e Von Solms (2020) categorizou os controles de segurança em: sociais (estrutura organizacional e humanos), técnicos (tecnologia e atividades de trabalho) e ambientais (requisitos legais, acordos, conformidade regulamentar etc.). Os resultados indicaram que adotar abordagens excessivamente tecnocêntricas não produz resultados significativamente positivos na proteção de ativos de informação, é necessária uma abordagem técnico-social.

Do mesmo modo, para Alotaibi, Furnell e Clarke (2019) as organizações podem acreditar que a implementação de controles técnicos mais avançados minimizará o risco

associado ao comportamento humano. No entanto, como muitos invasores começaram a incluir meios sociais em seus esforços mal-intencionados, por exemplo, engenharia social, surgiu a necessidade de uma abordagem holística no tratamento de problemas de segurança da informação, considerando um equilíbrio entre os controles técnicos e não técnicos (CONNOLLY *et al.*, 2017). Esse reconhecimento levou, e ainda leva, a muitos diferentes estudos sobre como entender e gerenciar os vários aspectos humanos, como conhecimento, atitude e comportamento em segurança da informação (KEARNEY; KRUGER, 2016).

Anteriormente, as avaliações de risco associadas à tecnologia concentravam-se em vários fatores de tecnologia, mas a partir do início do século XXI, o fator humano passou a ser a questão mais importante identificada nos estudos de risco de tecnologia.(STEWART; JÜRJENS, 2017). Muitas pesquisas têm reconhecido que o comportamento humano desempenha um papel crucial em muitas falhas de segurança. As pessoas podem ser facilmente influenciadas pelas circunstâncias e podem divulgar informações sensíveis (às vezes inconscientemente, outras vezes com intenções específicas) que podem ter um efeito prejudicial na segurança e integridade dos sistemas com os quais interagem (SNYMAN; KRUGER, 2017b). Essas fragilidades que os seres humanos exibem, quando comparados com camadas técnicas de segurança, fazem com que sejam considerados o elo mais fraco da cadeia de segurança (BURNS *et al.*, 2018; CONNOLLY *et al.*, 2017; HADLINGTON; PARSONS, 2017; MCCORMAC *et al.*, 2017a; PARSONS *et al.*, 2017; SAFA; MAPLE, 2016; ZWILLING *et al.*, 2020).

Diante desse contexto, tem havido um foco crescente em pesquisas sobre o papel que o comportamento humano desempenha no contexto da segurança da informação (ABDALLAH *et al.*, 2020; AL-HARTHY *et al.*, 2020; ARAÚJO, 2016; ARAÚJO; BATISTA; ARAÚJO, 2015; ARAUJO; ARAÚJO, 2016; HADLINGTON, 2018; HADLINGTON; PARSONS, 2017; MCCORMAC *et al.*, 2017b; SAFA *et al.*, 2015; SAFA; MAPLE, 2016; SAFA; VON SOLMS, 2016).

Para Hamid, Yumid e Yusof (2019), a falha em evitar violações de segurança custa à organização enormes perdas e má reputação. De acordo com o relatório de custo da violação de dados de 2022, realizado pela IBM em 550 empresas de 17 países e em 17 setores diferentes, impactadas por violações em segurança da informação, ataques do tipo *ransomware*[14] foram

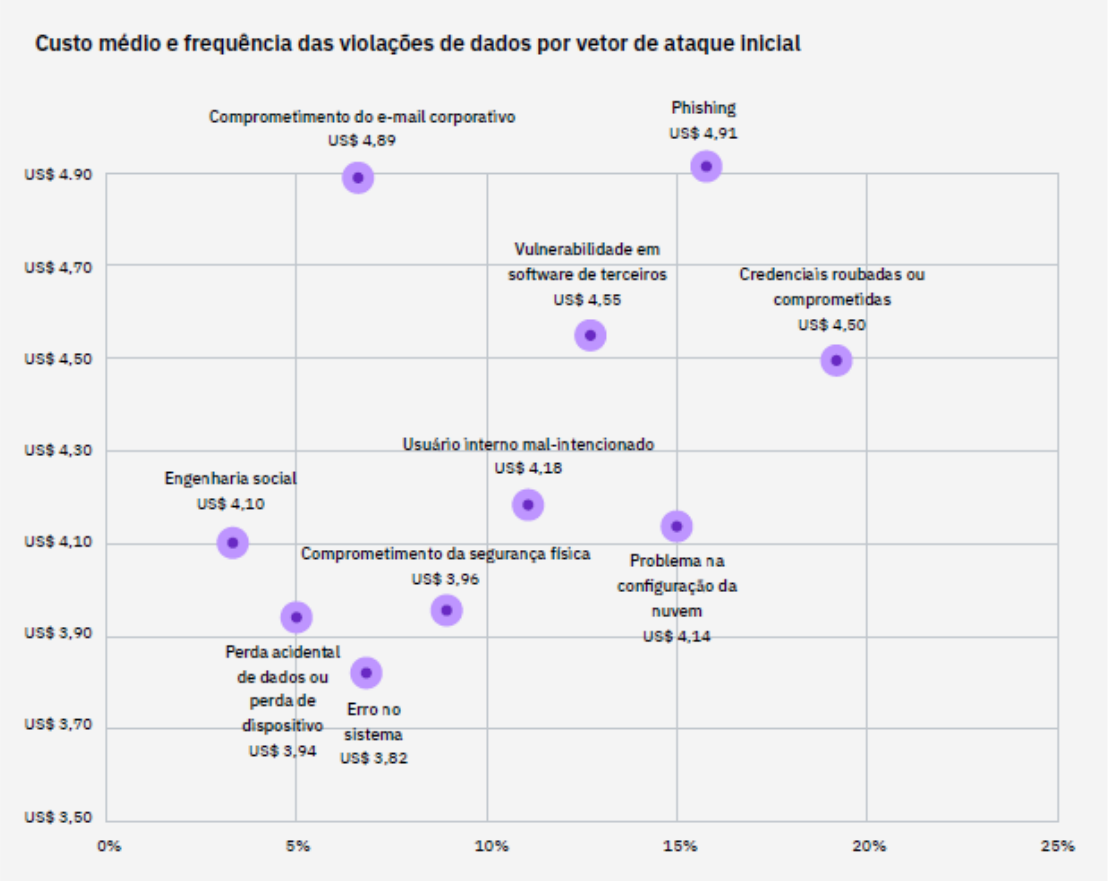
[14] Software nocivo que **é** usado para bloquear dados de computadores **e** servidores através do uso de algum tipo de criptografia. Esse *malware* **é** usado por *hackers* para exigir resgates para liberar os dados bloqueados. A proteção contra esse tipo de ataque consiste em não clicar em *links* inseguros, evitar a divulgação de informações pessoais, não abrir anexos de *e-mail* suspeitos, não usar *pendrives* USB desconhecidos, manter programas e sistemas operacionais atualizados e usar apenas fontes de download conhecidas.

responsável por 11% das violações, erros humanos, ou seja, violações causadas involuntariamente por ações negligentes de funcionários ou terceirizados, foram responsáveis por 21% das violações (IBM SECURITY, 2022). Apesar do relatório separar as estatísticas o ataque de *ransomware* se apropria de erros humanos.

O mesmo relatório identificou ainda, conforme Figura 12, os vetores de ataque inicial mais comuns em 2022 e o custo médio de cada violação, mensurado em milhões (US$). Os vetores relacionados ao comportamento humano: *phishing*, usuário interno mal-intencionado e engenharia social, apresentaram (16%), (11%) e (4%), respectivamente, dos ataques, sendo o *phishing* o vetor de ataque inicial que gerou mais custos em 2022, em média, (US$ 4,91 milhões). A soma dos três vetores gerou um custo médio de US$ 13,19 milhões para as empresas que participaram da pesquisa. Quanto ao custo médio de uma violação de dados por país, os Estados Unidos foram o país com o maior custo médio total de uma violação de dados de US$ 9,44 milhões. Isso representa US$ 0,39 milhão a mais do que os US$ 9,05 milhões em 2021.

O Brasil foi 16º país com o custo médio de US$ 1,38 em 2022, o que representa US$ 0,30 milhão a mais do que US$ 1,08 milhões em 2021. É importante destacar que, de acordo com o relatório, 60% das empresas participantes da pesquisa aumentaram o preço de seus produtos e serviços devido à violação de dados (IBM SECURITY, 2022). Esses resultados reforçam a importância da segurança da informação para as organizações e o papel do comportamento humano nessa segurança, além disso, podemos concluir que, de forma involuntária, o cidadão comum (consumidor de bens e serviços) termina por também sofrer as consequências dessas violações.

Figura 12 - Custo médio de frequência das violações de dados por vetor de ataque inicial



Fonte: Relatório de custo da violação de dados de 2022 (IBM SECURITY, 2022).

Embora as ações humanas possam introduzir ameaças, riscos e vulnerabilidades à segurança, os funcionários também são a primeira linha de defesa da organização para combater e mitigar ameaças à segurança cibernética (SAFA; VON SOLMS; FURNELL, 2016). As abordagens comportamentais mais comuns para ajudar a prevenir incidentes são as políticas de segurança da informação e as campanhas de conscientização. As políticas de segurança da informação descrevem os comportamentos adequados e proibidos dos funcionários, além de suas responsabilidades na prevenção de incidentes de segurança. As campanhas de conscientização geralmente têm o objetivo de aumentar o conhecimento dos funcionários sobre os riscos cibernéticos e a segurança cibernética para que possam entender melhor por que e como devem cumprir os regulamentos de segurança da informação (VAN DER KLEIJ; WIJN; HOF, 2020). Para Aurigemma e Mattson (2017b), os funcionários devem ser adequadamente capacitados e ter a motivação para cumprir as políticas de segurança da informação.

2.6 TEORIA DA MOTIVAÇÃO DE PROTEÇÃO

A Teoria da Motivação de Proteção (TMP) foi proposta por Rogers (1975) com o objetivo de apresentar um modelo conceitual que se propunha a esclarecer a influência de campanhas de comunicação com apelos ao medo sobre atitudes e comportamento. A excitação ao medo era originalmente considerada o mediador dos efeitos à mudança de atitude e comportamento. Posteriormente, a TMP foi ampliada e revisada, direcionando a ênfase para "motivação de proteção" ao invés do "medo" projetando-se para enfatizar a importância dos processos cognitivos (ROGERS, 1983).

Essa teoria tem sido usada em pesquisas em diferentes campos, incluindo a área da saúde, o campo político, segurança, ambiental e de nutrição, indicando que a TMP pode ser aplicada a qualquer ameaça para a qual exista uma autoproteção eficaz e que pode ser realizada por um indivíduo, tornando-se uma das melhores teorias explicativas para prever a intenção de comportamento protetor (FLOYD; PRENDICE-DUNN; ROGERS, 2000).

A TMP teoriza que, quando um indivíduo é provocado por uma ameaça, ele avalia cognitivamente a situação por meio de uma avaliação da ameaça e de um mecanismo de enfrentamento associado. Após o processo de avaliação, o indivíduo decide encenar um comportamento adaptativo[15] ou não adaptativo. Comportamentos adaptativos são respostas sugeridas que são consideradas eficazes para proteger o indivíduo contra a ameaça. As respostas não adaptativas são compostas de qualquer variedade de comportamentos nos quais o indivíduo não consegue executar a resposta recomendada (MENARD; WARKENTIN; LOWRY, 2018).

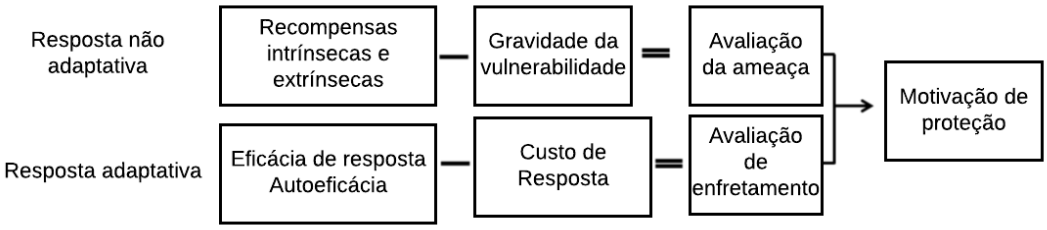
Nessa condição, Rogers (1983) explica o modelo da TMP com base no seguinte exemplo: medo e apelos a mudança de atitude poderiam ser adotados (por exemplo, começando a fumar). Os fatores que aumentam a probabilidade de resposta não adaptativa (isto é, reforços positivos) incluem recompensas intrínsecas (por exemplo, prazer corporal, satisfação) e recompensas extrínsecas (por exemplo, aprovação social). Os fatores que diminuem a probabilidade de ocorrência da resposta não adaptativa (ou seja, punidores) são a gravidade ou risco da ameaça e a expectativa de ser exposto à ameaça (ou seja, a vulnerabilidade). Embora a gravidade geralmente se refira a lesões corporais, ela também pode envolver ameaças intrapessoais (por exemplo, autoestima) e ameaças interpessoais (por exemplo, relações familiares e profissionais).

15 Comportamento adaptativo corresponde ao comportamento de prevenção ou comportamento de conformidade.

De acordo com Rogers (1983), supondo-se que a avaliação desses fatores aumente ou diminua a probabilidade de desadaptação para produzir a avaliação final de ameaça, o processo de avaliação de enfrentamento avalia a capacidade de lidar e evitar o perigo da ameaça. As crenças em aumentar a probabilidade da resposta adaptativa são as crenças de que a resposta de enfrentamento recomendada é eficaz (por exemplo, "parar de fumar é uma maneira eficaz de evitar os perigos associados ao tabagismo") e que pode executar com êxito a resposta de enfrentamento (por exemplo, "Eu posso parar de fumar").

A avaliação de enfrentamento é um resumo dessas avaliações da eficácia da resposta, autoeficácia e quaisquer "custos" da adoção das medidas de respostas preventivas recomendadas: inconveniência, despesa, desagrado, dificuldade, complexidade, efeitos colaterais, interrupção da vida diária e superação da força do hábito (ROGERS, 1983). A Figura 13, ilustra o modelo da TMP.

Figura 13 - Modelo da Teoria de Motivação de Proteção



Fonte: Rogers (1983).

No ambiente de segurança da informação, a TMP apresenta-se como uma das teorias que mais se mostrou eficaz na tentativa de prever e explicar o comportamento de prevenção (HWANG *et al.*, 2017b; JANSEN *et al.*, 2016; JANSEN; VAN SCHAIK, 2017, 2018a; MENARD; WARKENTIN; LOWRY, 2018; SAFA; VON SOLMS, 2016). Progressivamente, a TMP tem chamado a atenção das pesquisas sobre segurança da informação, fornecendo uma boa base para estudos nessa área, variando desde comportamento de conformidade com a política de segurança de sistemas da informação a adoção de *software* (JANSEN; VAN SCHAIK, 2018a).

Na TMP, o comportamento de prevenção corresponde à variável resultante da intenção de prosseguir, continuar ou evitar determinado comportamento (FLOYD; PRENDICE-DUNN; ROGERS, 2000). Compreendendo-se que essa teoria se configura nos componentes principais da avaliação das ameaças e avaliação de enfrentamento, deve-se especificar que dessas duas dimensões resultam seis variáveis: da avaliação de ameaça surgem – risco percebido,

vulnerabilidade percebida e gravidade percebida; da avaliação de enfrentamento surgem – eficácia de resposta, autoeficácia e custo de resposta.

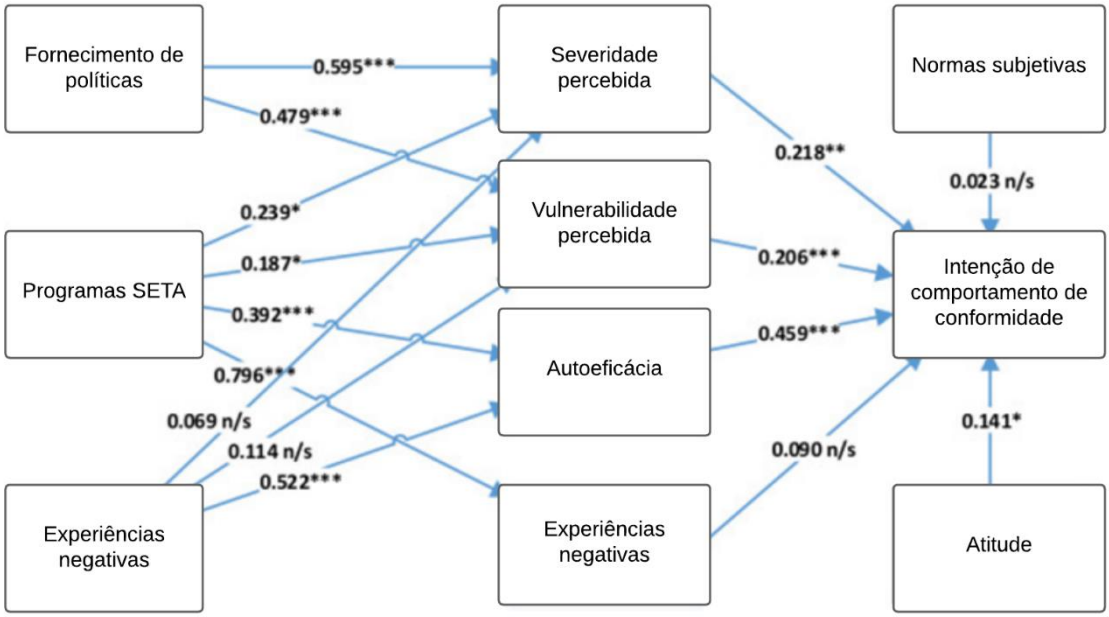
A avaliação de ameaça está relacionada com as percepções de como um indivíduo se sente ameaçado; o risco percebido é a avaliação de quão prejudicial é a ameaça; vulnerabilidade é a probabilidade de que um incidente indesejado possa acontecer caso não sejam tomadas medidas para impedi-lo; a gravidade percebida diz respeito ao impacto que uma ameaça pode causar ao indivíduo; os benefícios se referem a qualquer motivação intrínseca ou extrínseca para aumentar ou manter um comportamento desejado. A avaliação de enfrentamento centra-se nas respostas disponíveis que o indivíduo possui para lidar com a ameaça, dessa forma, a eficácia da resposta refere-se à crença que um indivíduo possui sobre a eficácia de um determinado comportamento em relação a minimizar uma ameaça; a autoeficácia corresponde a crença na capacidade de proteger informações e sistemas de informação contra divulgação não autorizada, modificação, perda, destruição e falta de disponibilidade; o custo da resposta é quantidade de tempo, dinheiro ou esforço necessário para executar a resposta recomendada (JANSEN; VAN SCHAIK, 2017; MENARD; WARKENTIN; LOWRY, 2018; SAFA; VON SOLMS, 2016b).

A partir da revisão sistemática de literatura, apresentada no início desta seção, foram identificados trinta e cinco artigos que estudaram o comportamento em segurança da informação associado aos princípios da TMP. Essas pesquisas apresentaram várias possibilidades de relações entre as variáveis. Alguns estudos omitem algumas variáveis da teoria, enquanto outros ampliam a TMP, inserindo novas variáveis ao modelo ou fazendo associações entre a TMP e outras teorias comportamentais. A avaliação do comportamento de segurança, geralmente utilizada como variável dependente, difere entre as pesquisas, umas concentram-se em medir a intenção de comportamento, enquanto outras medem o comportamento real em segurança da informação.

A pesquisa desenvolvida por Hina, Selvam e Lowry (2019) descreveu um teste empírico da influência da governança institucional na motivação de proteção e no comportamento planejado de funcionários em instituições de ensino superior da Malásia. Essa pesquisa associou variáveis de duas teorias testadas (TMP e Teoria do Comportamento Planejado), foram integrados ainda três fatores críticos adicionais - fornecimento de políticas de segurança da informação, programas e experiência negativa para avaliar a influência na intenção comportamental de cumprir as políticas de segurança da informação. Os resultados sugerem que o fornecimento de políticas e programas SETA, em conjunto com experiências pessoais negativas, são as principais fontes de informações de segurança em um contexto de instituições

de ensino superior. A vulnerabilidade percebida e a autoeficácia influenciam diretamente a intenção de comportamento de conformidade com as políticas de segurança da informação, conforme pode ser observado no resultado do modelo de pesquisa proposto, Figura 14.

Figura 14 - Modelo de pesquisa apresentado por Hina, Selvam e Lowry



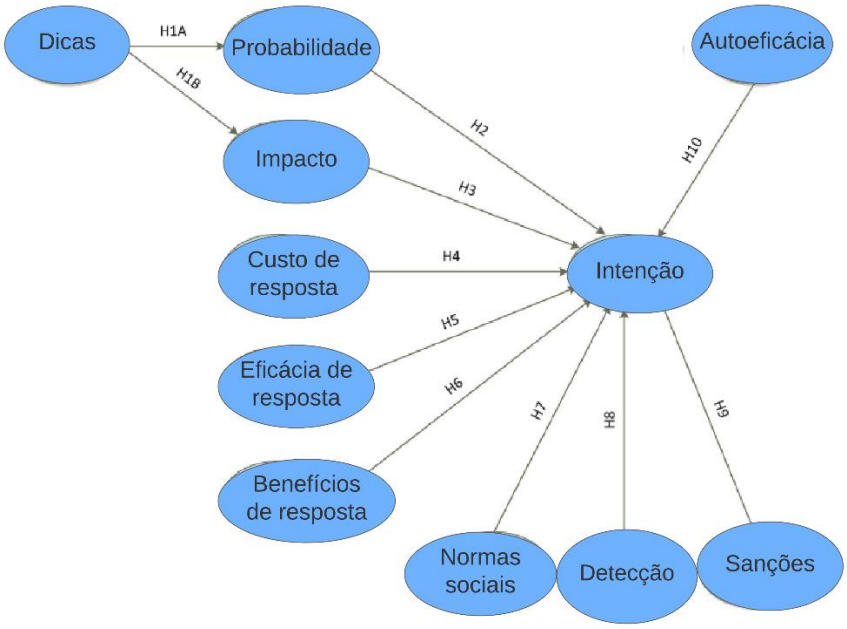
Fonte: Hina, Selvam e Lowry (2019).

Rajab e Eydgahi (2019) realizaram uma pesquisa que analisou a relação entre os fatores atitudinais, comportamentais e organizacionais com o cumprimento da política de segurança da informação pretendido com base em quatro referenciais teóricos suportados empiricamente, a saber: Teoria do Comportamento Planejado, TMP, Teoria Geral da Dissuasão e Teoria Organizacional. A pesquisa foi aplicada em universidades dos Estados Unidos e os resultados sinalizaram que sanções severas, supervisão de gestão próxima, pressão dos pares e atitudes em relação à segurança da informação não influenciam tanto quanto a vulnerabilidade percebida e a eficácia da resposta em garantir níveis mais altos de intenções de cumprir as políticas de segurança das universidades. O estudo recomenda que universidades e faculdades invistam em treinamento de segurança da informação aplicado aos funcionários, bem como para a comunidade universitária em geral.

A pesquisa realizada por Hooper e Blunt (2020), que objetivou determinar quais fatores influenciam o comportamento de segurança da informação dos funcionários de tecnologia da informação de empresas da Nova Zelândia, obteve como principal resultado que o

comportamento dos funcionários é influenciado pela autoeficácia e pelo impacto percebido de um evento potencial. A Figura 15 ilustra o modelo de pesquisa utilizado pelos pesquisadores.

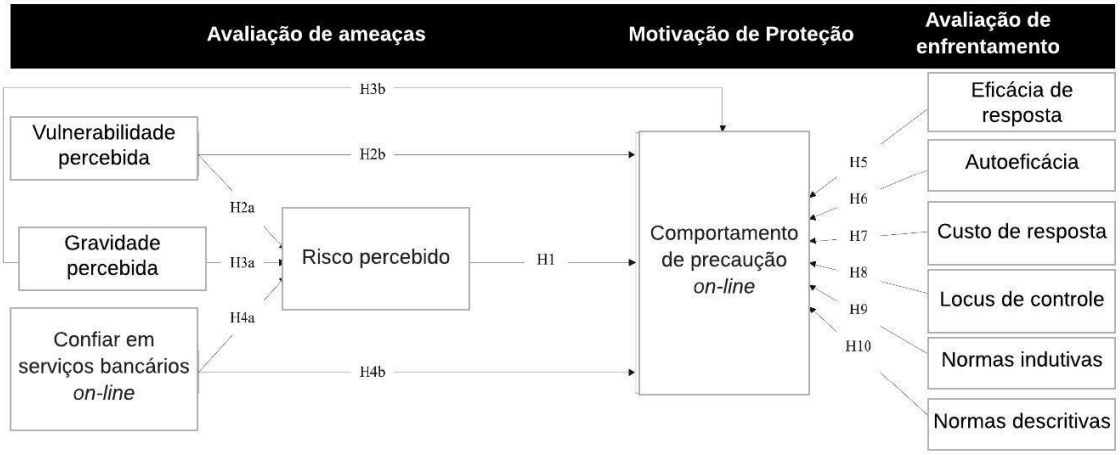
Figura 15 - Modelo de pesquisa apresentado Hooper e Blunt



Fonte: Hooper e Blunt (2020).

A pesquisa realizada por Jansen e Van Schaik (2018b), com objetivo de desenvolver um modelo de comportamento *on-line* de precaução para clientes de banco *on-line*, com base na TMP e outros modelos comportamentais, apresentou os resultados que fornecem suporte para a maioria dos relacionamentos hipotéticos e mostram que o modelo explica altos níveis de variação para o comportamento o*n-lin*e de precaução, bem como para a percepção de risco. A avaliação de ameaças e enfrentamento prevê com êxito a motivação de proteção dos clientes de serviços bancários *on-line*; em particular, a eficácia da resposta e a autoeficácia são as variáveis que mais influenciam no comportamento preventivo. A Figura 16 ilustra o modelo de pesquisa apresentado pelos referidos autores.

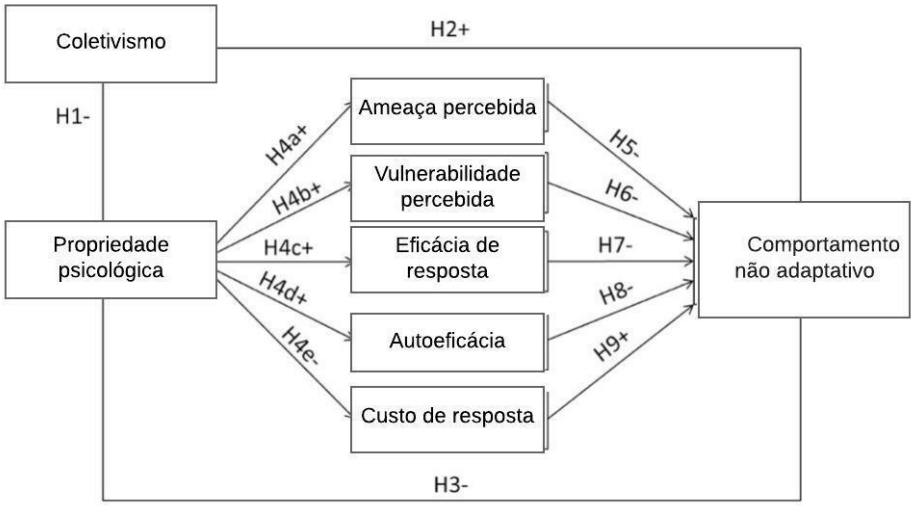
Figura 16 - Modelo de pesquisa apresentado por Jansen e Van Schaik



Fonte: Jansen e Van Schaik (2018b).

A pesquisa desenvolvida por Menard, Warkentin e Lowry (2018) analisou as potenciais diferenças entre características individuais – coletivismo e propriedade psicológica da informação – dentro do contexto de comportamentos relacionados à segurança da informação. Os resultados desse estudo indicam que a orientação pessoal de um indivíduo em relação ao coletivismo tem um impacto na propriedade psicológica e na intenção de não realizar comportamentos seguros. Além disso, a propriedade psicológica mostrou ter um impacto significativo nos construtos da motivação de proteção, bem como na intenção de comportamento. O modelo da pesquisa apresenta-se na Figura 17.

Figura 17 - Modelo de pesquisa apresentado por Menard, Warkentin e Lowry

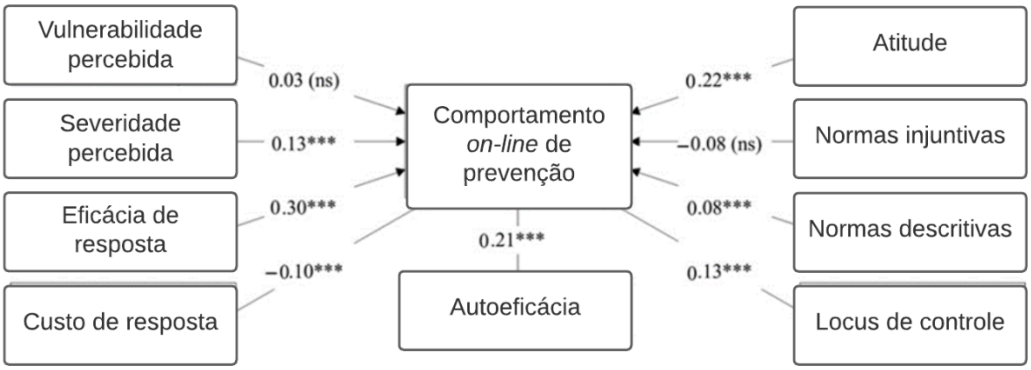


Fonte: Menard, Warkentin e Lowry (2018).

Em relação à pesquisa desenvolvida por Jansen e Van Schaik (2017) que comparou três modelos cognitivos sociais em sua capacidade de explicar as intenções do comportamento

preventivo *on-line*: TMP, Abordagem de Ação Racionalizada e um modelo integrado compreendendo variáveis desses dois modelos. Os resultados indicaram que 64% da variação no comportamento *on-line* de precaução é explicada pela TMP, a partir das variáveis: vulnerabilidade percebida, gravidade percebida, eficácia da resposta, autoeficácia e custos de resposta. A variável positiva mais forte foi a eficácia da resposta, seguida por autoeficácia e gravidade percebida, e o custo de resposta apresentou-se como variável negativa. A vulnerabilidade percebida não teve efeito significativo sobre o comportamento *on-line* de prevenção. Os resultados da pesquisa estão ilustrados na Figura 18.

Figura 18 - Modelo de pesquisa apresentado por Jansen e Van Schaik



Fonte: Jansen e Van Schaik (2017).

A partir dos resultados apresentados, compreende-se as várias possibilidades de utilizar a TMP para prever e explicar o comportamento de prevenção. Evidenciando que seus princípios podem ser cientificamente aplicáveis ao contexto das universidades. Para Rajab e Eydgahi (2019) a TMP fornece o melhor arcabouço teórico para compreender o comportamento dos funcionários do ensino superior em relação ao cumprimento da segurança da informação. A próxima seção apresenta a aplicação da TMP para compreender o comportamento em segurança da informação dos servidores das universidades federais e os procedimentos metodológicos estabelecidos para o desenvolvimento desta pesquisa

3 PROCEDIMENTOS METODOLÓGICOS

Nesta seção serão apresentados os fundamentos e os procedimentos metodológicos que foram estabelecidos para o desenvolvimento da pesquisa. A sua estrutura encontra-se organizada conforme a lógica da pesquisa científica com a apresentação da sua caracterização, descrição da tipologia, abordagens que foram utilizadas, universo e amostra selecionados, instrumentos de coleta de dados aplicados, validação do instrumento, detalhamento dos procedimentos de coleta de dados e, por fim, o método de análise dos dados.

3.1 CARACTERIZAÇÃO DA PESQUISA

A pesquisa caracterizou-se como aplicada, cujos objetivos classificam-na como descritiva e correlacional com apoiou na abordagem quali-quantitativa, uma vez que o objetivo dela foi analisar comportamento em segurança da informação dos servidores das universidades federais brasileiras, sob a ótica da Teoria da Motivação de Proteção.

A utilização da pesquisa aplicada justifica-se por essa metodologia permitir que o conhecimento gerado, a partir da análise de determinada problemática em condições da realidade, possa ser direcionado para a solução de problemas específicos do cotidiano (GIL, 2012). Nesse sentido, esta pesquisa atendeu ao objetivo específico de desenvolver um modelo de intenção de comportamento de prevenção para as universidades federais sob a perspectiva da TMP, de modo a possibilitar uma melhor compreensão sobre o comportamento dos servidores em relação à segurança da informação.

A pesquisa descritiva se dá pela necessidade de atingir os objetivos específicos de: identificar quais os controles relacionados ao comportamento humano são utilizados pelos servidores das universidades federais. A pesquisa descritiva busca, desse modo, descrever as características de determinada população, a partir de uma série de informações sobre o que se deseja pesquisar, além de exigir uma precisa delimitação de técnicas, métodos e teorias que orientarão a coleta e interpretação dos dados (GIL, 2012; TRIVIÑOS, 1987). Utilizamos ainda, a pesquisa correlacional para atingir o objetivo de investigar as relações entre vulnerabilidade percebida; gravidade percebida das ameaças; gravidade percebida das sanções; eficácia da resposta; autoeficácia; normas injuntivas; normas descritivas; conscientização; fortalecimento da política e capacitação com a intenção de comportamento de prevenção dos servidores. As pesquisas correlacionais possuem a finalidade conhecer a relação ou o grau de associações

existentes entre dois ou mais conceitos, categorias ou variáveis em um contexto específico. (SAMPIERE; COLLADO; LUCIO, 2013).

Quanto à abordagem, optou-se pela pesquisa quali-quantitativa de forma sequencial, iniciando-se com a qualitativa, seguida da quantitativa, mas adotando-se pesos diferentes. Neste estudo, a abordagem qualitativa obteve menor peso sobre a quantitativa. Na qualitativa, foram realizadas entrevistas semiestruturadas para uma melhor compreensão do problema e aprimoramento do instrumento de coleta de dados quantitativo. Nesse sentido, Richardson (2009) esclarece que a pesquisa social deve estar orientada à melhoria das condições de vida de uma população e, para tanto, é necessário, na medida do possível, integrar métodos, abordagens e técnicas para enfrentar esse desafio.

3.2 UNIVERSO E AMOSTRA DA PESQUISA

O universo ou população da pesquisa consiste no total de elementos que apresentam as características comuns que correspondem ao objeto de investigação (PARDAL; LOPES, 2011). Para esta pesquisa, o universo foi constituído pelos servidores (docentes e técnico-administrativos) das universidades federais brasileiras que, de acordo com as informações fornecidas pelo Ministério da Educação, por meio do Serviço de Informação ao Cidadão (SIC), em 04 de janeiro de 2022, o Brasil possui 69 universidades federais compostas por 85.763 docentes, 3.322 docentes do Ensino Básico, Técnico e Tecnológico (EBTT) e 100.709 técnico-administrativos, apresentando o total de 189.698 servidores.

De acordo com Gil (2012) os universos de pesquisa são classificados como finitos e infinitos: universos finitos são aqueles cujo número de sujeitos não excede a 100.000, enquanto que universos infinitos apresentam número de sujeitos superior a esse. Desse modo, esta pesquisa caracterizou-se como universo infinito por apresentar um número superior a 100.00 mil sujeitos.

Concernente à amostra, é importante considerar que esta pesquisa trabalhou com duas dimensões de abordagens: qualitativa seguida da quantitativa, condição que exigiu da pesquisa o trabalho com dois tipos de amostras. A amostra, ou população amostral, corresponde a uma parte do universo escolhido, seguindo a sua seleção a partir de determinado critério de representatividade (VERGARA, 2006).

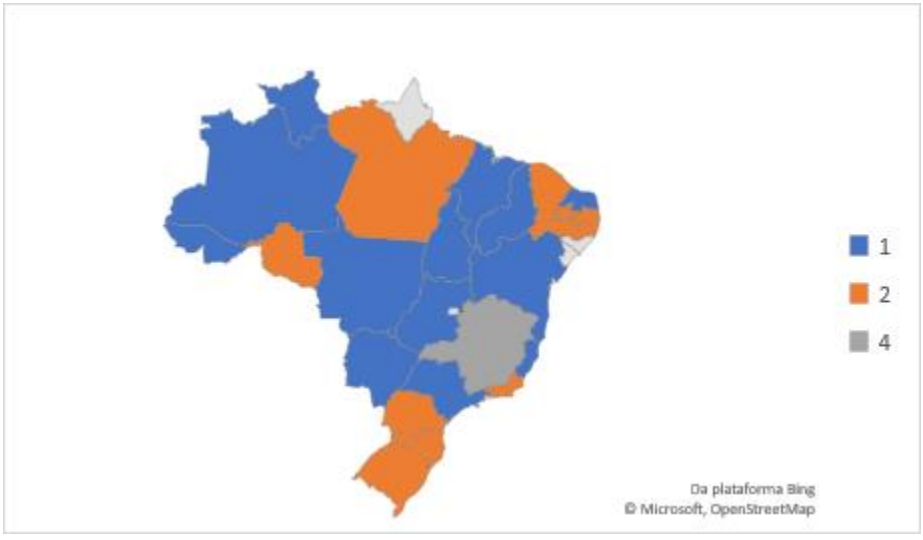
Quanto à amostra qualitativa, a pesquisa recorreu à amostra por acessibilidade ou conveniência, que correspondeu a dois especialistas em segurança da informação da UFPB. A escolha por esses profissionais ocorreu em virtude da pesquisadora ser servidora da referida

universidade. De acordo com Gil (2012) aplica-se este tipo de amostragem em estudos qualitativos, onde não é requerido elevado nível de precisão.

O estabelecimento da amostra quantitativa fundamentou-se no tipo intencional, constituindo-se como um tipo de amostra não probabilística e consiste em selecionar um subgrupo da população que, com base nas informações disponíveis, possa ser considerado representativo de toda a população (GIL, 2012). Essa amostra foi dividida em dois grupos: o primeiro grupo foi composto pelos gestores de segurança da informação das universidades federais. A partir de *sites* oficiais e grupos de *WhatsApp,* foram recuperados 42 contatos desses gestores, sendo a amostra constituída por 23 gestores de segurança da informação que responderam ao questionário *on-line*.

O segundo grupo da amostra desta pesquisa correspondeu à totalidade de servidores que responderam ao questionário *on-line*, ou seja, 663 servidores, sendo 227 docentes e 436 técnico-administrativos que representam 36 universidades federais, distribuídas nas cinco regiões do Brasil. O Mapa Coroplético, Figura 19 representa por cores o número de universidades que compõem a amostra da pesquisa por estado. O Quadro 10 discrimina as universidades e suas respectivas regiões. Destacamos que não houve critérios rígidos definidos para escolha das universidades na composição da amostra, uma vez que o convite para participar da pesquisa foi divulgado nos grupos de *WhatsApp e* nas comunidades da rede social *Facebook,* formados por servidores de universidades federais, e, principalmente, enviados por e-mails, obtidos por meio da plataforma Sucupira, bem como disponibilizados nos *sites* oficiais das universidades.

Figura 19 - Mapa Coroplético das universidades que compõem a pesquisa por estado.



Fonte: Elaborado pela autora (2023).

Quadro 10 - Universidades participantes da amostra da pesquisa e região

Universidades	Sigla	Região
Universidade Federal da Paraíba	UFPB	Nordeste
Universidade Federal de Campina Grande	UFCG	Nordeste
Universidade Federal do Ceará	UFC	Nordeste
Universidade Federal do Cariri	UFCA	Nordeste
Universidade Federal da Bahia	UFBA	Nordeste
Universidade Federal de Pernambuco	UFPE	Nordeste
Universidade Federal Rural de Pernambuco	UFRPE	Nordeste
Universidade Federal do Rio Grande do Norte	UFRN	Nordeste
Universidade Federal do Piauí	UFPI	Nordeste
Universidade Federal do Maranhão	UFMA	Nordeste
Universidade de Brasília	UnB	Centro-Oeste
Universidade Federal da Grande Dourados	UFGD	Centro-Oeste
Universidade Federal de Goiás	UFG	Centro-Oeste
Universidade Federal de Mato Grosso	UFMT	Centro-Oeste
Universidade Federal de Rondonópolis	UFR	Centro-Oeste
Universidade Federal do Acre	UFAC	Norte
Universidade Federal do Amazonas	UFAM	Norte
Universidade Federal do Pará	UFPA	Norte
Universidade Federal de Rondônia	UNIR	Norte
Universidade Federal do Tocantins	UFT	Norte
Universidade Federal do Sul e Sudeste do Pará	UNIFESSPA	Norte
Universidade Federal de Roraima	UFRR	Norte
Universidade Federal do Espírito Santo	UFES	Sudeste
Universidade Federal Fluminense	UFF	Sudeste
Universidade Federal de Juiz de Fora	UFJF	Sudeste
Universidade Federal de Uberlândia	UFU	Sudeste
Universidade Federal de Viçosa	UFV	Sudeste
Universidade Federal de Lavras	UFLA	Sudeste
Universidade Federal do Estado do Rio de Janeiro	UNIRIO	Sudeste
Universidade Federal de São Paulo	UNIFESP	Sudeste
Universidade Federal do Rio Grande do Sul	UFRGS	Sul
Universidade Federal da Fronteira Sul	UFFS	Sul
Universidade Federal de Santa Catarina	UFSC	Sul
Universidade Federal de Santa Maria	UFSM	Sul
Universidade Tecnológica Federal do Paraná	UTFPR	Sul
Universidade Federal do Paraná	UFPR	Sul

Fonte: Elaborado pela autora (2023),

Para validarmos a amostra, tornou-se necessário o cálculo do número mínimo de indivíduos que deve constitui-la. Assim, considerando uma margem de erro de 5%, um nível de confiança de 95% e uma heterogeneidade de 50%, a amostra considerada válida deve ser constituída de, no mínimo, 385 sujeitos, número obtido em decorrência de cálculos matemáticos e estatísticos. Ressalta-se que esse valor é o mínimo válido para as amostras de universo infinito. Como esta pesquisa obteve 663 respondentes, ou seja, um número 72,21% superior ao mínimo necessário, a referida amostra torna-se válida.

3.3 INSTRUMENTOS DE COLETA DE DADOS

Com o intuito de alcançar os objetivos propostos, utilizou-se, inicialmente, como instrumento de coleta de dados uma entrevista semiestruturada, aplicada a dois especialistas em segurança da informação da UFPB. As entrevistas, Apêndice A, possibilitaram uma melhor compreensão do problema e, principalmente, aprimorou o questionário *on-line*, utilizado para a coleta de dados com os servidores das universidades federais. A entrevista semiestruturada em um estágio exploratório ajuda os pesquisadores a explorar a questão de pesquisa antes de usar um questionário para coletar dados (ALI; DOMINIC; ALI, 2020). Ainda nesse sentido, para garantir que a instrumentação e a abordagem sejam adequadas, antes da coleta de dados primários, é importante submeter as medidas e instrumentação a especialistas no assunto (BURNS; POSEY; ROBERTS, 2021).

Em seguida, utilizou-se dois tipos de questionários; o primeiro foi aplicado aos gestores de segurança da informação das universidades, Apêndice B, para atender ao objetivo específico de: b) identificar quais os controles, relacionados ao comportamento humano em segurança da informação são utilizados pelos servidores das universidades federais. O segundo, Apêndice C, principal instrumento de coleta de dados desta pesquisa, foi aplicado aos servidores (docentes e técnicos) das universidades para cumprir os objetivos específicos de c) investigar as relações entre vulnerabilidade percebida; gravidade percebida das ameaças; gravidade percebida das sanções; eficácia da resposta; autoeficácia; normas injuntivas; normas descritivas; conscientização; fortalecimento da política e capacitação com a intenção de comportamento de prevenção dos servidores; e d) desenvolver um modelo de comportamento preventivo para as universidades federais, baseado na TMP. Para Richardson (2009), o questionário é uma série ordenada de perguntas que pode ser utilizado para obter informações acerca de grupos sociais, cumprindo pelo menos duas funções: descrever as características e medir determinadas variáveis de um grupo social.

A opção pela utilização do questionário *on-line* estruturado ocorreu por ser o instrumento mais utilizado nas pesquisas sobre comportamento humano em segurança da informação que abordam a TMP, identificadas pela Revisão Sistemática da Literatura (RSL), como nas pesquisas de (AURIGEMMA; MATTSON, 2019; BAX; MCGILL; HOBBS, 2021; BURNS; POSEY; ROBERTS, 2021; CHEN; CHEN; WU, 2018; DEBB; MCCLELLAN, 2021; HINA; SELVAM; LOWRY, 2019; HOOPER; BLUNT, 2020; JAEGER; JANSEN; VAN SCHAIK, 2019, 2017).

A RSL também nos direcionou ao uso da escala de *Likert* de cinco pontos: 1- Discordo totalmente, 2- Discordo parcialmente, 3 – Nem concordo nem discordo, 4 – Concordo parcialmente e 5 - Concordo totalmente. A escala de *Likert* é um conjunto de itens apresentados como afirmações para mensurar a relação do respondente em três, cinco ou sete categorias. Os itens ou enunciados consistem em afirmações ou juízos, sobre os quais os respondentes vão reagir. Para cada alternativa da escala é definido um valor numérico, que vai resultar numa pontuação para cada item, e no final, uma pontuação total para todas as afirmações (SAMPIERE; COLLADO; LUCIO, 2013). Definiu-se que quanto maior a pontuação, melhor os resultados. Para isso, foi necessário proceder à inversão da escala quando a afirmação estava com sentido negativo, como nos itens 9, 22, 23, 24, 25, 26, 27, 36 e 42. Nesses itens, a pontuação da escala ficou definida como: 5 - Discordo totalmente, 4 - Discordo parcialmente, 3 - Nem concordo nem discordo, 2 - Concordo parcialmente e 1 - Concordo totalmente.

As variáveis e os itens do questionário foram adaptados a partir de pesquisas de Hina, Selman e Lowry (2019); Rajab e Eydgahi, (2019) e Jansen e Van Schaik (2017), identificadas na RSL. Essas pesquisas utilizaram a TMP como suporte, de forma isolada ou associada a outras teorias comportamentais como a Teoria do Comportamento Planejado e a Teoria da Dissuasão.

A exceção foi a pesquisa de Pattinson *et al* (2019), utilizada como referência para medir a variável conscientização. Nesse estudo, os autores não abordaram uma teoria comportamental, mas estabeleceram ainda mais a validade ao Questionário de Aspectos Humanos de Segurança da Informação (HAIS-Q[16]), como um instrumento eficaz para medir a conscientização em segurança da informação, motivo pelo qual essa referência contribuiu para mensurar a referida variável. Para Hooper e Blunt (2020), sempre que possível, para aumentar a confiabilidade das variáveis e dos resultados, os itens do instrumento de pesquisa devem ser adaptados de pesquisas anteriores. Dessa forma, as variáveis do modelo já foram testadas e validadas em outros modelos comportamentais de segurança da informação.

16 *Human Aspects of the Information Security Questionnaire (HAIS-Q).*

Compreendendo que a TMP organiza suas variáveis em processos cognitivos[17] que os indivíduos aplicam para avaliar ameaças e as medidas de enfrentamento, deve-se especificar que desses dois processos resultam cinco variáveis: da avaliação de ameaça surgem – vulnerabilidade percebida e gravidade percebida; da avaliação de enfrentamento surgem – eficácia de resposta, autoeficácia e custo de resposta (FLOYD; PRENDICE-DUNN; ROGERS, 2000). Embora essa teoria seja a espinha dorsal desta pesquisa, inserimos na avaliação de ameaças a variável gravidade percebida das sanções e na avaliação de enfrentamento, inserimos as variáveis normas injuntivas, normas descritivas, fortalecimento da política de segurança da informação (PSI), capacitação e conscientização. De certo modo, a experiência e as crenças dos servidores em relação à segurança, as ações de conscientização e o treinamento oferecido por suas instituições têm um efeito significativo na percepção da gravidade da segurança da informação (LI *et al*., 2019). Portanto, acreditamos que as variáveis incluídas na TMP tornam essa teoria mais adequada para melhorar nossa compreensão sobre o comportamento em segurança da informação dos servidores das universidades federais.

Na TMP, o comportamento de prevenção corresponde à intenção de prosseguir, continuar ou evitar determinado comportamento (FLOYD; PRENDICE-DUNN; ROGERS, 2000). Nesta pesquisa, analisamos a variável intenção do comportamento de prevenção, uma vez que foram usados dados de pesquisa autorrelatados (questionário *on-line*) ao invés de comportamentos de segurança reais. Entretanto, anos de pesquisas sobre o comportamento humano usando teorias como teoria do comportamento planejado e TMP descobriram que a intenção comportamental geralmente levam ao comportamento real (AURIGEMMA; MATTSON, 2017a; FLOYD; PRENDICE-DUNN; ROGERS, 2000). Portanto, é importante verificar a relação entre variável intenção de comportamento de prevenção como as variáveis vulnerabilidade percebida, avaliação de ameaças, gravidade percebida das sanções, eficácia de resposta, autoeficácia, custo de resposta, normas injuntivas, normas descritivas, fortalecimento da política de segurança da informação, capacitação e conscientização.

Nesse sentido, no Quadro 11 estão apresentados os constructos, variáveis com suas descrições e respectivas fontes. Por constructo, entende-se uma variável ou um conjunto de variáveis que têm como objetivo representar o significado de um conceito, porém não pode ser medido direto e perfeitamente, mas deve ser medido aproximadamente por indicadores múltiplos (HAIR *et al.*, 2009).

17 Nesta pesquisa os processos cognitivos foram denominados constructos.

Quadro 11 - Relação dos constructos com as variáveis e a referida fonte

Constructos	Variáveis	Descrição	Fonte
Perfil do respondente	Universidade	Qual universidade você está vinculado	Inseridas ao modelo
	Sexo	( ) Feminino ( ) Masculino	
		( ) Não binário	
	Idade	Qual sua idade?	
	Categoria Profissional	( ) Docente ( )Técnico administrativos	
	Tempo de Serviço	Qual seu tempo de serviço?	
	Grau de Escolaridade	( ) Ensino médio incompleto	
		( ) Ensino médio	
		( ) Graduação incompleta	
		( ) Graduação	
		( ) Mestrado incompleto ( ) Mestrado	
		( ) Doutorado incompleto ( ) Doutorado	
		( ) Pós-doutorado ( ) Outros	
Avaliação da Ameaça (avalia o nível de perigo vinculado a um evento de segurança)	Vulnerabilidade Percebida	Avaliação da probabilidade de ocorrência de um incidente de segurança.	TMP
	Gravidade Percebida das Ameaças	Avaliação do impacto das consequências resultantes de um incidente de segurança.	TMP
	Gravidade Percebida das Sanções	Avaliação do impacto das sanções determinadas pelo incidente de segurança.	Inserida ao modelo. Adaptado de Rajab e Eydgahi (2019); Hina, Selvam e Lowry (2019).
Avaliação de enfrentamento (avalia uma determinada estratégia de enfrentamento para mitigar ou evitar um evento de segurança	Eficácia de Resposta	É a eficácia percebida de uma resposta de enfrentamento na redução de uma ameaça.	TMP
	Autoeficácia	Crença na capacidade de proteger informações e sistemas de informação contra divulgação não autorizada, modificação, perda, destruição e falta de disponibilidade.	TMP
	Custo de resposta	Quantidade de tempo, dinheiro ou esforço necessário para executar a resposta recomendada.	TMP

Constructos	Variáveis	Descrição	Fonte
ameaçador)	Normas Injuntivas	São percepções sobre o que deve ou não deve ser feito.	Inserida ao Modelo. Adaptado de Jansen e Van Schaik (2017).
	Normas Descritivas	São percepções de que outras pessoas estão ou não executando o comportamento de prevenção	Inserida ao Modelo. Adaptado de Jansen e Van Schaik (2017).
	Intenção de Comportamento de Prevenção	É a intenção de agir de acordo com as políticas e regras de segurança da informação.	Inserida ao Modelo. Adaptado de Hina, Selvam e Lowry (2019).
	Fortalecimento da Política de Segurança da Informação	A Política de Segurança da Informação está disponível a todos os servidores de forma clara e com procedimentos bem definidos.	Inserida ao Modelo. Adaptado de Hina, Selvam e Lowry, (2019).
	Capacitação	Treinamento realizado em diferentes formas de apresentação.	Inserida ao modelo. Adaptado de Hina, Selvam e Lowry (2019).
	Conscientização (Relato de Incidentes; Informação e Atualização; Uso de e-mail; e gerenciamento de senhas**)**	Reflete a consciência das responsabilidades com a segurança da informação e os meios pelos quais essas responsabilidades são realizadas.	Inserida ao modelo. Adaptado de Parsons *et al* (2017)

Fonte: Elaborado pela autora (2023).

Como pode ser observado no Quadro 11, além das variáveis que compõem o perfil do respondente, 12 variáveis foram estudadas. A variável ‘conscientização’ foi medida por meio de comportamentos relacionados as variáveis relato de incidentes; informação e atualização; uso de e-mail; e gerenciamento de senhas.

As variáveis vulnerabilidade percebida, eficácia de resposta, autoeficácia, custo de resposta, intenção de comportamento de prevenção, fortalecimento da política de segurança da informação e relato de incidentes foram medidas por quatro itens do questionário cada; gravidade percebida das ameaças, normas injuntivas, normas descritivas, capacitação, uso de e-mail, e informação e atualização foram abordados em três itens; gravidade percebida das sanções foi medida em dois itens; e a variável gerenciamento de senhas foi abordada em cinco itens, compondo um questionário de 59 itens. Conforme mencionado anteriormente, cada item

foi medido usando uma escala de *Likert* de cinco pontos, ancorados de "discordo totalmente" a “concordo totalmente”, com exceção dos itens relacionados ao perfil do respondente.

Após a definição das variáveis que foram estudadas e da escala utilizada, tornou-se necessário classificá-las, Quadro 12. As variáveis podem ser classificadas como qualitativas (não métricas ou categóricas) ou quantitativa (métricas). As variáveis qualitativas representam características de um indivíduo, objeto ou elemento que não podem ser medidas ou quantificadas, as respostas são dadas em categorias. As variáveis quantitativas representam características de um indivíduo, objeto ou elemento resultantes de uma contagem finita ou infinita de valores (FÁVERO; BELFIORE, 2017).

Quadro 12 - Classificação das variáveis e dos tipos de escalas da pesquisa

Variáveis	Tipo de variável	Tipo de escala
Universidade	Qualitativa	Nominal
Sexo	Qualitativa	Nominal
Idade	Quantitativa	Razão
Categoria Profissional	Qualitativa	Nominal
Tempo de Serviço	Quantitativa	Razão
Escolaridade	Qualitativa	Ordinal
Vulnerabilidade Percebida	Qualitativa	Ordinal
Gravidade Percebida das Ameaças	Qualitativa	Ordinal
Gravidade Percebida das Sanções	Qualitativa	Ordinal
Eficácia de Resposta	Qualitativa	Ordinal
Autoeficácia	Qualitativa	Ordinal
Custo de resposta	Qualitativa	Ordinal
Normas Injuntivas	Qualitativa	Ordinal
Normas Descritivas	Qualitativa	Ordinal
Intenção de Comportamento de Prevenção	Qualitativa	Ordinal
Fortalecimento da Política de Segurança da Informação	Qualitativa	Ordinal
Capacitação	Qualitativa	Ordinal
Conscientização	Qualitativa	Ordinal

Fonte: Elaborado pela autora (2023).

As variáveis ainda podem ser classificadas de acordo com o nível ou escala de mensuração. Mensuração é o processo de atribuir números ou rótulos a objetos, pessoas, estados ou eventos de acordo com as regras específicas para representar quantidades ou qualidades dos

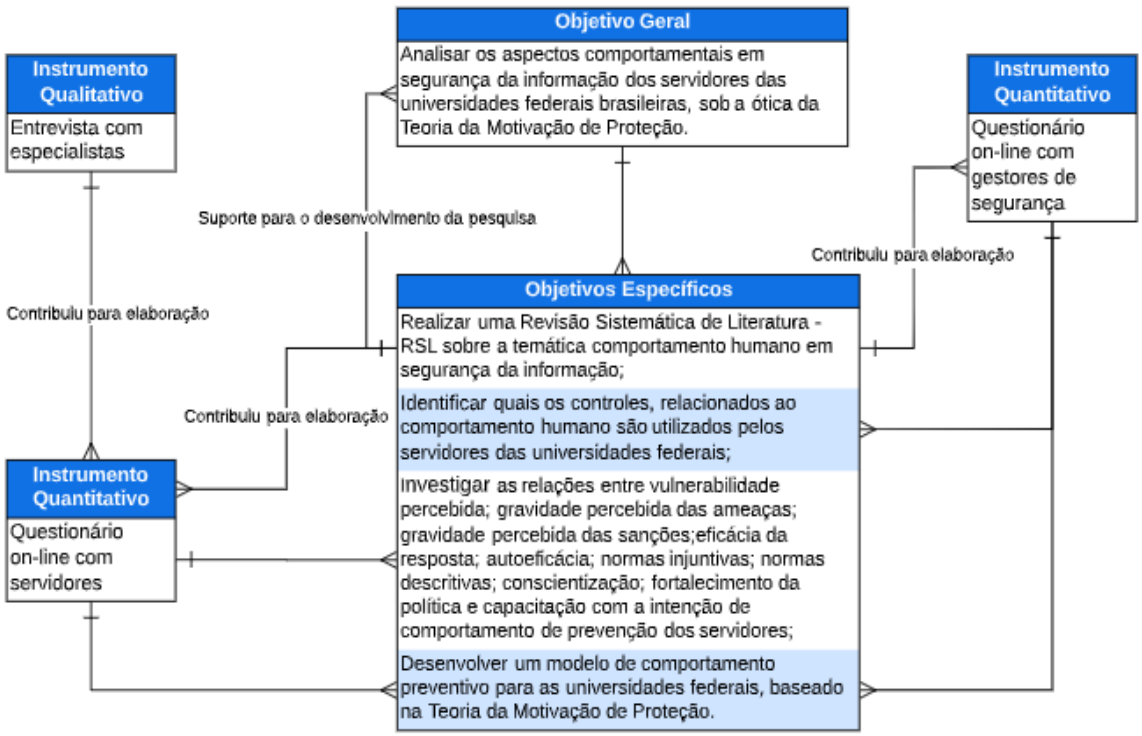
atributos. Regra é um guia, método ou comando que indica ao investigador como medir o atributo. Escala é um conjunto de símbolos ou números, construído com base em uma regra, e aplicável a indivíduos ou a seus comportamentos ou atitudes. As escalas de mensuração das variáveis qualitativas podem ser classificadas como nominal e ordinal, enquanto as variáveis quantitativas classificam-se em escala intervalar e de razão (SAMPIERE; COLLADO; LUCIO, 2013).

A escala nominal classifica as unidades em classes ou categorias em relação à caraterística representada, não estabelecendo qualquer relação de grandeza ou de ordem. É denominada nominal porque as categorias se diferenciam apenas pelo nome. A escala ordinal classifica as unidades em classes ou categorias em relação à característica representada, estabelecendo uma relação de ordem entre as unidades das diferentes categorias. Qualquer conjunto de valores pode ser atribuído às categorias das variáveis, desde que a ordem entre elas seja respeitada. Assim como na escala nominal, operações aritméticas, somas, diferenças, multiplicações e divisões, entre esses valores não fazem sentido (FÁVERO; BELFIORE, 2017). A escala de *Likert* é um tipo de escala classificada como ordinal, ou seja, as variáveis podem ser ordenadas ou ranqueadas em relação à quantia do atributo possuída. Os números empregados em escalas ordinais, contudo, são qualitativos porque indicam apenas posições relativas em uma série ordenada. As escalas ordinais não fornecem qualquer medida da quantia ou magnitude real em termos absolutos, mas apenas a ordem dos valores (HAIR *et al.*, 2009).

As escalas de mensuração das variáveis quantitativas possuem dados em escala intervalar ou de razão. As escalas intervalares e escalas de razão fornecem alto nível de precisão de medida, permitindo que quase todas as operações matemáticas sejam executadas. Essas duas escalas têm unidades constantes de medida, e, portanto, quaisquer dois pontos adjacentes em qualquer parte da escala são iguais. As escalas de razão representam a mais elevada forma de precisão de medida, pois possuem as vantagens de todas as escalas inferiores somadas à existência de um ponto zero absoluto. Todas as operações matemáticas são possíveis com medidas de escala de razão (FÁVERO; BELFIORE, 2017; HAIR *et al.*, 2009).

As relações entre os objetivos e os instrumentos de coleta de dados estão ilustradas na Figura 20.

Figura 20 - Relações dos objetivos com os instrumentos de coleta



Fonte: Elaborado pela autora (2023).

Após o desenvolvimento do questionário, fez-se necessário consolidar sua validação.

3.4 VALIDAÇÃO DO QUESTIONÁRIO

Validade, de forma geral, refere-se ao grau em que um instrumento realmente mensura a variável que pretende mensurar. De acordo com Sampieri, Collado e Lucio (2013), os tipos de validade mais utilizados são: a validade de conteúdo; a validade de critério; a validade de construto; e a validade de especialistas. A validade de conteúdo expressa o grau em que os conteúdos incluídos no instrumento representam adequadamente o que se pretende medir. A validade de critério consiste na capacidade que um teste tem para estimar o resultado numa medida tomada por critério. A validade de construto tem como objetivo avaliar em que medida os resultados dos testes representam os construtos teóricos que pretendem medir. A validade de especialistas refere-se ao grau em que aparentemente um instrumento mensura a variável em questão, de acordo com especialistas no tema (FORTIN, 1999). Para esta pesquisa, realizou-se a validade de conteúdo e de especialista.

A validade do conteúdo de uma variável é normalmente definida pela literatura por meio da teoria ou de estudos anteriores (SAMPIERE; COLLADO; LUCIO, 2013). A validade do

conteúdo foi obtida por meio da RSL em que foram analisados 160 artigos que abordam o comportamento humano em segurança da informação dos quais 35 abordaram a Teoria de Motivação de Proteção. A partir da análise desses artigos, muitas variáveis foram identificadas, entretanto, considerou-se as que se adequassem melhor ao ambiente das universidades federais. Assim, as variáveis foram definidas a partir das pesquisas de Hooper e Blunt (2020); Hina, Selman e Lowry (2019); Pattinson *et al* (2019); Jansen e Van Schaik (2017, 2018); Rajab e Eydgahi, (2019).

A validade dos especialistas ocorreu por meio da apreciação do questionário por dois especialistas em segurança da informação da UFPB. Segundo Fortin (1999) como componente da validação é fundamental a garantia, por parte de especialistas, de que o instrumento utilizado represente o que é pretendido avaliar.

3.5 PROCEDIMENTOS DE COLETA DE DADOS

Após submissão da pesquisa ao Comitê de Ética do Centro de Ciências da Saúde (Anexo A) da UFPB, os procedimentos de coleta foram iniciados com as entrevistas com os dois especialistas em segurança da informação da UFPB. O primeiro passo foi enviar o questionário com antecedência para apreciação dos especialistas. Na semana seguinte, as entrevistas aconteceram pela ferramenta *Google Meet*, nos dias 16 e 18 de agosto de 2021. As entrevistas possibilitaram uma melhor compreensão do problema, e principalmente, aprimorou o questionário *on-line* utilizado para a coleta de dados junto aos servidores das universidades federais.

Em seguida, aplicou-se o pré-teste com 15 servidores, representados por cinco docentes e 10 técnicos-administrativos, sendo 10 da UFPB, três da UFRPE, um da UNIRIO, um da UFCE. O questionário foi construído na ferramenta *Google Forms* e enviado *on-line*, no período de 05 a 15 de setembro de 2021, em que se obteve as repostas dos 15 convites enviados. A pesquisa foi acompanhada por uma página de rosto transmitindo o objetivo básico da pesquisa, o termo de consentimento, garantindo aos servidores seus direitos à privacidade, e uma declaração de participação voluntária. O pré-teste é a aplicação prévia do questionário a um grupo com as mesmas características da amostra da pesquisa, permitindo corrigir possíveis falhas das questões formuladas e acrescentar novas questões ao instrumento (RICHARDSON, 2009).

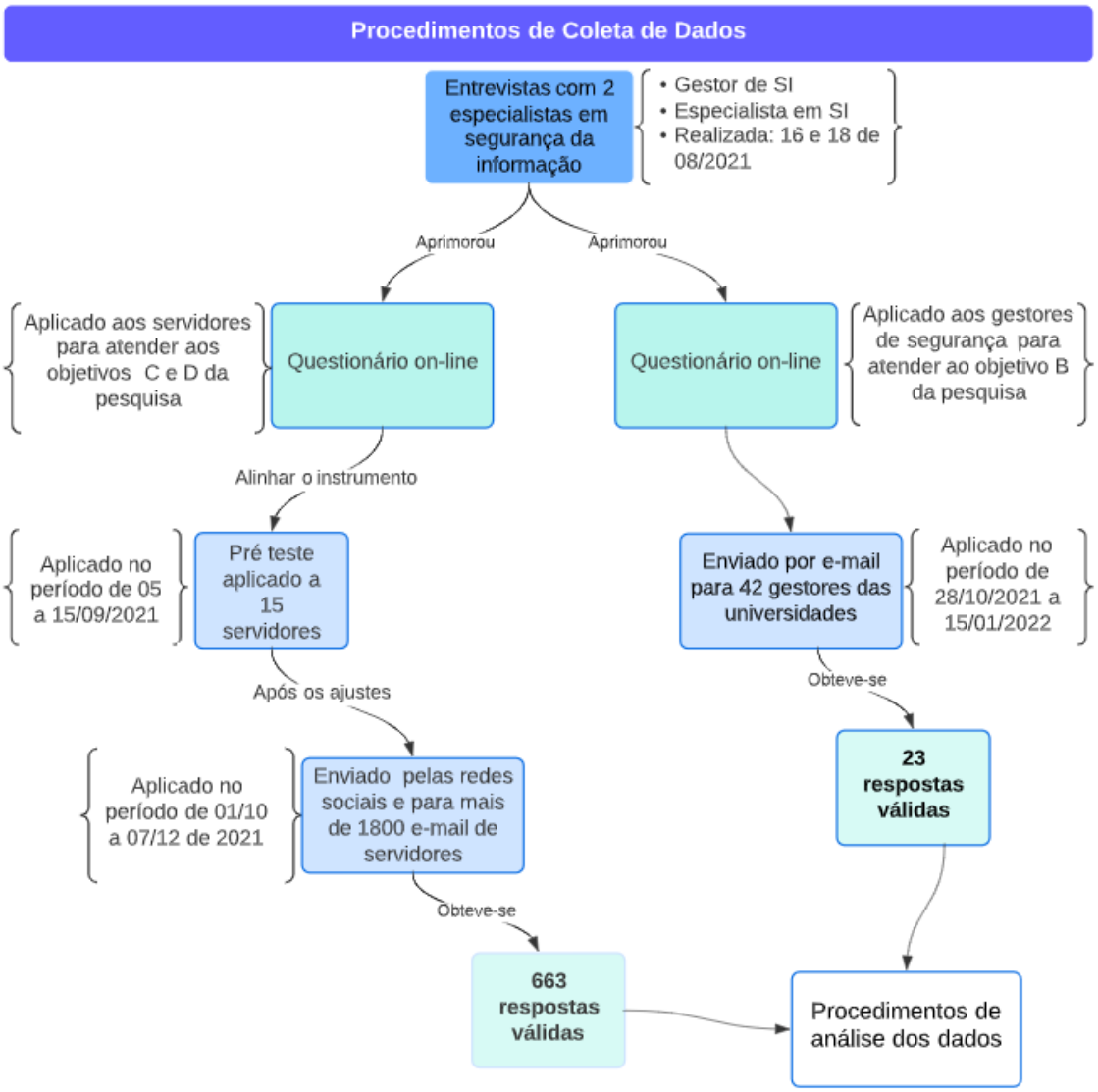
De posse das respostas, percebeu-se que o questionário necessitava ser reduzido e a redação ajustada para torná-lo mais claro e objetivo. Após a reformulação da redação e da

exclusão de questões redundantes, iniciou-se o procedimento de coleta. A coleta com os servidores ocorreu no período de 01 de outubro a 07 de dezembro de 2021.

O convite para participar da pesquisa e o referido *link* foram enviados majoritariamente por e-mail, mas se fez uso também de grupos de *Whatsapp* e de comunidades do *Facebook* formadas por servidores de universidades federais. É importante destacar que no convite havia uma instrução em vermelho orientando a quem a pesquisa era destinada. Serviram como fonte para recuperação dos e-mails a Plataforma Sucupira, disponibilizando os endereços eletrônicos dos programas de pós-graduação e os *sites* oficiais das universidades, onde estão disponibilizados *e-mails* das equipes e, frequentemente, os *e-mails* institucionais dos servidores. Foram recuperados manualmente aproximadamente 1.800 endereços de *e-mails*. Os convites foram enviados pelo *e-mail* institucional da pesquisadora e obteve-se 668 respostas, das quais cinco delas foram descartadas por apresentarem equívocos, como o respondente ser vinculado a um instituto federal, e não a uma universidade. A coleta desse questionário foi encerrada após termos atingido 663 respostas válidas, número superior à amostra mínima necessária de 385.

De forma paralela, iniciou-se em 28 de outubro de 2021 a pesquisa com os gestores de segurança da informação das universidades em que foram recuperados manualmente 42 endereços de *e-mails* de gestores dos *sites* oficiais das universidades. Este questionário também foi construído no *Google forms*, e os convites com o *link* da pesquisa foram enviados por *e-mails*. A pesquisa foi acompanhada por uma página de rosto transmitindo o objetivo básico da pesquisa, o termo de consentimento, garantindo aos gestores seus direitos à privacidade, e uma declaração de participação voluntária. A coleta com os gestores finalizou em 15 de janeiro de 2022 e obteve um total de 23 respostas. A Figura 21 ilustra os procedimentos de coleta de dados utilizados na pesquisa.

Figura 21 - Procedimento de coleta dos dados da pesquisa



Fonte: Elaborado pela autora (2023).

Uma vez que a coleta foi realizada, os dados foram exportados para uma planilha *Excel* para serem tratados. Nesse caso, fez-se necessário padronizar as respostas abertas relacionadas à variável tempo de serviço, uma vez que essa variável obteve resposta em ano e em meses. Posteriormente, todos os dados foram codificados e, em seguida, exportados para um programa estatístico para serem analisados.

3.6 PROCEDIMENTOS DE ANÁLISE DOS DADOS

Iniciamos os procedimentos de análise dos dados com escolha do programa estatístico *Statistical Package for the Social Sciences (SPSS), versão 25.* Em seguida, exportamos para o SPSS a planilha do Microsoft *Excel*, anteriormente codificada, com as respostas do questionário aplicado aos servidores das universidades. O SPSS também foi utilizado para calcular a confiabilidade do instrumento de coleta dos dados. Em seguida, identificamos como os dados estavam distribuídos, para finalmente realizar as análises estatísticas descritiva e inferencial.

3.6.1 Confiabilidade do instrumento de coleta

A confiabilidade do instrumento está relacionada ao grau em que ele produz resultados consistentes e coerentes. Os procedimentos mais utilizados para determinar a confiabilidade a partir de um coeficiente são: a) medida de estabilidade (confiabilidade por teste-reteste) - um mesmo instrumento é aplicado duas ou mais vezes para o mesmo grupo de pessoas após determinado período; b) método de formas alternativa ou paralelas - não se administra mais de uma vez o mesmo instrumento de medição, mas duas ou mais versões equivalentes; c) método de metades divididas (*split-halves*) - necessita de apenas uma aplicação da mensuração, no entanto, o conjunto total de assertivas é dividido em duas metades equivalentes e compara-se as duas metades dos resultados; e d) medida de consistência interna - exige apenas uma aplicação do instrumento de mensuração, sendo medida pelo coeficiente do alfa de Cronbach e pelos coeficientes KR-20 e KR-21 (PESTANA; GAGEIRO, 2008).

Escolher o coeficiente para avaliar a confiabilidade do questionário depende tanto da quantidade de vezes que o instrumento foi aplicado como da escala de mensuração utilizada para medir as variáveis. Para esta pesquisa, o procedimento mais adequado para medir a confiabilidade do questionário é a medida de consistência interna, a partir do coeficiente de alfa de Cronbach, uma vez que os coeficientes KR-20 e KR-21 são utilizados para medir itens dicotômicos (PESTANA; GAGEIRO, 2008).

A consistência interna de um questionário é a extensão em que os itens que o compõem medem o mesmo conceito ou variáveis, avaliando as correlações entre os itens. Por exemplo, se dez itens foram projetados para medir a mesma variável, o respondente deveria ter coerência nas respostas (PESTANA; GAGEIRO, 2008).

Para Fortin (1999), o alfa de Cronbach é o coeficiente mais utilizado para estimar a consistência interna de um grupo de variáveis de um questionário. Esse procedimento é

considerado um padrão de confiabilidade dos instrumentos de pesquisas (RAJAB; EYDGAHI, 2019).

O coeficiente de consistência interna a partir do alfa de Cronbach possibilitou a identificação de itens que apresentaram baixos coeficientes de correlação e, portanto, foram excluídos para manter a alta confiabilidade do instrumento e evitar possíveis erros de mensuração. O erro resulta no grau em que os itens não medem a mesma coisa (FÁVERO; BELFIORE, 2017).

3.6.2 Distribuição dos dados

Para identificar se a distribuição dos dados se apresentava de forma normal, ou não, são utilizados testes de normalidade. Para amostras com *(n* > 30) [18] o teste de normalidade utilizado é o *Kolmogorov-Smirnov* (K-S). Esse teste possui o objetivo de testar se os valores amostrais são oriundos de uma população com suposta distribuição esperada, neste caso a distribuição normal. O K-S assume as seguintes hipóteses: Hipótese nula (H0) - a amostra provém de uma população com distribuição normal; e Hipótese (H1): a amostra não provém de uma população com distribuição normal. O SPSS calcula o K-S a partir do *P-value* que corresponde ao menor nível de significância observado que levaria à rejeição da hipótese nula P < 0,05 (FÁVERO; BELFIORE, 2017). Assim, se o P > 0,05 não rejeitamos e hipótese nula (dados com distribuição normal); se P < 0,05 rejeitamos a hipótese nula (dados com distribuição não normal).

Nos casos em que os dados da pesquisa possuem uma distribuição não normal, deve-se utilizar os testes estatísticos não paramétricos; e para distribuição normal dos dados, usa-se os testes estatísticos paramétricos (PESTANA; GAGEIRO, 2008).

Os testes não paramétricos podem formular hipóteses sobre características qualitativas da população, podendo então ser aplicados para dados de natureza qualitativa, em escala nominal ou ordinal. Nos testes não paramétricos não se pode realizar nenhuma operação aritmética, o que torna os dados bastante limitados em seu uso na estimação de coeficientes do modelo (HAIR *et al.*, 2009). Como as suposições em relação à distribuição dos dados são em menor número e mais fracas do que as provas paramétricas, são também conhecidos como testes livres de distribuição**.** Possuem menos pressupostos, são mais simples e de fácil aplicação, porém, menos robustos quando comparados aos testes paramétricos (FÁVERO; BELFIORE, 2017).

18(*n)* corresponde ao número de participantes da amostra. Nesta pesquisa o valor de *n* é de 663.

Os testes paramétricos são aplicados para dados de natureza quantitativa, formulam hipóteses sobre os parâmetros da população, como a média populacional, o desvio-padrão populacional, a variância populacional e a proporção populacional. São utilizados quando indivíduos diferem em quantia ou grau em relação a um atributo em particular. Variáveis metricamente medidas refletem quantidade ou grau relativo e são apropriadas para atributos envolvendo quantia ou magnitude, como o nível de satisfação, compromisso com um emprego ou idade. As duas escalas de medida métrica são as escalas intervalares e de razão (HAIR *et al.*, 2009).

A partir dessa constatação, foi possível estabelecer como realizar a análise estatística descritiva e definir, a partir da estatística inferencial, quais os testes de hipóteses seriam utilizados.

3.6.3 Estatística descritiva univariada

A estatística descritiva descreve e sintetiza as características principais observadas em um conjunto de dados por meio de tabelas, gráficos e medidas, permitindo ao pesquisador melhor compreensão do comportamento dos dados. A análise é baseada no conjunto de dados, sem tirar quaisquer conclusões ou inferências acerca da população. A estatística descritiva pode apresentar uma única variável (estatística descritiva univariada), duas variáveis (estatística descritiva bivariada) ou mais de duas variáveis (estatística descritiva multivariada) (FÁVERO; BELFIORE, 2017). Neste estudo, utilizamos a estatística descritiva univariada.

A estatística descritiva univariada contempla os seguintes tópicos: a) a frequência de ocorrência de um conjunto de observações por meio de tabelas de distribuições de frequências; b) a representação da distribuição de uma variável por meio de gráficos; e c) medidas representativas de uma série de dados, como medidas de posição (média, mediana, moda, quartis, decis e percentis), medidas de dispersão (amplitude, desvio-médio, variância, desvio-padrão, erro-padrão e coeficiente de variação) e medidas de forma (FÁVERO; BELFIORE, 2017).

O tipo de variável é essencial no cálculo de estatísticas descritivas e na representação dos resultados (PESTANA; GAGEIRO, 2008). Nesta pesquisa, as variáveis definidas como qualitativas são: universidade, sexo, categoria profissional, grau de escolaridade, vulnerabilidade percebida, gravidade percebida das ameaças, gravidade percebida das sanções, eficácia de resposta, autoeficácia, custo de resposta, normas injuntivas, normas descritivas, intenção de comportamento de prevenção, fortalecimento da política de segurança da

informação, capacitação e conscientização. Apenas as variáveis idade e tempo de serviço são classificadas como quantitativas.

As variáveis qualitativas são apresentadas pela distribuição de frequência, que consiste em uma técnica estatística utilizada para apresentar uma coleção de dados classificados e agrupados em variáveis, de modo a destacar a frequência existente em cada variável (FÁVERO; BELFIORE, 2017).

As variáveis quantitativas são apresentadas pelas medidas de posição, medidas de dispersão e medidas de forma. Essas medidas possuem como objetivo principal a representação do comportamento da variável em estudo por meio de seus valores, posição, suas dispersões ou formas de distribuição dos seus valores em torno da média (FÁVERO; BELFIORE, 2017).

As únicas exceções das medidas de posição que fazem sentido ser utilizadas em variável qualitativas são à moda (em variáveis qualitativas nominas ou ordinais) e a mediana (qualitativa ordinal). À moda fornece o valor mais frequente de determinada variável. Enquanto a mediana, é uma medida de localização do centro da distribuição de um conjunto de dados ordenados de forma crescente. Seu valor separa a série em duas partes iguais, de modo que 50% dos elementos são menores ou iguais à mediana e os outros 50% são maiores ou iguais à mediana. podendo assim também ser calculada para variáveis qualitativas (PESTANA; GAGEIRO, 2008).

Diante do exposto, para as variáveis desta pesquisa classificadas como qualitativa nominal e qualitativa ordinal, a análise estatística descritiva apresentada contém tabelas de distribuições de frequência e as medidas de posição à moda e a mediana. As variáveis quantitativas (idade e tempo de serviço) foram apresentadas a partir da medida de posição, média, e a medida de dispersão, desvio padrão. A média consiste na soma de todos os valores dividido pelo número de dados do conjunto. O desvio padrão é uma medida que expressa o grau de dispersão de um conjunto de dados em relação a sua média. Quanto mais próximo de zero for o valor do desvio padrão, mais homogêneo e constante é o conjunto de dados analisados (FÁVERO; BELFIORE, 2017).

3.6.4 Estatística Inferencial

A análise estatística inferencial, utilizada para estimar parâmetros e testar hipóteses a partir da distribuição amostral, também foi utilizada. A análise de correlação tem como objetivo medir a intensidade ou o grau de associação entre duas variáveis, sob um contexto de influência

mútua", ou seja, é uma medida de influência bilateral. A variável x influencia y na mesma intensidade que y influencia x (PESTANA; GAGEIRO, 2008).

Esse teste supõe a não associação entre as variáveis analisadas, ou seja, partem da hipótese nula de que não há associação entre as variáveis estudadas. No SPSS o *P-value* representa a probabilidade associada ao valor observado da amostra, indicando o menor nível de significância que levaria à rejeição da hipótese nula. Em outras palavras, *P-value* representa um índice decrescente de confiabilidade de um resultado; quanto mais baixo seu valor, menos se pode acreditar na hipótese nula. Assim, para um nível de confiança de 95%, se *P-value* < 0,05, a hipótese nula é rejeitada e podemos afirmar que há associação entre as variáveis. Por outro lado, se *P-value* > 0,05, conclui-se pela independência das variáveis (SAMPIERE; COLLADO; LUCIO, 2013).

Segundo Callegari-Jacques (2003, p. 90), o coeficiente de correlação pode ser avaliado qualitativamente da seguinte forma: se 0,00 < correlação < 0,30, existe fraca correlação; se 0,30 ≤ correlação < 0,60, existe moderada correlação; se 0,60 ≤ correlação < 0,90, existe forte correlação; e se 0,90 ≤ correlação < 1,00, existe correlação muito forte.

Diante do exposto, para testar as hipóteses da pesquisa utilizamos o coeficiente de Spearman, também denominado de ρ (rho) de Spearmanque que é uma medida de associação entre duas variáveis qualitativas ordinais, que varia entre -1 (associação negativa perfeita) e 1 (associação positiva perfeita), sendo o zero indicativo de não existência de associação, ou seja,. a proximidade do zero indica o poder da relação. O sinal de positivo ou negativo indica a direção desta relação, se positiva, o aumento em uma variável implica no aumento na outra variável. Para 95% de confiança, *P-value* < 0,05 indica que há associação entre as variáveis (FÁVERO; BELFIORE, 2017).

A partir da definição dos procedimentos de análise, a próxima seção apresenta a análise dos dados.

4 APRESENTAÇÃO E ANÁLISE DOS DADOS

Nesta seção serão apresentados e analisados os dados coletados nesta pesquisa em concordância com a teoria adotada. Iniciamos com o teste de confiabilidade do questionário, seguido da análise de distribuição dos dados, análise estatística descritiva e finalizamos com a análise estatística inferencial, de modo a alcançar os objetivos da pesquisa.

4.1 VERIFICAÇÃO DA CONFIABILIDADE DO QUESTIONÁRIO

O alfa de Cronbach utiliza uma fórmula que gera o coeficiente de confiabilidade que pode oscilar entre zero e um, em que o coeficiente zero significa nenhuma confiabilidade e um representa o máximo de confiabilidade (FORTIN, 1999). Landis e Koch (1977) classificam o coeficiente alfa de Cronbach em: pequeno, de 0 a 0,20; razoável, de 0,21 a 0,40; moderado de 0,41 a 0,60; substancial, de 0,61 a 0,80 e muito bom, de 0.81 a 1,0.

O coeficiente do alfa de Cronbach do questionário total desta pesquisa apresentou o valor de 0,9, considerado quase perfeito, de acordo com a classificação de Landis e Koch (1977). No entanto, segundo Tavakol e Dennick (2011) quando o questionário utiliza mais de uma variável ou conceitos, o cálculo do valor do alfa de Cronbach para todas as respostas indistintamente pode inflar o resultado e camuflar a confiabilidade do instrumento de mensuração. O alfa deve ser calculado para cada uma das variáveis e não para o instrumento de mensuração ou escala inteira.

Assim, foi necessário estimar o coeficiente de correlação de cada variável, bem como calcular a correlação do item-escala da variável. Essa última representa a intensidade de cada item com a escala total da variável. A intensidade da correlação entre os itens de um questionário pode ser verificada eliminando-se um item da escala de medição. Caso o coeficiente alfa aumente, pode-se assumir que esse item não é altamente correlacionado com os demais itens da variável. Por outro lado, caso o coeficiente diminua, assume-se que este item é altamente correlacionado com os demais itens da escala. Os itens que apresentam baixos coeficientes de correlação com a escala da variável podem ser excluídos (PESTANA; GAGEIRO, 2008). O *software* SPSS, utilizado nesta pesquisa para calcular o coeficiente do alfa de Cronbach, também nos possibilitou calcular a relação entre os itens de cada variável. A partir desses cálculos, cinco itens apresentaram baixos coeficientes de correlação. Assim, para aumentar a consistência interna e evitar problemas nas análises, esses itens foram retirados do conjunto de dados.

O Quadro 13, apresenta as 12 variáveis mensuradas nesta pesquisa, a quantidade de itens utilizados para medir cada variável, os sete itens que foram excluídos e o valor do coeficiente do alfa de Cronbach. Os itens relacionados ao perfil do respondente não foram calculados por apresentar escalas de mensuração variadas.

Quadro 13 - Relação de variáveis e itens excluídos com Alfa de Cronbach

Variáveis	Número de itens	Itens excluídos	Alfa de Cronbach
Vulnerabilidade Percebida	4	9 - Em termos de riscos à segurança da informação na minha instituição, a vulnerabilidade do meu computador e dos dados é muito alta.	0,72
Gravidade Percebida das Ameaças	3	12 - Eu entendo que ter alguém violando ou danificando os recursos de informação no trabalho é muito perigoso.	0,82
Gravidade Percebida das Sanções	2	-	0,65
Eficácia de Resposta	4	19 - Medidas de segurança em minha instituição evitam que *hackers* tenham acesso as informações pessoais ou educacionais confidenciais.	0,87
Autoeficácia	4	23 - Posso ativar as medidas de segurança em meu computador institucional, mas apenas quando sou instruído.	0,85
Custo de Resposta	4	27 - O custo de implementação de medidas excede os benefícios de não as aplicar.	0,71
Normas Descritivas	3	-	0,85
Normas Injuntivas	3	-	0,87
Intenção de Comportamento de prevenção	4	-	0,85
Fortalecimento da PSI	4	-	0,89
Capacitação	3	-	0,95
Conscientização	15	36 - Se eu perceber que meu colega descumpre as regras de segurança, eu não vou denunciá-lo. 42 - Eu clico em *links* de e-mail enviado por pessoas desconhecidas, se eu entender que a informação seja interessante.	0,74

Fonte: Elaborado pela autora (2023).

A partir do cálculo do coeficiente do alfa de Cronbach, verifica-se que as variáveis ‘gravidade percebida das ameaças’, ‘eficácia de resposta’, ‘autoeficácia’, ‘normas descritivas’, ‘normas injuntivas’, ‘intenção de comportamento de prevenção’, ‘fortalecimento da política de segurança da informação’ e ‘capacitação’, ou seja, oito das 13 variáveis mensuradas

apresentaram o alfa acima de 0,81, que são considerados de níveis altos de correlação. As demais variáveis ‘vulnerabilidade percebida’, ‘gravidade percebida das sanções’ e ‘custo de resposta’ e ‘conscientização’ apresentaram níveis de correlação considerados substancial, alfa entre 0,61 e 0,80.

A quantidade de itens utilizados para mensurar uma variável pode influenciar no coeficiente do alfa de Cronbach. Quanto mais itens houver, maior será a confiabilidade (PESTANA; GAGEIRO, 2008). Entretanto, as variáveis mensuradas nessa pesquisa apresentaram, em sua maioria, apenas três ou quatro itens de mensuração, e obtiveram os valores do alfa de até 0,95, o que demonstra alta correlação entre os itens, pouca variação específica do item e, consequentemente, uma consistência interna superior ao substancial.

Após o cálculo da confiabilidade do questionário, a partir do coeficiente do alfa de Cronbach, a próxima subseção apresentará a distribuição dos dados.

4.2 DISTRIBUIÇÃO DOS DADOS COLETADOS NA PESQUISA

Nesta pesquisa, a maioria das variáveis foram classificadas como qualitativas e os dados foram coletados em escalas nominais e ordinais. Portanto, nesses casos, não houve necessidade de realizar testes de normalidade para identificar se a distribuição dos dados apresentava-se de forma normal ou não, uma vez que variáveis qualitativas nominal e ordinal não apresentam distribuição normal (FORTIN, 1999).

Para as variáveis classificadas como quantitativas, neste caso, ‘idade’ e ‘tempo de serviço’, tornou-se necessário realizar o teste de normalidade para identificar como os dados dessas variáveis estão distribuídos. Como a amostra desta pesquisa possui *(n* > 30), realizou-se, a partir do SPSS, o teste de normalidade *Kolmogorov-Smirnov*, apresentado na Tabela 1. De acordo com esse teste são consideradas duas hipóteses para cada variável testada. Para a variável ‘idade’, são consideradas as seguintes hipóteses: H0 – A variável ‘idade’ provém de uma população com distribuição normal; e H1 – A variável ‘idade’ provém de uma população com distribuição não normal. De modo equivalente, para a variável ‘tempo de serviço’ são avaliadas as seguintes hipóteses: H0 – A variável ‘tempo de serviço’ provém de uma população com distribuição normal; e H1 – a variável ‘tempo de serviço’ provém de uma população com distribuição não normal.

Tabela 1 - Teste de normalidade *Kolmogorov-Smirnov*

Variáveis	*N*	P- *value*
Idade	663	<, 001
Tempo de serviço	663	<, 001

Fonte: Elaborado pela autora (2023).

Como o P-*value* das duas variáveis apresentaram valores P < 0,05, rejeitamos as seguintes hipóteses nulas: H0 – A variável 'idade' provém de uma população com distribuição normal; e H0 – A variável 'tempo de serviço' provém de uma população com distribuição normal, o que nos permite concluir, ao nível de confiança de 95%, que a amostra das variáveis 'idade' e 'tempo de serviço' foi obtida de uma população com distribuição não normal.

Portanto, devemos concluir que tanto as variáveis qualitativas como as quantitativas desta pesquisa possuem uma distribuição não normal, o que nos direcionou a utilizar os testes estatísticos não paramétricos.

4.3 ANÁLISE DESCRITIVA UNIVARIADA DOS DADOS DA PESQUISA

Esta subseção analisou, por meio de estatística descritiva, os 52 itens (59 itens menos os 7 excluídos a partir do teste de confiabilidade) auferidos nas 663 respostas válidas dos servidores das universidades pesquisadas. Esses itens se relacionam a todos os três construtos (perfil do respondente, avaliação da ameaça e avaliação de enfrentamento). Esses constructos foram compostos das seguintes variáveis: 'idade', 'categoria profissional', 'tempo de serviço', 'escolaridade', 'região', 'vulnerabilidade percebida', 'gravidade percebida das ameaças', 'gravidade percebida das sanções', 'eficácia de resposta', 'autoeficácia', 'custo de resposta', 'normas injuntivas', 'normas descritivas', 'intenção de comportamento de prevenção', 'fortalecimento da política de segurança da informação', 'capacitação e a variável conscientização' (medida pelas variáveis relato de incidentes; informação e atualização; uso de e-mail; e gerenciamento de senhas), totalizando 17 variáveis. As variáveis foram apresentadas por meio da estatística descritiva univariada, com exceção das variáveis pertencentes ao constructo perfil do respondente, que foram apresentados de forma conjunta.

Conforme mencionado anteriormente, para as variáveis que utilizaram a escala de *Likert* (qualitativas ordinais), definiu-se que quanto maior a pontuação na escala, melhor os resultados, sendo o ponto neutro (nem concordo nem discordo) o divisor entre a parte positiva e a negativa da escala. A pontuação da escala varia entre 1- Discordo totalmente, 2- Discordo parcialmente, 3 – Nem concordo nem discordo, 4 – Concordo parcialmente e 5 - Concordo totalmente.

A medida estatística utilizada para apresentar as variáveis qualitativas nominais foi a distribuição de frequência. Para descrever os resultados das variáveis quantitativas utilizamos a média como medida de posição e o desvio padrão como medida de dispersão e, para as variáveis qualitativas ordinais, utilizamos a distribuição de frequência e as medidas de posição moda e mediana.

4.3.1 Análise descritiva do constructo perfil dos servidores

Por meio dos dados que compõem o perfil dos servidores (idade, tempo de serviço, gênero, categoria profissional, grau de escolaridade e região), observou-se que os servidores que responderam à pesquisa possuíam uma média de idade de 43,93 anos (DP = 10,33). O participante mais jovem da amostra possuía 23 anos, enquanto o mais velho possuía 74 anos. O tempo médio de serviço dos respondentes foi de 12,90 anos (DP = 10,12). O sexo feminino representou a maioria dos respondentes (*f* = 369; 56%), sendo (*f* = 291; 44%) pertencente ao sexo masculino. Quanto a categoria profissional, a maioria foi composta por servidores técnico-administrativos (*f* = 436; 66%); a categoria docente representou (*f* = 217; 44%). O grau de escolaridade de mestrado (*f* = 212; 32%) foi o mais representativo, seguido de especialização (*f* = 176; 27%) e doutorado (*f* = 170; 26%). A pesquisa envolveu servidores de universidades federais de todas as regiões, predominando a região nordeste do país (*f* = 247; 37%), Tabelas 2 e 3.

Tabela 2 - Distribuição de frequência do perfil do respondente

Variáveis	Respostas	Frequência (f)	Porcentagem (%)
Sexo	Masculino	291	44%
	Feminino	369	56%
	Não binário	3	< 1%
	Total	663	100%
Categoria Profissional	Docente	227	34%
	Técnico-administrativo	436	66%
	Total	663	100%
Grau de escolaridade	Ensino médio	5	> 1%
	Graduação incompleta	2	< 1%
	Graduação	42	6%
	Especialização	176	27%
	Mestrado	212	32%
	Doutorado	170	26%

Variáveis	Respostas	Frequência (f)	Porcentagem (%)
	Pós-doutorado	56	8%
	Total	663	100%
Região	Sul	137	21%
	Sudeste	94	14%
	Centro Oeste	75	11%
	Norte	115	17%
	Nordeste	242	37%
	Total	663	100%

Fonte: Elaborado pela autora (2023).

Tabela 3 – Resumo das variáveis idade e tempo de serviço

Variáveis	*N*	Mínimo	Máximo	Média	Desvio padrão (DP)
Idade	663	23	74	43,93	10,33
Tempo de serviço	663	0,17	52	12,90	10,12

Fonte: Elaborado pela autora (2023).

4.3.2 Análise descritiva do constructo avaliação de ameaça

O constructo avaliação de ameaça avaliou o nível de perigo vinculado a um evento de segurança. Nesta pesquisa, esse constructo foi composto das variáveis 'vulnerabilidade percebida', 'gravidade percebida das ameaças' e 'gravidade percebida das sanções'.

A Tabela 4 apresenta os resultados dos três itens (7, 8 e 10) utilizados para medir a variável 'vulnerabilidade percebida' - avaliação da probabilidade de ocorrência de um incidente de segurança da informação. Os resultados evidenciados pelos três itens apresentaram maior frequência de respostas do lado positivo da escala, ou seja, os pontos da escala que são posteriores ao ponto neutro, neste caso, representado pelo concordo totalmente com a afirmativa 386 (58,2%), 395 (59,6%) e 256 (38,6%) respectivamente, o que indica que os servidores percebem a probabilidade de um incidente de segurança, caso não haja o cumprimento das políticas de segurança da informação da instituição. Os valores das medidas moda e mediana de (5;5;5) e (5;5;4) respectivamente, confirmam essa tendência.

Tabela 4 - Estatística descritiva da variável 'Vulnerabilidade Percebida'

Itens	Escala	Frequência	Mediana	Moda
7 Eu sei que minha instituição pode estar vulnerável a violações de segurança se eu não aderir às suas Políticas de Segurança da	1 Discordo totalmente	9 (1,4%)	5	5
	2 Discordo parcialmente	24 (3,6%)		
	3 Neutro	71 (10,7%		

Itens	Escala	Frequência	Mediana	Moda
Informação	4 Concordo parcialmente	173 (26,1%)		
	5 Concordo totalmente	386 (58,2%)		
8 Posso ser vítima de um ataque malicioso se não cumprir as Políticas de Segurança da Informação da minha instituição	1 Discordo totalmente	12 (1,8%)	5	5
	2 Discordo parcialmente	12 (1,8%)		
	3 Neutro	61 (9,2%)		
	4 Concordo parcialmente	183 (27,6%)		
	5 Concordo totalmente	395 (59,6%)		
10 Informações importantes ou recursos de computação podem ser danificados devido à minha negligência em relação às Políticas de Segurança da Informação	1 Discordo totalmente	57 (8,6%)	4	5
	2 Discordo parcialmente	64 (9,7%)		
	3 Neutro	103 (15,5%)		
	4 Concordo parcialmente	183 (27,6%)		
	5 Concordo totalmente	256 (38,6%)		

Fonte: Elaborado pela autora (2023).

Os itens 11 e 13 do questionário foram utilizados para medir a variável ‘gravidade percebida das ameaças’ - a avaliação do impacto das consequências resultantes de um incidente de segurança da informação -, Tabela 5. Os resultados direcionaram ao lado positivo da escala, em que 598, (90,2%) e 91 (13,7%) dos servidores concordaram totalmente com as afirmativas, enquanto 56, (8,4%) e 251 (37,9%) concordaram parcialmente, indicando que a maioria dos servidores percebem a gravidade das ameaças à segurança da informação.

Tabela 5 - Estatística descritiva da variável ‘Gravidade Percebida da Ameaças’

Itens	Escala	Frequência	Mediana	Moda
11 Na minha opinião, proteger as informações da minha instituição é importante.	1 Discordo totalmente	1 (0,2%)	5	5
	2 Discordo parcialmente	2 (0,3%)		
	3 Neutro	6 (0,9%)		
	4 Concordo parcialmente	56 (8,4%)		
	5 Concordo totalmente	598, (90,2%)		
13 Para mim, tomar precauções de segurança da informação é fácil.	1 Discordo totalmente	41 (6,2%)	4	4
	2 Discordo parcialmente	127 (19,1%)		
	3 Neutro	153 (23,1%)		
	4 Concordo parcialmente	251 (37,9%)		
	5 Concordo totalmente	91 (13,7%)		

Fonte: Elaborado pela autora (2023).

A Tabela 6 apresenta os resultados dos itens (14 e 15) do questionário que foram utilizados para medir a variável ‘gravidade percebida das ameaças das sanções’ - avaliação do

impacto das sanções determinadas pelo incidente de segurança. De acordo com os servidores pesquisados, o ponto neutro, nem concordo nem discordo das afirmativas, apresentaram maior frequência de respostas nos dois itens, 288 (43,4%) e 230 (34,7%), respectivamente, o que indica que os servidores desconhecem a existência de medidas corretivas ou punitivas relacionadas a incidentes de segurança da informação. Esse resultado corrobora a pesquisa de Hina, Selvam, Lowry(2019) desenvolvida em instituições de ensino superior da Malásia, em que os autores identificaram que os funcionários dessas universidades não compreendiam suas responsabilidades na proteção das informações institucionais e pessoais, a fim de se protegerem de possíveis violações de segurança. Entretanto, os resultados das pesquisas de Chen *et al.* (2020b) em empresas e universidades chinesas identificaram que a certeza da gravidade e celeridade da sanção têm impactos positivos no comportamento de conformidade com as políticas de segurança da informação.

Tabela 6 - Estatística descritiva da variável "Gravidade Percebida das Sanções"

Itens	Escala	Frequência	Mediana	Moda
14 Há ações corretivas e disciplinares estabelecidas para os casos de quebra de segurança da informação.	1 Discordo totalmente	55 (8,3%)	3	3
	2 Discordo parcialmente	93 (14,0%)		
	3 Neutro	288 (43,4%)		
	4 Concordo parcialmente	145 (21,9%)		
	5 Concordo totalmente	82 (12,4%)		
15 Se eu fosse pego violando as políticas de segurança da informação da minha instituição, seria severamente punido.	1 Discordo totalmente	53 (8,0%)	3	3
	2 Discordo parcialmente	89 (13,4%)		
	3 Neutro	230 (34,7%)		
	4 Concordo parcialmente	145 (21,9%)		
	5 Concordo totalmente	146 (22,0%)		

Fonte: Elaborado pela autora (2023).

A próxima subseção apresenta os resultados das variáveis que compuseram o constructo avaliação de enfrentamento.

4.3.3 Análise descritiva do constructo avaliação de enfrentamento

O constructo avaliação de enfrentamento avaliou uma determinada estratégia de enfrentamento para mitigar ou evitar um evento de segurança ameaçador. Esse constructo foi composto das seguintes variáveis: 'eficácia de resposta', 'autoeficácia', 'custo de resposta', 'normas injuntivas', 'normas descritivas', 'intenção de comportamento de prevenção', 'fortalecimento da política de segurança da informação', 'capacitação' e a variável

‘conscientização’ (medida pelas variáveis relato de incidentes; informação e atualização; uso de e-mail; e gerenciamento de senhas).

A Tabela 7 apresenta os resultados dos três itens (16,17 e 18) utilizados para medir a variável ‘eficácia de resposta’ - eficácia percebida de uma resposta de enfrentamento na redução de uma ameaça. Nos dois primeiros itens, os servidores sinalizaram, marcando com maior frequência o ponto neutro da escala, 239 (36,0%) e 234 (35,3%), que desconhecem a eficácia das medidas utilizadas para proteger as informações na instituição. Entretanto, no terceiro item, os resultados avançaram sutilmente para o positivo, uma vez que 205 (30,9%) dos servidores concordaram parcialmente e 239 (36,0%) concordaram totalmente que as medidas preventivas de que a instituição dispõe para lidar com conteúdos maliciosos são importantes. Esses resultados indicam que apesar dos servidores desconhecerem a eficácia dos esforços e das medidas institucionais utilizadas para proteger as informações, eles acreditam na importância dessas medidas.

Tabela 7 - Estatística descritiva da variável Eficácia de Resposta

Itens	Escala	Frequência	Mediana	Moda
16 Em minha instituição, os esforços para garantir a segurança das informações confidenciais são eficazes.	1 Discordo totalmente	38 (5,7%)	3	3
	2 Discordo parcialmente	94 (14,2%)		
	3 Neutro	239 (36,0%)		
	4 Concordo parcialmente	212 (32,0%)		
	5 Concordo totalmente	80 (12,1%)		
17 Em minha instituição, as medidas de segurança disponíveis para proteger as informações de trabalho contra violações de segurança são eficazes.	1 Discordo totalmente	41 (6,2%)	3	3
	2 Discordo parcialmente	101 (15,2%)		
	3 Neutro	234 (35,3%)		
	4 Concordo parcialmente	222 (33,5%)		
	5 Concordo totalmente	65 (9,8%)		
18 As medidas preventivas de que disponho na minha instituição para lidar com conteúdos maliciosos são importantes	1 Discordo totalmente	29 (4,4%)	4	4
	2 Discordo parcialmente	66 (10,0%)		
	3 Neutro	197 (29,7%)		
	4 Concordo parcialmente	205 (30,9%)		
	5 Concordo totalmente	166 (25,0%)		

Fonte: Elaborado pela autora (2023).

Os itens (20,21 e 22) mediram a variável ‘Autoeficácia’ - crença na capacidade de proteger informações e sistemas de informação contra divulgação não autorizada, modificação, perda, destruição e falta de disponibilidade. Os resultados indicaram que o ponto da escala com maior frequência de respostas nos dois primeiros itens foi concordo parcialmente, 205 (30,9%)

e 215 (32,4%) respectivamente, enquanto no terceiro item a maior frequência foi o ponto de discordo parcialmente, 185 (27,9%), sinalizando que os servidores não conhecem muito bem suas capacidades relacionadas à proteção das informações e dos sistemas de informação institucional. Isso fica mais evidente com a frequência significativa de resposta no ponto neutro da escala 154 (23,2%), 144 (21,7%) e 146 (22,0%), conforme Tabela 8. Os resultados da pesquisa de Alanazi *et al.* (2020), realizado nos hospitais da Arábia Saudita, indicaram a autoeficácia como uma das variáveis que mais influencia o comportamento preventivo entre os funcionários.

Tabela 8 - Estatística descritiva da variável Autoeficácia

Itens	Escala	Frequência	Mediana	Moda
20 Eu acredito que tenho as competências necessárias para me proteger de violações de segurança da informação.	1 Discordo totalmente	87 (13,1%)	3	4
	2 Discordo parcialmente	159 (24,0%)		
	3 Neutro	154 (23,2%)		
	4 Concordo parcialmente	205 (30,9%)		
	5 Concordo totalmente	58 (8,7%)		
21 Acredito que desenvolvi a capacidade de impedir que as pessoas obtenham minhas informações confidenciais.	1 Discordo totalmente	81 (12,2%)	3	4
	2 Discordo parcialmente	163 (24,6%)		
	3 Neutro	144 (21,7%)		
	4 Concordo parcialmente	215 (32,4%)		
	5 Concordo totalmente	60 (9,0%)		
22 Acredito que está sob meu controle me proteger de violações de segurança da informação.	1 Discordo totalmente	85 (12,8%)	3	2
	2 Discordo parcialmente	185 (27,9%)		
	3 Neutro	146 (22,0%)		
	4 Concordo parcialmente	177 (26,5%)		
	5 Concordo totalmente	70 (10,6%)		

Fonte: Elaborado pela autora (2023).

A tabela 9 apresenta os resultados dos itens (24,25 e 26) que mediram a variável ‘custo de resposta’ - quantidade de tempo, dinheiro ou esforço necessário para executar a resposta recomendada. Conforme mencionado anteriormente, para cada alternativa da escala foi definido um valor numérico que vai resultar numa pontuação para cada item, definindo-se que quanto maior a pontuação, melhor os resultados. Desse modo, para os itens que apresentaram sentido negativo, a escala foi invertida: 5 - Discordo totalmente, 4 - Discordo parcialmente, 3 - Nem concordo nem discordo, 2 - Concordo parcialmente e 1 - Concordo totalmente. Para medir a variável ‘custo de resposta’ foi necessário inverter a escala dos três itens que mediram a variável.

De acordo com os resultados, uma frequência significativa de servidores não conseguiu indicar o custo de uma resposta de segurança, marcando o ponto neutro como opção de resposta, 234 (35,3%), 182 (27,5%) e 120 (18,1%). Os dois primeiros itens (24 e 25) apresentaram uma maior frequência de respostas no sentido negativo da escala. Nesses itens, 162 (24,4%) e 186 (28,1%) dos servidores concordaram parcialmente com a afirmativa e 98 (14,8%) e 155 (23,4%) indicaram que concordaram totalmente com a afirmativa. No item 26 que se referiu a afirmativa de que cumprir as regras de segurança exigiria iniciar um novo hábito, 171 (25,8%) discordavam totalmente e 224 (33,8%) dos servidores sinalizaram que discordaram parcialmente da afirmativa. Apesar da dificuldade na identificação do custo de resposta recomendada, essa variável influencia tanto o mal adaptativo, como o comportamento preventivo (MCGILL; THOMPSON, 2021).

Tabela 9 - Estatística descritiva da variável 'Custo de Resposta'

Itens	Escala	Frequência	Mediana	Moda
24 Seguir as regras de segurança é demorado.	5 Discordo totalmente	32 (4,8%)	3	3
	4 Discordo parcialmente	137 (20,7%)		
	3 Neutro	234 (35,3%)		
	2 Concordo parcialmente	162 (24,4%)		
	1 Concordo totalmente	98 (14,8%)		
5 Cumprir as regras de segurança requer muito esforço mental.	5 Discordo totalmente	33 (5,0%)	2	2
	4 Discordo parcialmente	107 (16,1%)		
	3 Neutro	182 (27,5%)		
	2 Concordo parcialmente	186 (28,1%)		
	1 Concordo totalmente	155 (23,4%)		
26 Cumprir as regras de segurança exigiria iniciar um novo hábito.	5 Discordo totalmente	171 (25,8%)	4	4
	4 Discordo parcialmente	224 (33,8%)		
	3 Neutro	120 (18,1%)		
	2 Concordo parcialmente	88 (10,3%)		
	1 Concordo totalmente	60 (9,0%)		

Fonte: Elaborado pela autora (2023).

A Tabela 10 apresenta os resultados dos itens (28, 29 e 30), utilizados para medir a variável 'normas injuntivas' - percepções sobre o que deve ou não deve ser feito. Nos três itens, representaram o maior número os servidores que marcaram o ponto neutro da escala, 297 (48,8%), 209 (31,5%) e 195 (29,4%). Quando analisamos as respostas com relação ao ponto neutro, percebemos que os servidores possuem uma maior inclinação ao lado positivo da escala,

representado pelo concordo parcialmente 144 (21,7%), 139 (21,0%) e 154 (23,2%); e concordo totalmente 134 (20,2%), 178 (26,8%) e 177 (26,7%), respectivamente.

Tabela 10 - Estatística descritiva da variável Normas Injuntivas

Itens	Escala	Frequência	Mediana	Moda
28 Meus colegas acham que devo seguir as políticas de segurança da informação da minha instituição.	1 Discordo totalmente	41 (6,2%)	3	3
	2 Discordo parcialmente	47 (7,1%)		
	3 Neutro	297 (48,8%)		
	4 Concordo parcialmente	144 (21,7%)		
	5 Concordo totalmente	134 (20,2%)		
29 Meu gestor recomenda que devo seguir as políticas de segurança da informação da instituição.	1 Discordo totalmente	66 (10,0%)	3	3
	2 Discordo parcialmente	71 (10,7%)		
	3 Neutro	209 (31,5%)		
	4 Concordo parcialmente	139 (21,0%)		
	5 Concordo totalmente	178 (26,8%)		
30 A alta administração recomenda que devo seguir as políticas de segurança da informação da instituição.	1 Discordo totalmente	57 (8,6%)	3	3
	2 Discordo parcialmente	80 (12,1%)		
	3 Neutro	195 (29,4%)		
	4 Concordo parcialmente	154 (23,2%)		
	5 Concordo totalmente	177 (26,7%)		

Fonte: Elaborado pela autora (2023).

Os itens (31, 32 e 33) mediram a variável ‘Normas descritivas’ - Percepções de que outras pessoas estão ou não executando o comportamento de prevenção. Os resultados indicaram que apesar do ponto neutro da escala possuir a maior frequência de respostas nos três itens, 264 (39,8%), 225 (33,9%) e 210 (31,7%), respectivamente, o lado positivo da escala apresentou uma frequência mais significativa de respostas, em detrimento do lado negativo da escala, evidenciado pela frequência de respostas no ponto de concordo parcialmente nos três itens, 158 (23,8%), 184 (27,8%) e 210 (31,7%), conforme Tabela 11.

Tabela 11 - Estatística descritiva da variável ‘Normas Descritivas’

Itens	Escala	Frequência	Mediana	Moda
31 Acredito que meus colegas implementam medidas de segurança para se proteger contra as ameaças à segurança da informação.	1 Discordo totalmente	54 (8,1%)	3	3
	2 Discordo parcialmente	111 (16,7%)		
	3 Neutro	264 (39,8%)		
	4 Concordo parcialmente	158 (23,8%)		
	5 Concordo totalmente	76 (11,5%)		
32 Acredito que meu gestor	1 Discordo totalmente	53 (8,0%)	3	3

Itens	Escala	Frequência	Mediana	Moda
implementa medidas de segurança para se proteger contra as ameaças à segurança da informação.	2 Discordo parcialmente	77 (11,6%)		
	3 Neutro	225 (33,9%)		
	4 Concordo parcialmente	184 (27,8%)		
	5 Concordo totalmente	124 (18,7%)		
33 Acredito que a alta administração implementa as medidas de segurança para se proteger contra as ameaças à segurança da informação.	1 Discordo totalmente	41 (6,26%)		
	2 Discordo parcialmente	68 (10.3%)		
	3 Neutro	210 (31,7%)	4	3
	4 Concordo parcialmente	210 (31,7%)		
	5 Concordo totalmente	134 (20,2%)		

Fonte: Elaborado pela autora (2023).

A tabela 12 apresenta os resultados da medição da variável ‘conscientização’ - reflete a consciência das responsabilidades com a segurança da informação e os meios pelos quais essas responsabilidades são realizadas. Essa variável foi medida a partir das variáveis “relato de incidentes”; “informação e atualização”; “uso de e-mail”; e “gerenciamento de senhas”. Os resultados de 12 dos 13 itens que mediram a variável ‘conscientização’ inclinaram para o lado positivo da escala, indicando que a maior frequência de servidores concordou parcialmente ou concordaram totalmente com as afirmativas que mediram a variável. A exceção foi o item 45 relacionado a variável ‘gerenciamento de senhas’, em que os servidores indicaram negativamente sobre a troca frequente de senhas.

As descobertas da pesquisa de Ki-Aries e Faily, (2017) sugerem que uma abordagem de conscientização da segurança da informação centrada na pessoa tem a capacidade de se adaptar ao tempo e aos recursos necessários para sua implementação na organização, além de oferecer uma contribuição positiva para reduzir ou mitigar riscos à segurança da informação. Quando os funcionários estão cientes da política e dos procedimentos de segurança da informação de sua empresa, eles são mais competentes para gerenciar tarefas de segurança. (LI *et al.*, 2019). Bélanger *et al.* (2017) destacam ainda a importância da conscientização para influenciar a mudança de comportamento.

Tabela 12 - Estatística descritiva da variável ‘Conscientização’

Itens/variáveis	Escala	Frequência	Mediana	Moda
Relato de Incidentes				
34 Tenho conhecimento do setor que devo me reportar caso tenha conhecimento ou sofra algum incidente de segurança da	1 Discordo totalmente	67 (10,1%)		
	2 Discordo parcialmente	82 (12,4%)		
	3 Neutro	61 (9,2%)	4	5

Itens/variáveis	Escala	Frequência	Mediana	Moda
Relato de Incidentes				
informação.	4 Concordo parcialmente	162 (24,4%)		
	5 Concordo totalmente	291 (43,9%)		
35 Se eu perceber algum comportamento suspeito, eu reportarei ao setor competente.	1 Discordo totalmente	12 (1,8%)	5	5
	2 Discordo parcialmente	19 (2,9%)		
	3 Neutro	60 (9,0%)		
	4 Concordo parcialmente	192 (29,0%)		
	5 Concordo totalmente	380 (57,3%)		
37 Se eu souber de algum incidente de segurança da informação, reportarei ao setor competente.	1 Discordo totalmente	9 (1,4%)	5	5
	2 Discordo parcialmente	19 (2,9%)		
	3 Neutro	57 (8,6%)		
	4 Concordo parcialmente	204 (30,8%)		
	5 Concordo totalmente	374 (56,4%)		
Informação e Atualização				
38 Minha instituição informa periodicamente sobre as questões de violações de segurança da informação por meio de campanhas de conscientização (e-mail, folheto / seminário / workshop).	1 Discordo totalmente	67 (10,1%)	2	1
	2 Discordo parcialmente	82 (12,4%)		
	3 Neutro	61 (9,2%)		
	4 Concordo parcialmente	162 (24,4%)		
	5 Concordo totalmente	291 (43,9%)		
39 Minha instituição me mantém atualizado sobre violações de segurança da informação e medidas preventivas.	1 Discordo totalmente	12 (1,8%)	3	2
	2 Discordo parcialmente	19 (2,9%)		
	3 Neutro	60 (9,0%)		
	4 Concordo parcialmente	192 (29,0%)		
	5 Concordo totalmente	380 (57,3%)		
40 Minha instituição continua instruindo os funcionários sobre suas responsabilidades de segurança de computador.	1 Discordo totalmente	9 (1,4%)	3	1
	2 Discordo parcialmente	19 (2,9%)		
	3 Neutro	57 (8,6%)		
	4 Concordo parcialmente	204 (30,8%)		
	5 Concordo totalmente	374 (56,4%)		
Uso de e-mail				
41 Eu não clico em todos os links de e-mail, mesmo se o remetente for uma pessoa conhecida.	1 Discordo totalmente	32 (4,8%)	4	5
	2 Discordo parcialmente	68 (10,3%)		
	3 Neutro	59 (8,9%)		
	4 Concordo parcialmente	187 (28,2%)		
	5 Concordo totalmente	317 (47,8%)		
43 Eu não abro e-mail se o remetente for um desconhecido.	1 Discordo totalmente	86 (13,0%)	3	5
	2 Discordo parcialmente	153 (23,1%)		

Itens/variáveis	Escala	Frequência	Mediana	Moda
Relato de Incidentes				
	3 Neutro	94 (14,2%)		
	4 Concordo parcialmente	111 (16,7%)		
	5 Concordo totalmente	219 (33,0%)		
Gerenciamento de senha				
44 Uso diferentes senhas para acessar contas pessoais e do trabalho.	1 Discordo totalmente	51 (7,7%)	5	5
	2 Discordo parcialmente	70 (10,6%)		
	3 Neutro	46 (6,9%)		
	4 Concordo parcialmente	164 (24,7%)		
	5 Concordo totalmente	332 (50,1%)		
45 Troco minhas senhas com frequência.	1 Discordo totalmente	143 (21,6%)	3	4
	2 Discordo parcialmente	142 (21,4%)		
	3 Neutro	113 (17,0%)		
	4 Concordo parcialmente	166 (25,0%)		
	5 Concordo totalmente	99 (14,9%)		
46 Não compartilho minhas senhas com meus colegas de trabalho.	1 Discordo totalmente	16 (2,4%)	5	5
	2 Discordo parcialmente	28 (4,2%)		
	3 Neutro	21 (3,2%)		
	4 Concordo parcialmente	87 (13,1%)		
	5 Concordo totalmente	511 (77,1%)		
47 Uso combinações de letras, números e símbolos para minhas senhas do trabalho.	1 Discordo totalmente	17 (2,6%)	5	5
	2 Discordo parcialmente	24 (3,6%)		
	3 Neutro	34 (5,1%)		
	4 Concordo parcialmente	144 (21,7%)		
	5 Concordo totalmente	444 (67.0%)		
48 Bloqueio a tela do computador por meio de senha antes de me ausentar da minha estação de trabalho.	1 Discordo totalmente	117 (17,6%)	4	5
	2 Discordo parcialmente	81 (12,2%)		
	3 Neutro	79 (11,9%)		
	4 Concordo parcialmente	113 (17,0%)		
	5 Concordo totalmente	273 (41,2%)		

Fonte: Elaborado pela autora (2023).

Os itens (49, 50 e 51) mediram a variável ‘Capacitação’ - treinamento realizado em diferentes formas de apresentação, conforme Tabela 13. Os resultados dos três itens que mensuraram a referida variável indicaram uma maior frequência de respostas do lado negativo da escala. O ponto de maior recorrência de respostas nos três itens foi discordo totalmente, 240 (36,2%), 219 (33,0%) e 200 (30,2%), respectivamente, sinalizando que para os servidores

pesquisados, as universidades não possuem um programa de capacitação constante, eficiente e que venha a contribuir para o desenvolvimento de habilidades necessárias para adotar um comportamento seguro. No entanto, a capacitação é um método eficaz de conscientizar os funcionários na área de segurança da informação. Os resultados da pesquisa têm demonstrado grande eficácia da capacitação como método não apenas de aprimorar o conhecimento sobre segurança da informação, mas principalmente aquele que tem um impacto significativo no real comportamento dos funcionários (STEFANIUK, 2020).

Tabela 13 - Estatística descritiva da variável 'Capacitação'

Itens	Escala	Frequência	Mediana	Moda
49 Minha instituição possui um programa de capacitação constante para que eu me mantenha informado sobre atualização das políticas e de procedimentos de segurança da informação.	1 Discordo totalmente	240 (36,2%)	2	1
	2 Discordo parcialmente	173 (26,1%)		
	3 Neutro	151 (22,8%)		
	4 Concordo parcialmente	74 (11,2%)		
	5 Concordo totalmente	25 (3,8%)		
50 Os programas de capacitação em segurança da informação da minha instituição me mantêm bem-informado contra ameaças à segurança.	1 Discordo totalmente	219 (33,0%)	2	1
	2 Discordo parcialmente	177 (26,7%)		
	3 Neutro	162 (24,4%)		
	4 Concordo parcialmente	73 (11,0%)		
	5 Concordo totalmente	32 (4,8%)		
51 Os programas de capacitação em segurança da informação da minha instituição contribuem para que eu desenvolva habilidades necessárias para adotar um comportamento seguro.	1 Discordo totalmente	200 (30,2%)	2	1
	2 Discordo parcialmente	162 (24,4%)		
	3 Neutro	179 (27,0%)		
	4 Concordo parcialmente	80 (12,1%)		
	5 Concordo totalmente	42 (6,3%)		

Fonte: Elaborado pela autora (2023).

A Tabela 14 apresenta os resultados dos itens (52, 53, 54 e 55), utilizados para medir a variável 'intenção de comportamento de prevenção' – intenção de agir de acordo com as políticas e regras de segurança da informação. Nos quatro itens os servidores indicaram de forma muito expressiva, representado pela frequência de respostas nos pontos concordam totalmente 482 (72,7%), 508 (76,6%), 513 (77,4%) e 255 (38,5%); e concordo parcialmente 142 (21,4%), 121 (18,3%), 118 (17,8%) e 181 (27,3%), que possuem a intenção de agir de acordo com as políticas de segurança da informação das instituições as quais pertencem.

Tabela 14 - Estatística descritiva da variável 'Intenção de Comportamento de Prevenção'

Itens	Escala	Frequência	Mediana	Moda
52 Pretendo cumprir os requisitos das Políticas de Segurança da Informação da minha instituição no futuro.	1 Discordo totalmente	7 (1,1%)	5	5
	2 Discordo parcialmente	3 (0,5%)		
	3 Neutro	29 (4,4%)		
	4 Concordo parcialmente	142 (21,4%)		
	5 Concordo totalmente	482 (72,7%)		
53 Pretendo cumprir minhas responsabilidades em relação às Políticas de Segurança da Informação no futuro.	1 Discordo totalmente	7 (1,1%)	5	5
	2 Discordo parcialmente	3 (0,5%)		
	3 Neutro	24 (3,6%)		
	4 Concordo parcialmente	121 (18,3%)		
	5 Concordo totalmente	508 (76,6%)		
54 É minha intenção continuar a cumprir as Políticas de Segurança da Informação institucionais.	1 Discordo totalmente	0 (0,0%)	5	5
	2 Discordo parcialmente	1 (0,2%)		
	3 Neutro	31 (4,7%)		
	4 Concordo parcialmente	118 (17,8%)		
	5 Concordo totalmente	513 (77,4%)		
55 A Política de Segurança da Informação da minha instituição influencia nas minhas rotinas de trabalho.	1 Discordo totalmente	27 (4,1%)	4	5
	2 Discordo parcialmente	65 (9,8%)		
	3 Neutro	135 (20,4%)		
	4 Concordo parcialmente	181 (27,3%)		
	5 Concordo totalmente	255 (38,5%)		

Fonte: Elaborado pela autora (2023).

Por fim, a Tabela 15 apresenta os resultados dos itens (56,57,58 e 59) do questionário que foram utilizados para medir a variável 'fortalecimento da política de segurança da informação' – a política de segurança da informação está disponível a todos os servidores de forma clara e com procedimentos bem definidos. A frequência de respostas ficou fragmentada nos cinco pontos da escala. O ponto neutro apresentou uma frequência significativa de respostas nos quatro itens 222 (33,5%), 181 (27,3%), 198 (29,9%) e 196 (29,6%), respectivamente, o que indica que nas universidades as políticas de segurança da informação não possuem a publicidade necessária, bem como as regras e procedimentos não se apresentam de forma clara para esses servidores. De acordo com a pesquisa desenvolvida por Ogbanufe, Crossler e Biros (2021) nos EUA, as ameaças à segurança, a política de segurança e o suporte organizacional ajudam a fomentar a identidade de segurança da informação relacionada ao trabalho e aos comportamentos de segurança dos funcionários.

Tabela 15 - Estatística descritiva da variável 'Fortalecimento da Política de SI'.

Itens	Escala	Frequência	Mediana	Moda
56 Minha instituição garante que as Políticas de Segurança da Informação estejam disponíveis para todos os funcionários.	1 Discordo totalmente	104 (15,7%)	3	3
	2 Discordo parcialmente	130 (19,6%)		
	3 Neutro	222 (33,5%)		
	4 Concordo parcialmente	105 (15,8%)		
	5 Concordo totalmente	102 (15,4%)		
57 Acredito que minha instituição tenha estabelecido regras de conduta para o uso de recursos de informática.	1 Discordo totalmente	56 (8,4%)	3	4
	2 Discordo parcialmente	97 (14,6%)		
	3 Neutro	181 (27,3%)		
	4 Concordo parcialmente	203 (30,6%)		
	5 Concordo totalmente	126 (19,0%)		
58 Minha instituição tem diretrizes específicas que regem o que os funcionários têm permissão para fazer com seus computadores.	1 Discordo totalmente	88 (13,3%)	3	3
	2 Discordo parcialmente	129 (19,5%)		
	3 Neutro	198 (29,9%)		
	4 Concordo parcialmente	162 (24,4%)		
	5 Concordo totalmente	86 (13,0%)		
59 Acredito que minha instituição definiu códigos de conduta explicando o que devemos e não devemos fazer em relação à segurança da informação.	1 Discordo totalmente	89 (13,4%)	3	3
	2 Discordo parcialmente	112 (16,9%)		
	3 Neutro	196 (29,6%)		
	4 Concordo parcialmente	179 (27,0%)		
	5 Concordo totalmente	87 (13,1%)		

Fonte: Elaborado pela autora (2023).

A próxima subseção apresenta o resultado descritivo do questionário aplicado aos gestores de segurança da informação das universidades.

4.4 ANÁLISE DESCRITIVA DO QUESTIONÁRIO APLICADO AOS GESTORES

Por meio de estatística descritiva, foram analisados os 23 questionários respondidos pelos gestores de segurança da informação das universidades. Esse questionário, contendo quatro itens, possibilitou atender o objetivo específico de identificar quais os controles, relacionados ao comportamento humano em segurança da informação, são utilizados pelas universidades federais.

Para Alotaibi, Furnell e Clarke (2019), muitas organizações implementam os controles técnicos mais avançados na tentativa de minimizar o risco associado ao fator humano. No entanto, o humano ainda representa a maior ameaça bem como a maior vulnerabilidade. Assim,

considerar um equilíbrio entre os controles técnicos e não técnicos proporciona uma maior proteção aos ativos de informação. De acordo com a *International Organization for Standartization e a International Electrotechnical Commission* (ISO/IEC 27000, 2014), os controles de segurança da informação incluem qualquer processo, política, dispositivo, prática ou outras ações que minimizem o risco. Os controles devem assegurar que os riscos sejam reduzidos a um nível aceitável, o que diminui prováveis incidentes de segurança da informação.

No item um foi apresentado aos gestores uma lista de controles relacionados ao comportamento humano em segurança da informação, adaptados da Associação Brasileira de Normas Técnicas (ABNT NBR ISO/IEC 27002, 2013b), em que foi solicitado a sinalização dos controles utilizados pela respectiva universidade. Ressalta-se que havia a opção para o gestor inserir outros controles não listados. Os resultados estão apresentados na Tabela 16.

Tabela 16 - Instrumentos de controle utilizados pelas universidades pesquisadas

Item	Instrumentos de controle	Frequência
1 Quais desses instrumentos de controle existem na sua instituição? (Marque quantas opções forem necessárias).	Política de segurança da informação	16 (69,6%)
	Controle de acesso físico ao ambiente de trabalho	13 (56,5%)
	Política para uso de correio eletrônico	11 (47,8%)
	Política de Senhas	6 (26,1%)
	Capacitação em conscientização da segurança da informação	4 (17,4%)
	Campanhas de conscientização em segurança da informação.	4 (17,4%)
	Termo de responsabilidade e confidencialidade dando ciência do conhecimento das normas e suas principais responsabilidades em relação à segurança da informação.	3 (13,0%)
	Política de Classificação da Informação	2 (8,7%)
	Política de Mesa Limpa/Tela Limpa	1 (4,3%)

Fonte: Elaborado pela autora (2023).

A partir das respostas dos gestores de segurança da informação, percebeu-se que a utilização de controles relacionados ao comportamento humano ainda é modesta nas universidades federais brasileiras. A política de segurança da informação foi o controle mais representativo, com a frequência de 16 (69,6%). No entanto, o Governo Federal havia instituído desde 13 de junho de 2000 a política de segurança da informação nos órgãos e entidades da administração pública federal por meio do Decreto Presidencial nº 3.505. O referido decreto foi revogado pelo Decreto nº 9.637, de 26 de dezembro de 2018 que institui a Política Nacional de Segurança da Informação, ficando ainda sobre a competência das entidades da administração pública federal, conforme Art. 15, inciso II, do referido decreto “elaborar sua política de

segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República" (BRASIL, 2018).

O controle de acesso físico ao ambiente de trabalho, ou seja, prevenir o acesso físico não autorizado, obteve a frequência de 13 (56,5%), apresentando-se como o segundo controle mais utilizado pelas universidades pesquisadas. Para Aurigemma e Mattson (2017a), os controles de acesso físico, incluindo os "guardas de segurança", são eficazes na mitigação parcial da ameaça de utilização não autorizada, mas esses controles podem ser menos eficientes quando negam as ameaças humanas associadas à manifestação de cortesia. No entanto, quando esses "guardas de segurança" são conscientizados sobre a importância da salva guarda dessas informações e conscientes de suas responsabilidades relacionadas ao não cumprimento de suas atribuições, eles tornam-se um importante aliado à segurança da informação, uma vez que os controles de acesso físico como sensores, dispositivos biométricos e cartões de identificação, às vezes, tornam-se difíceis ou impossíveis de serem implementados de forma adequada, dadas as restrições físicas, jurídicas e financeira.

A política para uso de correio eletrônico, seguida da política de senhas também foram indicadas como controles utilizados pelas universidades representando 11 (47,8%) e 6 (26,1%), respectivamente. A política para o uso de correio eletrônico é um importante controle que contribui na mitigação de incidentes causados por ataques de *phishing*.

Nas universidades federais, o uso da política de senhas ainda se apresenta de forma incipiente. No entanto, para Bélanger *et al.* (2017), esse é um dos controles de segurança mais comumente usados pelas organizações e um método primário de autenticação do usuário. Muitas técnicas têm sido exploradas para aprimorar o uso de senhas, como a criação de uma senha forte e alterações frequentes de senha continuam a ser técnicas fundamentais para aumentar a segurança. A aplicação tecnológica dessa política, como por exemplo, por meio de uma combinação de um *software* de verificação de senha e uma política de bloqueio, geralmente aumenta sua eficácia.

A utilização de capacitação e de campanhas de conscientização em segurança da informação, pelas universidades pesquisadas, obtiveram a frequência de 4 (17,4%). A conscientização em segurança da informação é adquirida por meio de campanhas e de capacitação, dessa forma o servidor consegue obter uma compreensão quanto à gravidade das ameaças à segurança da informação (QAZI; RAZA; KHAN, 2020).

A conscientização em segurança da informação é considerada o fator crucial para ajudar as organizações a prevenir incidentes de violação de segurança da informação (SAFA;

VON SOLMS, 2016a; VEIGA *et al*., 2020). É uma ferramenta vital para inculcar a consciência de segurança e garantir um comportamento compatível com a segurança entre os funcionários (MD AZMI *et al.*, 2021; SAFA *et al.*, 2019). Os programas de conscientização e capacitação em segurança são os principais determinantes de um comportamento preventivo (BARLOW *et al.*, 2018; CONNOLLY; LANG; WALL, 2019; MD AZMI *et al.*, 2021). Da mesma forma, a pesquisa de Safa e Maple (SAFA; MAPLE, 2016) descobriu que os funcionários conscientizados e capacitados considerarão as consequências de suas ações antes de se envolver em qualquer atividade que possa causar danos ao sistema de segurança da informação da organização. Além disso, as descobertas de Connolly, Lang e Wall (2019) mostraram que quando os funcionários percebem que há uma razão válida por trás de um regulamento específico, eles tendem a cumprir as regras.

Isso demonstra a importância de as universidades investirem na capacitação e conscientização dos seus servidores, incluindo os novos, a fim de que todos tenham o conhecimento suficiente em segurança para avaliar as possíveis ameaças. De acordo com os resultados da pesquisa de Barlow *et al.* (2018) realizada nos EUA, as organizações usam programas de educação, capacitação e conscientização sobre segurança para combater as ameaças à segurança interna e promover a conformidade com as políticas de segurança da informação.

Com relação aos incidentes de segurança relacionados ao comportamento humano, item dois do questionário, os gestores de segurança da informação indicaram que os ataques por *phishing* 10 (43,5%) e engenharia social 5 (21,7%) são os mais recorrentes, apesar de 7 (30,4%) das universidades sinalizarem que ainda não realizam esse mapeamento, conforme Tabela 17.

A engenharia social consiste em usar a fraude, a influência e a manipulação psicológica de pessoas para a execução de ações ou para a divulgação de informações confidenciais. O *phishing* é uma tática da engenharia social representada pela tentativa de adquirir informações confidenciais ou pessoais *por e-mail*. O remetente se disfarça como legítimo e solicita que o destinatário execute uma ação, como clicar em um *link* fornecido (PARSONS *et al.*, 2017). Os dois ataques são exemplos de erros de comportamento humano em segurança da informação. Os ataques de *phishing* são muito comuns em universidades, de acordo com a pesquisa de Schuetz *et al.* (2020), desenvolvida em universidades americanas. Para Hina, Selvam e Lowry (2019) o número e a gravidade das violações de segurança da informação em instituições de ensino superior estão aumentando continuamente devido aos baixos níveis de conscientização dos servidores. Do mesmo modo, as pesquisas de Aleroud *et al.* (2020) e de Flores e Ekstedt

(2016b) identificaram que a engenharia social possui uma associação direta com a conscientização em segurança da informação.

Tabela 17 - Incidentes de segurança mais frequentes nas universidades

Item	Incidentes de segurança	Frequência
2 Quais incidentes de segurança relacionados aos aspectos humanos ocorrem com mais frequência na sua instituição?	*Phishing*	10 (43,5%)
	Engenharia Social	5 (21,7%)
	Defacement[19]	2 (8,7%)
	Acesso indevido por compartilhamento de senhas	2 (8,7%)
	Acesso indevido a rede sem fio por terceirizados com senhas de alunos	1 (4,3%)
	Ransomware	1 (4,3%)
	Não há mapeamento ainda.	7 (30,4%)

Fonte: Elaborado pela autora (2023).

O item três abordou gestão de incidentes de segurança da informação a partir dos canais de comunicação. De acordo com a Associação Brasileira de Normas Técnicas (ABNT NBR ISO/IEC 27002, 2013b) o controle gestão de incidentes de segurança da informação objetiva assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação. De acordo com as respostas dos gestores, o e-mail foi o canal de comunicação com maior frequência de uso pelas universidades para informar sobre incidentes de segurança da informação, 20 (87,0%), seguido pelo telefone, 6 (26,1%) e pelo site institucional, 5 (21,7%), conforme Tabela 18.

Tabela 18 - Canais de comunicação

Item	Canais de comunicação	Frequência
3 Quais os canais de comunicação para informar incidentes de segurança ou denúncias de quebra de segurança pela comunidade acadêmica? (Pode marcar mais de uma opção)	E-mail	20 (87,0%)
	Telefone	6 (26,1%)
	Site institucional	5 (21,7%)
	Sistema interno de chamados	4 (17,4%)
	Redes sociais	3 (13,0%)
	Não existe ponto de contato	3 (13,0%)

Fonte: Elaborado pela autora (2023).

19 Consiste na realização de modificações de conteúdo e estética de uma página da web.

O item quatro abordou sobre as responsabilidades pela quebra de segurança. Estabelecer responsabilidades pela segurança da informação é um dos objetivos do controle organizacional da segurança da informação (ABNT NBR ISO/IEC 27002, 2013). Para Cannolly *et al.* (2017), as sanções organizacionais, recompensas, educação e treinamento em segurança e políticas de segurança da informação são todas formas de controles organizacionais formais. Nesse sentido, para 10 (43,5%) dos gestores pesquisados, raramente o servidor é responsabilizado pela quebra da segurança, Tabela 19. Isso pode ser consequência da inexistência de processo disciplinar formal para a violação da segurança da informação nas universidades (ARAÚJO, 2016).

Tabela 19 - responsabilizado pela quebra de segurança

Item	Escala	Frequência
4 O servidor é responsabilizado pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso.	Nunca	4 (17,4%)
	Raramente	10 (43,5%)
	Ocasionalmente	4 (17,4%)
	Quase sempre	3 (13,0%)
	Sempre	2 (8,7%)

Fonte: Elaborado pela autora (2023).

A existência de normas e políticas de segurança da informação não garante que os servidores desempenhem um comportamento preventivo. Eles podem não se comportar como esperado, seja por comportamento intencional de violação da política, ou mesmo por falta de compreensão de seu conteúdo. Os funcionários que não cumprem as normas ou que desconhecem a política de segurança da informação se tornaram uma grande ameaça à organização (ALOTAIBI; FURNELL; CLARKE, 2019). Logo, ressalta-se a relevância de esclarecer ao servidor sobre suas responsabilidades e possíveis penalidades diante do manuseio indevido da informação, evitando possíveis sanções em virtude da falta de conhecimento necessário às práticas previstas nas normas e políticas de segurança da informação da instituição (ARAÚJO, 2016).

4.5 TESTE DAS HIPÓTESES DA PESQUISA

Para atingir os objetivos específicos de: investigar as relações entre vulnerabilidade percebida; gravidade percebida das ameaças; gravidade percebida das sanções; eficácia da resposta; autoeficácia; normas injuntivas; normas descritivas; conscientização; fortalecimento da política e capacitação com a intenção de comportamento de prevenção dos servidores; e

desenvolver um modelo de comportamento preventivo para as universidades federais, baseado na TMP, realizamos o teste de correlação do coeficiente ρ (rho) de Spearman no *software* SPSS. Esse teste permitiu identificar as relações entre as variáveis para o desenvolvimento do modelo, e assim, verificar as hipóteses de pesquisa.

O resultado do teste de correlações de ρ de Spearman está representado na Tabela 20. Antes da execução desse teste, foi necessário transformar as variáveis que possuíam mais de um item no questionário, a partir da soma dos resultados dos seus itens, tornando-as variáveis compostas.

Tabela 20 - Correlações de Spearman entre as variáveis da pesquisa e a intenção de comportamento de prevenção

Variáveis da pesquisa	**ρ (rho) e *p - value***	Intenção de Comportamento de Prevenção
Vulnerabilidade Percebida	ρ (rho)	,245**
	p – value	0,000
Gravidade Percebida da Ameaça	ρ (rho)	,232**
	p – value	0,000
Gravidade Percebida das Sanções	ρ (rho)	,271**
	p – value	0,000
Eficácia de Resposta	ρ (rho)	,275**
	p – value	0,000
Autoeficácia	ρ (rho)	,195**
	p – value	0,000
Custo de Resposta	ρ (rho)	-0,018
	p – value	0,636
Normas Injuntivas	ρ (rho)	,363**
	p – value	0,000
Normas Descritivas	ρ (rho)	,299**
	p – value	0,000
Conscientização	ρ (rho)	,345**
	p – value	0,000
Capacitação	ρ (rho)	,215**
	p – value	0,000
Fortalecimento da Política	ρ (rho)	,324**
	p – value	0,000
Região	ρ (rho)	-0,026
	p – value	0,506
Sexo	ρ (rho)	0,018
	p – value	0,646
Idade	ρ (rho)	-0,011
	p – value	0,772
Categoria Profissional	ρ (rho)	0,081
	p – value	0,063
Tempo de serviço	ρ (rho)	-0,016
	p – value	0,673

Variáveis da pesquisa	ρ (rho) e *p - value*	Intenção de Comportamento de Prevenção
Escolaridade	ρ (rho)	-0,056
	p – value	0,150

Fonte: Elaborado pela autora (2023).
Nota: A correlação é significativa no nível 0,01 (2 extremidades)**

A partir do teste de correlação, apresentado na Tabela 20, podemos identificar que há correlações significativas e positivas entre as variáveis vulnerabilidade percebida (ρ = 0,245; *p* < 0,001), gravidade percebida da ameaça (ρ = 0,232; *p* < 0,001), gravidade percebida das sanções (ρ = 0,271; *p* < 0,001), eficácia de resposta (ρ = 0, 275; *p* < 0,001), autoeficácia (ρ = 0, 195; *p* < 0,001), normas injuntivas (ρ = 0, 363; *p* < 0,001), normas descritivas (ρ = 0, 299; *p* < 0,001), conscientização (ρ = 0, 345; *p* < 0,001), capacitação (ρ = 0, 215; *p* < 0,001) e fortalecimento da política (ρ = 0, 324; *p* < 0,001) e a intenção de comportamento de prevenção dos servidores das universidades, uma vez que, essas correlações possuem valores de p -*value* < 0,05 e coeficientes ρ (rho) significativos e positivos. Portanto, todas as hipóteses são aceitas, exceto a H6, relacionada à variável custo de resposta (ρ = - 0,018; *p* > 0,05). Nesse caso, não rejeitamos a H0[20] – Não há relação entre custo de resposta e a intenção de comportamento de prevenção, conforme apresentado no Quadro 14.

Quadro 14 - Resultado do teste de hipóteses

Hipóteses da pesquisa	Resultado do teste
H1 A vulnerabilidade percebida está relacionada positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H2 A gravidade percebida da ameaça está relacionada positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H3 A gravidade percebida das sanções está relacionada positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H4 A eficácia da resposta está relacionada positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H5 A autoeficácia está relacionada positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H6 O custo de resposta está relacionado negativamente com a intenção de comportamento de prevenção.	Não rejeita a hipótese nula
H7 As normas injuntivas estão relacionadas positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H8 As normas descritivas estão relacionadas positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H9 A conscientização está relacionada positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula

[20] Hipótese nula

Hipóteses da pesquisa	Resultado do teste
H10 O fortalecimento da política está relacionado positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula
H11 A capacitação está relacionada positivamente com a intenção de comportamento de prevenção.	Rejeita a hipótese nula

Fonte: Elaborado pela autora (2023).

As variáveis que se relacionaram com intenção de comportamento de prevenção e que se comportaram de acordo com a literatura são: vulnerabilidade percebida e a eficácia da resposta (HINA; SELVAM; LOWRY, 2019; RAJAB; EYDGAHI, 2019); gravidade percebida da ameaça (HINA; SELVAM; LOWRY, 2019; JANSEN; VAN SCHAIK, 2017); autoeficácia (AHMAD *et al*., 2019; BARLETTE; JAOUEN, 2019; ZHEN; XIE; DONG, 2020a); gravidade percebida das sanções (SAFA *et al*., 2019); normas descritivas (JANSEN; VAN SCHAIK, 2017); conscientização (HINA; SELVAM; LOWRY, 2019; PARSONS *et al*., 2017); capacitação e fortalecimento da política (HINA; SELVAM; LOWRY, 2019).

Normas injuntivas foi a variável de maior correlação com a intenção de comportamento de prevenção dos servidores das universidades, comportamento diferente do apresentado nos resultados do modelo integrado proposto na pesquisa de Jansen e Van Schailk (2017) aplicada aos usuários de bancos na Holanda, em que essa variável não apresentou correlação significativa com comportamento de prevenção. Do mesmo modo, o custo de resposta também apresentou resultado antagônico, uma vez que, essa variável não apresentou relação significativa negativa com a intenção do comportamento de prevenção no contexto desta pesquisa como esperado na literatura (JANSEN; VAN SCHAIK, 2018b).

As variáveis referentes ao perfil do servidor respondente: região ($\rho = - 0{,}026$; $p > 0{,}05$), sexo ($\rho = 0{,}018$; $p > 0{,}05$), idade ($\rho = - 0{,}011$; $p > 0{,}05$), categoria profissional ($\rho = 0{,}081$; $p > 0{,}05$), tempo de serviço ($\rho = - 0{,}016$; $p > 0{,}05$) e escolaridade ($\rho = - 0{,}056$; $p > 0{,}05$) não apresentaram relação com a intenção de comportamento de prevenção, uma vez que, apresentaram o valor de $p > 0{,}05$.

Entre as variáveis preditoras[21] da TMP (vulnerabilidade percebida, gravidade percebida da ameaça, eficácia de resposta e autoeficácia), a eficácia da resposta, a vulnerabilidade percebida e a gravidade percebida da ameaça são, respectivamente, as de maior correlação com a intenção de comportamento de prevenção. Isso significa que, no contexto dos servidores das universidades federais, quanto maior a avaliação da probabilidade de ocorrência de um

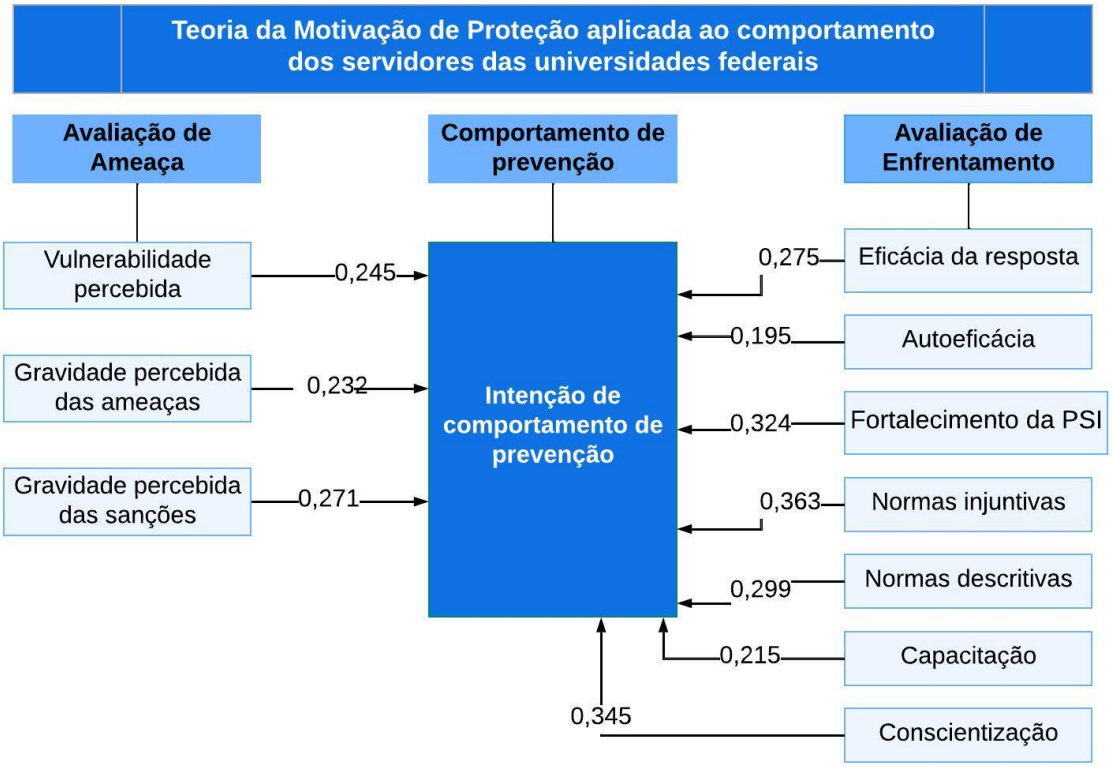
[21] O mesmo que variável independente, ou seja, é a causa presumida de qualquer mudança na variável dependente.

incidente de segurança, quanto maior a avaliação do impacto das consequências desse incidente e quanto mais eficaz uma medida é percebida pelo servidor, maior será a intenção de um comportamento de prevenção.

Os resultados revelaram que das variáveis inseridas ao modelo, a conscientização, as normas injuntivas e o fortalecimento da política foram as que mais possuíam relação com a intenção de comportamento de prevenção. O que nos leva a inferir que quanto maior a conscientização em segurança da informação, quanto maior a percepções do servidor sobre o que ele deve ou não fazer e quanto mais a política de segurança da informação está disponível de forma clara e com procedimentos bem definidos maior será a intenção de um comportamento de prevenção do servidor das universidades federais.

Diante do exposto, a Figura 22 ilustra o modelo de pesquisa aplicado aos servidores das universidades federias, a partir da TMP. Ressaltamos que foram inseridas ao modelo apenas as variáveis que apresentaram relação com a intenção de comportamento de prevenção.

Figura 22 - Modelo de comportamento aplicado às universidades federais



Fonte: Elaborado pela autora (2023).

A próxima seção apresenta as principais considerações sobre o desenvolvimento, a aplicação e os resultados desta pesquisa.

5 CONSIDERAÇÕES FINAIS

Para compreender como a segurança da informação vem sendo conduzida no contexto das universidades federais brasileiras, esta pesquisa se propôs a analisar o comportamento humano em segurança da informação, a partir da Teoria da Motivação de Proteção (TMP). Como foi observado na Revisão Sistemática de Literatura (RSL), desenvolvida para atender ao primeiro objetivo específico desta pesquisa, essa temática ainda é pouco explorada em contexto brasileiro, apesar da grande incidência de ciberataques sofridos pelo Brasil, inclusive no setor público, de acordo com o Relatório do Symantec (2019).

No início do desenvolvimento desta pesquisa, a partir da RSL, foi possível identificar as principais características das produções científicas relacionadas ao comportamento humano em segurança da informação. A análise dos 160 artigos obtidos nos permitiu traçar um panorama de como a temática foi estudada no período de 2017-2021. A partir da análise bibliométrica, dentre outros fatores, identificamos a preferência dos autores pelas metodologias que incluem estudos empíricos com abordagem quantitativa e o uso de questionários *on-line* como principal instrumento de coleta, sendo os Estados Unidos da América (EUA), seguido da China e da Austrália os países que mais estudam essa temática. A variedade de teorias identificadas para estudar o comportamento humano em segurança da informação destaca a abordagem interdisciplinar da temática, tornando necessária uma visão global que inclua não apenas o ponto de vista tecnológico, mas também, a perspectiva de outras disciplinas, como a Ciência da Informação que, por ser um campo interdisciplinar, possibilita um estudo mais rico da segurança da informação, sob a ótica da gestão da informação e do conhecimento.

A RSL ainda nos possibilitou, a partir da análise lexicométrica, realizar a Classificação Hierárquica Descendente pelo método de Reinert, que consistiu na organização dos artigos em quatro classes, o qual permitiu esclarecer a forma como se relacionam os estudos que abordam a temática comportamento humano em segurança da informação com outras temáticas como: Cultura Organizacional, Políticas de Segurança da Informação, Conscientização, Capacitação, Educação, *Phishing*, Conformidade e Teorias Comportamentais, e como essas relações são necessárias para uma melhor compreensão desse comportamento. De outro modo, a análise de similitude nos permitiu visualizar graficamente a estrutura do conteúdo de cada classe a partir da força da relação entre as palavras.

Com relação aos aspectos metodológicos, a utilização de entrevistas com especialistas e a aplicação de questionário *on-line* aos gestores de segurança e aos servidores (técnicos e

docentes) das universidades federais de todas as regiões do país nos permitiu uma maior compreensão sobre a temática, contribuindo para a criação de um modelo de comportamento de prevenção mais representativo da realidade das universidades públicas federais.

Em resposta ao primeiro questionamento desta pesquisa, bem como, para atender ao terceiro objetivo específico, identificamos a relação das variáveis do modelo ampliado da TMP, testado nesta pesquisa, com a intenção de comportamento de prevenção dos servidores das universidades. A partir do teste das hipóteses da pesquisa compreendemos a força e a direção dessas relações. Como mencionado anteriormente, a TMP possui dois processos cognitivos centrais, sendo avaliação de ameaça e avaliação de enfrentamento. Das variáveis que compõem a avaliação de ameaça, a gravidade percebida das sanções foi a que apresentou maior força na relação, seguida da vulnerabilidade percebida e da gravidade percebida das ameaças. Isso significa que: quanto maior a avaliação do impacto das sanções determinadas pelo incidente de segurança, maior é a intenção do comportamento de prevenção; quanto maior a avaliação da probabilidade de ocorrência de um incidente de segurança, maior é a intenção do comportamento de prevenção; e quanto maior a avaliação do impacto das consequências resultantes de um incidente de segurança, maior é a intenção do comportamento de prevenção. O fato de a gravidade percebida das sanções ter apresentado, nesta pesquisa, maior força de relação pode ser explicado, parcialmente, pelo medo do servidor em responder a um processo administrativo disciplinar que poderia acarretar constrangimentos, prejuízos financeiros ou, em casos mais graves a exemplo da exoneração.

A identificação da existência da relação significativa e positiva das variáveis vulnerabilidade percebida, gravidade percebida e gravidade percebida das sanções com a intenção de comportamento de prevenção dos servidores das universidades nos leva a deduzir que o servidor avalia o nível de perigo vinculado a um evento de segurança, o que é extremamente importante, uma vez que, da avaliação da ameaça inicia a avaliação de enfrentamento.

Quanto às variáveis relacionadas à avaliação de enfrentamento (eficácia de resposta, autoeficácia, custo de resposta, normas injuntivas, normas descritivas, conscientização, capacitação e fortalecimento da política), todas apresentaram relação significativa e positiva com a intenção de comportamento de prevenção, exceto o custo de resposta, o que pode ser explicado pelo desconhecimento do servidor quanto à quantidade de tempo, dinheiro ou esforço necessário para executar a resposta recomendada ou simplesmente pela inexistência de uma resposta recomendada pela instituição.

Nesse sentido, a variável com maior força da relação com intenção de comportamento de prevenção foi as normas injuntivas, seguida da conscientização, fortalecimento da política de segurança, normas descritivas, eficácia de resposta, capacitação e autoeficácia. Isso significa que: quanto maior as percepções sobre o que o servidor deve ou não deve fazer em relação à segurança da informação, maior a intenção de um comportamento de prevenção; quanto maior a consciência das responsabilidades com a segurança da informação e dos meios pelos quais essas responsabilidades são realizadas, maior a intenção de um comportamento de prevenção; quanto mais disponíveis e claras forem as políticas de segurança, maior a intenção de um comportamento de prevenção; quanto maior as percepções de que outros servidores estão ou não executando o comportamento de prevenção, maior a intenção de um comportamento de prevenção; quanto maior é a eficácia percebida de uma resposta de enfrentamento na redução de uma ameaça, maior a intenção de um comportamento de prevenção; quanto mais capacitado em segurança da informação, maior a intenção de um comportamento de prevenção; e quanto mais um servidor acredita que é capaz de realizar a medida de segurança, maior a intenção de um comportamento de prevenção.

A partir desses resultados percebemos como as variáveis estão interligadas, uma vez que, as percepções sobre o que o servidor deve ou não deve fazer em relação a segurança (normas injuntivas) podem ser construídas por meio de campanhas de conscientização, capacitação dos servidores e uma política de segurança da informação acessível, clara e com procedimentos bem definidos.

Esses resultados nos levaram a compreender que o modelo ampliado da TMP é mais eficaz para explicar parcialmente a intenção do comportamento de prevenção dos servidores, no contexto das universidades públicas federais, uma vez que todas as variáveis inseridas ao modelo possuem relação positiva e significativa com o comportamento de prevenção. É certo que uma teoria pode ser mais adequada para relacionar ou explicar um comportamento específico em determinada população, e outra seja necessária para explicar diversos comportamentos em uma outra população específica. É incerto especificar até que ponto os resultados são generalizáveis para outras universidades (estaduais e privadas), uma vez que essas instituições possuem culturas diferentes e são regidas por outras políticas.

A identificação das variáveis que apresentaram uma relação significativa com a intenção de comportamento de prevenção em segurança da informação mostra uma direção para alcançar um aumento dessa intenção comportamental e, assim, contribuir para a redução do número de incidentes em segurança nas universidades públicas federais brasileiras. Portanto, esse estudo não apenas expande nossa compreensão teórica sobre a intenção de comportamento de

prevenção, mas também, fornece uma orientação prática às universidades sobre as ações estratégicas voltadas ao comportamento dos servidores dessas instituições.

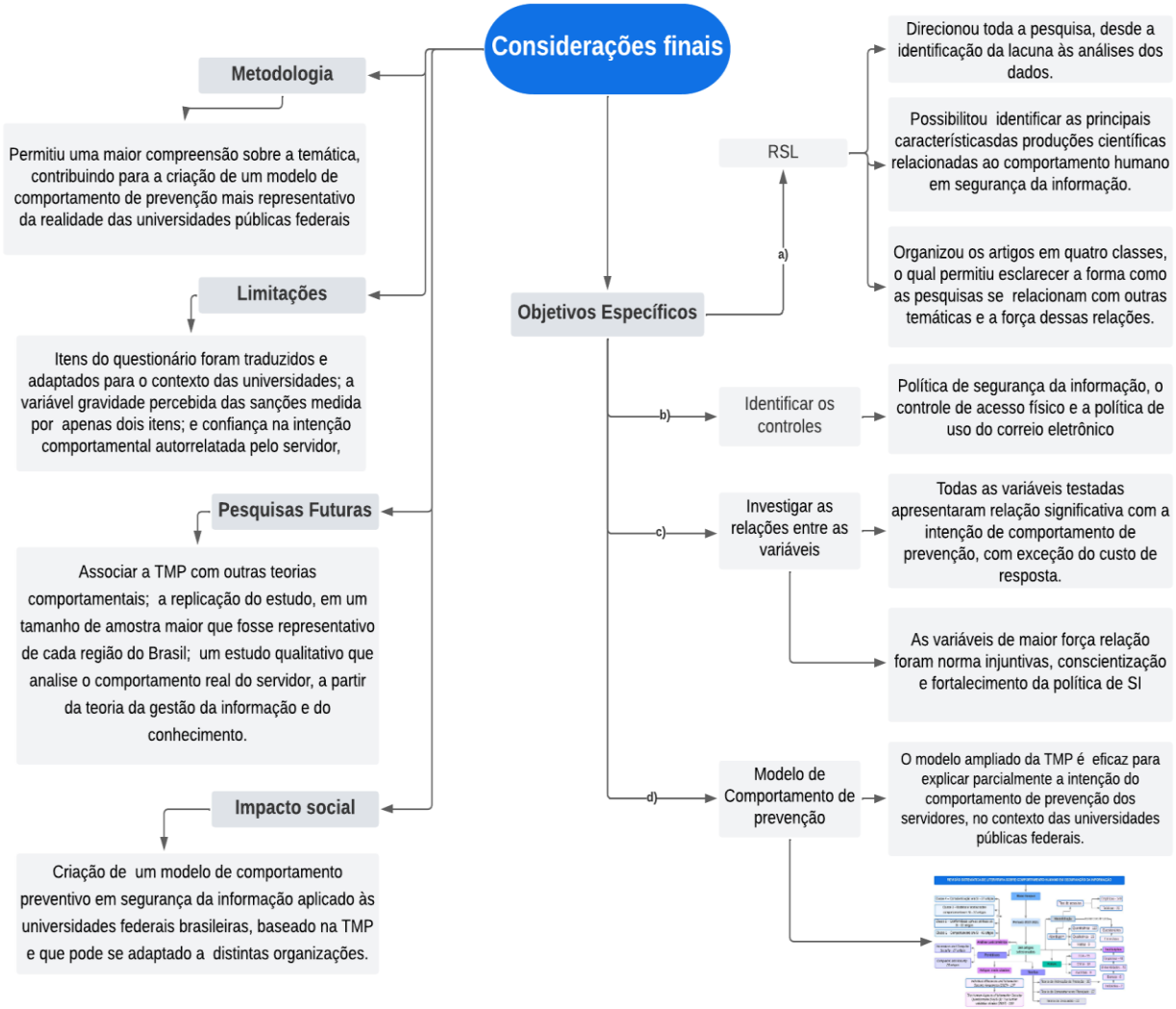
Como resposta ao segundo questionamento da pesquisa, assim como para atender ao segundo objetivo específico, identificamos os controles relacionados ao comportamento humano, sinalizados pelos gestores de segurança da informação das universidades. Os resultados indicaram como os controles mais utilizados na política de segurança da informação, o controle de acesso físico e a política de uso do correio eletrônico. Ressaltamos que a política de segurança da informação é uma exigência do governo federal que, embora seja muitas vezes criada pelas instituições, não possui a publicidade necessária para a sua disseminação, bem como não se apresenta de forma clara e com procedimentos bem definidos. A conscientização e a capacitação em segurança da informação ainda são abordadas de forma inexpressiva pelas universidades, apesar dos ataques do tipo p*hishing* serem majoritariamente os mais recorrentes. Isso nos leva a deduzir que o comportamento humano ainda não é compreendido como uma problemática que precisa ser abordada pelas universidades, não obstante a informação não ser apenas de responsabilidade técnica; é um requisito de trabalho de todos. A segurança da informação engloba mais do que a segurança de rede e de software, aplicando-se à proteção de informações na forma em que ela é apresentada (impressa ou digital), e sua gestão se torna eficaz com um trabalho integrado nas três perspectivas (tecnológica, pessoas e processos).

Nosso estudo apresentou algumas limitações. Primeiro, embora as escalas que usamos e as relações que encontramos fossem predeterminadas com base na teoria TMP e em outros estudos, os itens do questionário foram traduzidos e adaptados para o contexto das universidades, o que pode ter causado alteração em alguma variável. Segundo, a variável gravidade percebida das sanções contém apenas dois itens para o teste de hipóteses, o que potencialmente pode comprometer a confiabilidade da variável. Uma terceira limitação que podemos considerar é a confiança na intenção comportamental autorrelatada pelo servidor, uma vez que não analisamos o comportamento real.

O impacto social desta pesquisa consiste na contribuição prática de um modelo de comportamento preventivo em segurança da informação aplicado às universidades federais brasileiras, baseado na TMP, o que pode colaborar com a atuação dos profissionais de segurança da informação, não apenas das universidades, no desenvolvimento de estratégias de segurança da informação direcionadas ao comportamento preventivo dos funcionários de distintas organizações.

Referente às reflexões e direcionamentos considerados por esta pesquisa, acredita-se que há necessidade de maiores estudos que apontem outras variáveis relacionadas ao comportamento humano preventivo em segurança da informação, neste sentido, sugerimos associar a TMP com outras teorias comportamentais como, por exemplo, a teoria do comportamento planejado, buscando ampliar o modelo para melhor explicar o comportamento dos servidores das universidades públicas brasileiras. Em segundo lugar, sugerimos a replicação do estudo, em um tamanho de amostra maior que fosse representativo de cada região do Brasil, possibilitando uma comparação entre o comportamento dos servidores por região. Por fim, sugerimos um estudo qualitativo que analise o comportamento real do servidor, a partir da teoria da gestão da informação e do conhecimento, abrangendo ações preventivas e controles relativos ao comportamento humano em segurança da informação. A Figura 23 ilustra o resumo das considerações finais desta pesquisa.

Figura 23 - Considerações finais



Fonte: Elaborado pela autora (2023).

REFERÊNCIAS

ABDALLAH, N.; ABDALLA, O.; ALKHAZALEH, H.; IBRAHIM, A. Information security awareness behavior among higher education students: Case study. **Journal of Theoretical and Applied Information Technology**, *[S. l.]*, v. 8, n. 10, p. 3825–3836, 2020.

ABNT NBR ISO/IEC 27002. **NBR ISO/IEC 27002:** tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro.

AHMAD, A.; DESOUZA, K. C.; MAYNARD, S. B.; NASEER, H.; BASKERVILLE, R. L. How integration of cyber security management and incident response enables organizational learning. **Journal of the Association for Information Science and Technology**, *[S. l.]*, v. 71, n. 8, p. 939–953, 2020. DOI: 10.1002/asi.24311. Disponível em: https://asistdl.onlinelibrary.wiley.com/doi/10.1002/asi.24311. Acesso em 05 jan. 2022.

AHMAD, Z.; ONG, T. S.; LIEW, T. H.; NORHASHIM, M. Security monitoring and information security assurance behaviour among employees: An empirical analysis. **Information and Computer Security**, *[S. l.]*, v. 27, n. 2, p. 165–188, 2019. DOI: 10.1108/ICS-10-2017-0073. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-10-2017-0073/full/html. Acesso em 10 fev. 2022.

AIGBEFO, Q. A.; BLOUNT, Y.; MARRONE, M. The influence of hardiness and habit on security behaviour intention. **Behaviour and Information Technology**, *[S. l.]*, 2020. DOI: 10.1080/0144929X.2020.1856928. Disponível em: https://www.tandfonline.com/doi/full/10.1080/0144929X.2020.1856928. Acesso em 05 jan. 2022.

AJZEN, Icek. The theory of planned behaviour: reactions and reflections. **Psychology & Health**, *[S. l.]*, v. 26, n. 9, p. 1113–1127, 2011. DOI: https://doi.org/10.1080/08870446.2011.613995. Disponível em: http://doi-org.ez15.periodicos.capes.gov.br/10.1080/08870446.2011.613995. Acesso em: 15 dez. 2021.

AL-HARTHY, I. M.; RAHIM, F. A.; ALI, N.; SINGUN, A. P. Dimensions of protection behaviors: A systematic literature review. **Journal of Theoretical and Applied Information Technology**, *[S. l.]*, v. 98, n. 17, p. 3668–3697, 2020. Acesso em 05 jan. 2022.

ALANAZI, S. T.; ANBAR, M.; EBAD, S. A.; KARUPPAYAH, S.; AL-ANI, H. A. Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. **Symmetry**, *[S. l.]*, v. 12, n. 9, 2020. DOI: 10.3390/SYM12091544. Disponível em: https://www.mdpi.com/2073-8994/12/9/1544, Acesso em 05 jan. 2022.

ALEROUD, A.; ABU-SHANAB, E.; AL-AIAD, A.; ALSHBOUL, Y. An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. **Journal of Information Security and Applications**, *[S. l.]*, v. 55, 2020. DOI: 10.1016/j.jisa.2020.102614. Disponível em: https://www.sciencedirect.com/science/article/pii/S2214212620307791?via%3Dihub, Acesso em 05 jan. 2022.

ALI, R. F.; DOMINIC, P. D. D.; ALI, K. Organizational governance, social bonds and information security policy compliance: a perspective towards oil and gas employees. **Sustainability (Switzerland)**, *[S. l.]*, v. 12, n. 20, p. 1–27, 2020. DOI: 10.3390/su12208576. Disponível em: https://www.mdpi.com/2071-1050/12/20/8576. Acesso em 15 jan. 2022.

ALMINDEEL, R.; MARTINS, J. T. Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. **Information Technology and People**, *[S. l.]*, 2020. DOI: 10.1108/ITP-06-2019-0269. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ITP-06-2019-0269/full/html. Acesso em 05 jan. 2022.

ALOTAIBI, M. J.; FURNELL, S.; CLARKE, N. A framework for reporting and dealing with end-user security policy compliance. **Information and Computer Security**, *[S. l.]*, v. 27, n. 1, p. 2–25, 2019. DOI: 10.1108/ICS-12-2017-0097. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2017-0097/full/html. Acesso em 05 jan. 2022.

ALSHAIKH, M. Developing cybersecurity culture to influence employee behavior: A practice perspective. **Computers and Security**, *[S. l.]*, v. 98, 2020. DOI: 10.1016/j.cose.2020.102003. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820302765?via%3Dihub. Acesso em 12 jan. 2022.

ALSHAIKH, M.; ADAMSON, B. From awareness to influence: toward a model for improving employees' security behaviour. **Personal and Ubiquitous Computing**, *[S. l.]*, v. 25, n. 5, p. 829–841, 2021. DOI: 10.1007/s00779-021-01551-2. Disponível em: https://link.springer.com/article/10.1007/s00779-021-01551-2. Acesso em 12 jan. 2022.

ALSHAIKH, M.; MAYNARD, S. B.; AHMAD, A. Applying social marketing to evaluate current security education training and awareness programs in organisations. **Computers and Security**, *[S. l.]*, v. 100, 2021. DOI: 10.1016/j.cose.2020.102090. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820303631?via%3Dihub. Acesso em 12 jan. 2022.

ALSHARE, K. A.; LANE, P. L.; LANE, M. R. Information security policy compliance: a higher education case study. **Information and Computer Security**, *[S. l.]*, v. 26, n. 1, p. 91–108, 2018. DOI: 10.1108/ICS-09-2016-0073. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-09-2016-0073/full/html. Acesso em 05 jan. 2022.

ALYAMI, A.; SAMMON, D.; NEVILLE, K.; MAHONY, C. Exploring IS security themes: a literature analysis. **Journal of Decision Systems**, *[S. l.]*, 2021. DOI: 10.1080/12460125.2020.1848379. Disponível em: https://www.tandfonline.com/doi/full/10.1080/12460125.2020.1848379. Acesso em 12 jan. 2022.

ALZAHRANI, A.; JOHNSON, C. AHP-based Security decision making: How intention and intrinsic motivation affect policy compliance. **International Journal of Advanced Computer Science and Applications**, *[S. l.]*, v. 10, n. 6, p. 1–8, 2019. DOI: 10.14569/ijacsa.2019.0100601. Disponível em:

https://thesai.org/Publications/ViewPaper?Volume=10&Issue=6&Code=IJACSA&SerialNo=1. Acesso em 05 jan. 2022.

ALZAHRANI, L. Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study. **International Journal of Advanced Computer Science and Applications**, *[S. l.]*, v. 12, n. 10, p. 437–447, 2021. DOI: 10.14569/IJACSA.2021.0121049. Disponível em: https://thesai.org/Publications/ViewPaper?Volume=12&Issue=10&Code=IJACSA&SerialNo=49. Acesso em 10 jan. 2022.

AMANKWA, E.; LOOCK, M.; KRITZINGER, E. Establishing information security policy compliance culture in organizations. **Information and Computer Security**, *[S. l.]*, v. 26, n. 4, p. 420–436, 2018. DOI: 10.1108/ICS-09-2017-0063. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-09-2017-0063/full/html. Acesso em: 10 jan. 2021.

AMINI, M.; VAKILIMOFRAD, H.; SABERI, M. K. Human factors affecting information security in libraries. **Bottom Line**, *[S. l.]*, v. 34, n. 1, p. 45–67, 2021. DOI: 10.1108/BL-04-2020-0029. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/BL-04-2020-0029/full/html. Acesso em 20 jan. 2022.

ARAÚJO, C. A. A. de. Fundamentos da CI: correntes teóricas e o conceito de informação. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n.1, p.57-79, jan./jun. 2014.

ARAÚJO, S. G. L. A.; BATISTA, R. R.; ARAÚJO, W. J. Aspectos humanos da segurança da informação. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. ENANCIB 2015, João Pessoa. **Anais** [...]. João Pessoa: UFPB, 2015.

ARAÚJO, S. G. L. A. **A dimensão humana no processo de gestão da segurança da informação:** um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba. 2016. UFPB, João Pessoa, 2016. Dissertação (Mestrado em Ciência da Informação) Universidade Federal da Paraíba , João Pessoa, 2016.

ARAÚJO, S. G. L. A; ARAÚJO, W. J. **Dimensão humana da segurança da informação**. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. ENANCIB 2015, João Pessoa. **Anais** [...] 2016. UFBA, Salvador, 2016.

ARAÚJO, W. J. **Segurança do conhecimento nas práticas da gestão de segurança da informação e da gestão do conhecimento**. 2009. 280 f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2009.

AURIGEMMA, S.; MATTSON, T. Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. **Computers and Security**, *[S. l.]*, v. 66, p. 218–234, 2017. a. DOI: 10.1016/j.cose.2017.02.006. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404817300329?via%3Dihub Acesso em: 10 jan. 2021.

AURIGEMMA, S.; MATTSON, T. Deterrence and punishment experience impacts on ISP compliance attitudes. **Information and Computer Security**, *[S. l.]*, v. 25, n. 4, p. 421–436,

2017. b. DOI: 10.1108/ICS-11-2016-0089. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-11-2016-0089/full/html. Acesso em 20 jan. 2022.

AURIGEMMA, S.; MATTSON, T. Generally speaking, context matters: Making the case for a change from universal to particular ISP research. **Journal of the Association for Information Systems**, *[S. l.]*, v. 20, n. 12, p. 1700–1742, 2019. DOI: 10.17705/1jais.00583. Disponível em: https://aisel.aisnet.org/jais/vol20/iss12/7/. Acesso em 20 jan. 2022.

AURIGEMMA, S.; MATTSON, Thomas. Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. **Computers and Security**, *[S. l.]*, v. 66, p. 218–234, 2017. c. DOI: 10.1016/j.cose.2017.02.006. Disponível em: http://dx.doi.org/10.1016/j.cose.2017.02.006. Acesso em: 10 jan. 2021.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edição 70, 2010.

BARLETTE, Y.; JAOUEN, A. Information security in SMEs: Determinants of CEOs' protective and supportive behaviors. **Systemes d'Information et Management**, *[S. l.]*, v. 24, n. 3, p. 7–40, 2019. DOI: 10.3917/sim.193.0007. Disponível em: https://www.cairn.info/revue-systemes-d-information-et-management-2019-3-page-7.htm?ref=doi. Acesso em: 10 jan. 2021.

BARLOW, J. B.; WARKENTIN, M.; ORMOND, D.; DENNIS, A. R. Don't even think about it! the effects of antineutralization, informational, and normative communication on information security compliance. **Journal of the Association for Information Systems**, *[S. l.]*, v. 19, n. 8, p. 689–715, 2018. DOI: 10.17705/1jais.00506. Disponível em: https://aisel.aisnet.org/jais/vol19/iss8/3/. Acesso em: 15 jan. 2021.

BAUER, S.; BERNROIDER, E. W. N.; CHUDZIKOWSKI, K. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. **Computers and Security**, *[S. l.]*, v. 68, p. 145–159, 2017. DOI: 10.1016/j.cose.2017.04.009. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404817300871?via%3Dihub. Acesso em: 10 jan. 2021.

BAX, S.; MCGILL, T.; HOBBS, V. Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. **Computers and Security**, *[S. l.]*, v. 106, 2021. DOI: 10.1016/j.cose.2021.102278. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404821001024?via%3Dihub.Acesso em: 10 jan. 2021.

BÉLANGER, France; COLLIGNON, Stéphane; ENGET, Kathryn; NEGANGARD, Eric. Determinants of early conformance with information security policies. **Information and Management**, *[S. l.]*, v. 54, n. 7, p. 887–901, 2017. DOI: 10.1016/j.im.2017.01.003. Disponível em: http://dx.doi.org/10.1016/j.im.2017.01.003. Acesso em: 12 jan. 2021.

BERNDTSSON, J.; JOHANSSON, P.; KARLSSON, M. Value conflicts and non-compliance: Attitudes to whistleblowing in Swedish organisations. **Information and Computer Security**, *[S. l.]*, v. 26, n. 2, p. 246–258, 2018. DOI: 10.1108/ICS-08-2017-0057.

Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-08-2017-0057/full/html. Acesso em: 10 jan. 2021.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018 Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação **Diário Oficial [da] República Federativa do Brasil**, Brasil, DF, 2018.

BRASIL. PORTARIA Nº 93, DE 26 DE SETEMBRO DE 2019. Presidência da República. Gabinete de Segurança Institucional. PORTARIA Nº 93, DE 26 DE SETEMBRO DE 2019, Glossário de Segurança da Informação. Brasil, DF, 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em 07 jul. 2022.

BRUIJN, H.; JANSSEN, M. Building Cybersecurity Awareness: The need for evidence-based framing strategies. **Government Information Quarterly**, *[S. l.]*, v. 34, n. 1, p. 1–7, 2017. DOI: 10.1016/j.giq.2017.02.007. Disponível em: https://www.sciencedirect.com/science/article/pii/S0740624X17300540?via%3Dihub. Acesso em: 08 jan. 2021.

BURNS, A. J.; POSEY, C.; ROBERTS, T. L. Insiders' Adaptations to Security-Based Demands in the Workplace: An Examination of Security Behavioral Complexity. **Information Systems Frontiers**, *[S. l.]*, v. 23, n. 2, p. 343–360, 2021. DOI: 10.1007/s10796-019-09951-9. Disponível em: https://link.springer.com/article/10.1007/s10796-019-09951-9. Acesso em: 10 jan. 2021.

BURNS, A. J.; ROBERTS, T. L.; POSEY, C.; BENNETT, R. J.; COURTNEY, J. F. Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. **Decision Sciences**, *[S. l.]*, v. 49, n. 6, p. 1187–1228, 2018. DOI: 10.1111/deci.12304. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/deci.12304. Acesso em: 22 jan. 2021.

CAMARGO, L. S.; BARBOSA, R. R. Bibliometria, cienciometria e um possível caminho para a construção de indicadores e mapas da produção científica. **Ponto de Acesso**, *[S. l.]*, v. 12, p. 109–125, 2018. DOI: DOI: http://dx.doi.org/10.9771/rpa.v12i3.28408. Disponível em: https://portalseer.ufba.br/index.php/revistaici/article/view/28408/18030. Acesso em: 20 ago. 2022.

CANO, M. J. J.; ALMANZA, A. Study of the evolution of information security in Colombia: 2000-2018 | Estudio de la evolución de la seguridad de la información en Colombia: 2000-2018. **RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao**, *[S. l.]*, v. 2020, n. E27, p. 470–483, 2020.

CHEN, H.; CHAU, P. Y. K.; LI, W. The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. **Information Technology and People**, *[S. l.]*, v. 32, n. 4, p. 973–992, 2019. DOI: 10.1108/ITP-12-2017-0421. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ITP-12-2017-0421/full/html. Acesso em: 08 jan. 2021.

CHEN, H.; LI, Y.; CHEN, L.; YIN, J. Understanding employees' adoption of the Bring-Your-

Own-Device (BYOD): the roles of information security–related conflict and fatigue. **Journal of Enterprise Information Management**, *[S. l.]*, 2020. a. DOI: 10.1108/JEIM-10-2019-0318. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/JEIM-10-2019-0318/full/html. Acesso em: 12 jan. 2021.

CHEN, L.; ZHEN, J.; DONG, K.; XIE, Z. Effects of sanction on the mentality of information security policy compliance. **Revista Argentina de Clinica Psicologica**, *[S. l.]*, v. 29, n. 1, p. 39–49, 2020. b. DOI: 10.24205/03276716.2020.6. Disponível em: https://www.revistaclinicapsicologica.com/article.php?doi=10.24205/03276716.2020.6. Acesso em: 12 jan. 2021.

CHEN, X.; CHEN, L.; WU, D. Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. **Journal of Computer Information Systems**, *[S. l.]*, v. 58, n. 4, p. 312–324, 2018. DOI: 10.1080/08874417.2016.1258679. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08874417.2016.1258679. Acesso em: 22 jan. 2021.

CHINYEMBA, M. K.; PHIRI, J. An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector. **Journal of Computer Science**, *[S. l.]*, v. 14, n. 10, p. 1389–1400, 2018. DOI: 10.3844/jcssp.2018.1389.1400. Disponível em: https://thescipub.com/abstract/10.3844/jcssp.2018.1389.1400. Acesso em: 04 jan. 2021.

CHOI, S.; MARTINS, J. T.; BERNIK, I. Information security: Listening to the perspective of organisational insiders. **Journal of Information Science**, *[S. l.]*, v. 44, n. 6, p. 752–767, 2018. DOI: 10.1177/0165551517748288. Disponível em: https://journals.sagepub.com/doi/10.1177/0165551517748288. Acesso em: 12 jan. 2021.

CHOI, Y. Organizational control policy, information security deviance, and moderating effect of power distance orientation: Organizational control policy and information security deviance. **International Journal of Cyber Behavior, Psychology and Learning**, *[S. l.]*, v. 9, n. 3, p. 48–60, 2019. DOI: 10.4018/IJCBPL.2019070104. Disponível em: https://www.igi-global.com/gateway/article/236160 Acesso em: 14 jan. 2021.

CHU, A. M. Y.; SO, M. K. P. Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. **Sustainability (Switzerland)**, *[S. l.]*, v. 12, n. 8, p. 1–25, 2020. DOI: 10.3390/SU12083163. Disponível em: https://www.mdpi.com/2071-1050/12/8/3163 Acesso em: 16 jan. 2021.

CHULKOV, D. V. Escalation of commitment and information security: Theories and implications. **Information and Computer Security**, *[S. l.]*, v. 25, n. 5, p. 580–592, 2017. DOI: 10.1108/ICS-02-2016-0015. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049889835&doi=10.1108%2fICS-09-2017-.0066&partnerID=40&md5=062867c0144b032238c7a8a311ec4f58. Acesso em: 12 jan. 2022.

CONNOLLY, L. Y.; LANG, M.; WALL, D. S. Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. **Information Systems Management**, *[S.*

l.], v. 36, n. 4, p. 306–322, 2019. DOI: 10.1080/10580530.2019.1651113. Disponível em: https://www.tandfonline.com/doi/full/10.1080/10580530.2019.1651113. Acesso em: 14 jan. 2021.

CONNOLLY, Lena Yuryna; LANG, Michael; GATHEGI, John; TYGAR, Doug J. Organisational culture, procedural countermeasures, and employee security behaviour A qualitative study. **Information and Computer Security**, *[S. l.]*, v. 25, n. 2, p. 118–136, 2017. DOI: 10.1108/ICS-03-2017-0013. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020694854&doi=10.1108%2fICS-03-2017-0013&partnerID=40&md5=ab5856280edc71ab817c5cf6be713d91. Acesso em: 05 jan. 2022.

CROSSLER, R. E.; BÉLANGER, F.; ORMOND, D. The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. **Information Systems Frontiers**, *[S. l.]*, v. 21, n. 2, p. 343–357, 2019. DOI: 10.1007/s10796-017-9755-1. Disponível em: https://link.springer.com/article/10.1007/s10796-017-9755-1, Acesso em: 12 jan. 2022.

D'ARCY, J.; LOWRY, P. B. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. **Information Systems Journal**, *[S. l.]*, v. 29, n. 1, p. 43–69, 2019. DOI: 10.1111/isj.12173. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/isj.12173. Acesso em: 05 jan. 2022.

DANG-PHAM, D.; PITTAYACHAWAN, S.; BRUNO, V. Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. **Computers and Security**, *[S. l.]*, v. 68, p. 1–15, 2017. a. DOI: 10.1016/j.cose.2017.03.010. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85016474700&doi=10.1016%2fj.cose.2017.03.010&partnerID=40&md5=06d740be68aecb1794eb8d5eeff08549. Acesso em: 12 jan. 2022.

DANG-PHAM, D.; PITTAYACHAWAN, S.; BRUNO, V. Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace. **Information and Management**, *[S. l.]*, v. 54, n. 5, p. 625–637, 2017. b. DOI: 10.1016/j.im.2016.12.003. Disponível em: https://www.sciencedirect.com/science/article/pii/S0378720616303858?via%3Dihub. Acesso em: 18 jan. 2022.

DANG-PHAM, Duy; PITTAYACHAWAN, Siddhi; BRUNO, Vince. Exploring behavioral information security networks in an organizational context: An empirical case study. **Journal of Information Security and Applications**, *[S. l.]*, v. 34, p. 46–62, 2017. c. DOI: 10.1016/j.jisa.2016.06.002. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84979644230&doi=10.1016%2fj.jisa.2016.06.002&partnerID=40&md5=15a4814700b77cb0b9f9fe1ff1664562. Acesso em: 10 jan. 2022.

DAVIS, J.; AGRAWAL, D.; GUO, X. Enhancing users' security engagement through cultivating commitment: the role of psychological needs fulfilment. **European Journal of Information Systems**, *[S. l.]*, 2021. DOI: 10.1080/0960085X.2021.1927866. Disponível em: https://www.tandfonline.com/doi/full/10.1080/0960085X.2021.1927866

DEBB, S. M.; MCCLELLAN, M. K. Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. **Cyberpsychology, Behavior, and Social Networking**, *[S. l.]*, v. 24, n. 9, p. 605–611, 2021. DOI: 10.1089/cyber.2021.0043. Disponível em: https://www.liebertpub.com/doi/10.1089/cyber.2021.0043. Acesso em: 18 jan. 2022.

DOHERTY, N. F.; TAJUDDIN, S. T. Towards a user-centric theory of value-driven information security compliance. **Information Technology and People**, *[S. l.]*, v. 31, n. 2, p. 348–367, 2018. DOI: 10.1108/ITP-08-2016-0194. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044586438&doi=10.1108%2fITP-08-2016-0194&partnerID=40&md5=b77e25254bf6f4478d8d356788c4b3b9. Acesso em: 12 jan. 2022.

DONG, K.; ALI, R. F.; DOMINIC, P. D. D.; ALI, S. E. A. The effect of organizational information security climate on information security policy compliance: the mediating effect of social bonding towards healthcare nurses. **Sustainability (Switzerland)**, *[S. l.]*, v. 13, n. 5, p. 1–25, 2021. DOI: 10.3390/su13052800. Disponível em: https://www.mdpi.com/2071-1050/13/5/2800. Acesso em: 18 jan. 2022.

FARSHADKHAH, S.; VAN SLYKE, C.; FULLER, B. Onlooker effect and affective responses in information security violation mitigation. **Computers and Security**, *[S. l.]*, v. 100, 2021. DOI: 10.1016/j.cose.2020.102082. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820303552?via%3Dihub. Acesso em: 22 jan. 2022.

FÁVERO, L. P.; BELFIORE, P. **Manual de Análise de Dados -Estatística e Modelagem Multivariada com Excel, SPSS e Stata**. 1. ed. Rio: Elsevier, 2017. Disponível em: http://dergipark.gov.tr/cumusosbil/issue/4345/59412.

FENG, G.; ZHU, J.; WANG, N.; LIANG, H. How paternalistic leadership influences it security policy compliance: The mediating role of the social bond. **Journal of the Association for Information Systems**, *[S. l.]*, v. 20, n. 11, p. 1650–1691, 2019. DOI: 10.17705/1jais.00581. Disponível em: https://aisel.aisnet.org/jais/vol20/iss11/2/. Acesso em: 18 jan. 2022.

FLORES, W. R.; EKSTEDT, M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. **Computers and Security**, *[S. l.]*, v. 59, p. 26–44, 2016. a. DOI: 10.1016/j.cose.2016.01.004. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404816000067?via%3Dihub. Acesso em: 05 jan. 2022.

FLOYD, D. L.; PRENDICE-DUNN, S.; ROGERS, R. W. A Meta-Analysis o. **Journal of applied social psychology**, *[S. l.]*, v. 30, p. 407–429, 2000. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.2000.tb02323.x. Acesso em: 12 jan. 2022.

FONTES, Edison Luiz Goncalves. **Segurança da informação: o usuário faz a diferença**. São Paulo: Saraiva, 2016.

FORTIN, M. F. **O processo de investigação - Fortin.pdf**. Loures: Edições Técnicas e

Científicas Lda., 1999.

GANGIRE, Y.; VEIGA, A.; HERSELMAN, M. Assessing information security behaviour: a self-determination theory perspective. **Information and Computer Security**, *[S. l.]*, v. 29, n. 4, p. 625–646, 2021. DOI: 10.1108/ICS-11-2020-0179. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-11-2020-0179/full/html. Acesso em: 18 jan. 2022.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2012.

GRIMES, M.; MARQUARDSON, J. Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. **Decision Support Systems**, *[S. l.]*, v. 119, p. 23–34, 2019. DOI: 10.1016/j.dss.2019.02.010. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167923619300387?via%3Dihub. Acesso em: 22 jan. 2022.

GUAN, B.; HSU, C. The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. **Internet Research**, *[S. l.]*, v. 30, n. 5, p. 1383–1405, 2020. DOI: 10.1108/INTR-06-2019-0260. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/INTR-06-2019-0260/full/html. Acesso em: 05 jan. 2022.

GUHR, N.; LEBEK, B.; BREITNER, M. H. The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. **Information Systems Journal**, *[S. l.]*, v. 29, n. 2, p. 340–362, 2019. DOI: 10.1111/isj.12202. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/isj.12202. Acesso em: 18 jan. 2022.

GWEBU, K. L.; WANG, J.; HU, M. Y. Information security policy noncompliance: An integrative social influence model. **Information Systems Journal**, *[S. l.]*, v. 30, n. 2, p. 220–269, 2020. DOI: 10.1111/isj.12257. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/isj.12257. Acesso em: 08 jan. 2022.

HAAG, S.; SIPONEN, M.; LIU, F. Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. **Data Base for Advances in Information Systems**, *[S. l.]*, v. 52, n. 2, p. 25–67, 2021. DOI: 10.1145/3462766.3462770. Disponível em: https://dl.acm.org/doi/10.1145/3462766.3462770. Acesso em: 18 jan. 2022.

HADLINGTON, L. Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. **International Journal of Cyber Criminology**, *[S. l.]*, v. 12, n. 1, p. 269–281, 2018. DOI: 10.5281/zenodo.1467909. Acesso em: 22 jan. 2022.

HADLINGTON, L.; BINDER, J.; STANULEWICZ, N. Fear of Missing out Predicts Employee Information Security Awareness above Personality Traits, Age, and Gender. **Cyberpsychology, Behavior, and Social Networking**, *[S. l.]*, v. 23, n. 7, p. 459–464, 2020. DOI: 10.1089/cyber.2019.0703. Disponível em: https://zenodo.org/record/1467909#.ZAkreXbMK00. Acesso em: 08 jan. 2022.

HADLINGTON, L.; BINDER, J.; STANULEWICZ, N. Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. **Computers in Human Behavior**, *[S. l.]*, v. 114, 2021. DOI: 10.1016/j.chb.2020.106557. Disponível em: https://www.sciencedirect.com/science/article/pii/S0747563220303071?via%3Dihub. Acesso em: 18 jan. 2022.

HADLINGTON, L.; POPOVAC, M.; JANICKE, H.; YEVSEYEVA, I.; JONES, K. Exploring the role of work identity and work locus of control in information security awareness. **Computers and Security**, *[S. l.]*, v. 81, p. 41–48, 2019. DOI: 10.1016/j.cose.2018.10.006. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404818308897?via%3Dihub. Acesso em: 29 jan. 2022.

HADLINGTON, Lee; PARSONS, Kathryn. Can Cyberloafing and Internet Addiction Affect Organizational Information Security? **Cyberpsychology, Behavior, and Social Networking**, *[S. l.]*, v. 20, n. 9, p. 567–571, 2017. DOI: 10.1089/cyber.2017.0239. Disponível em: https://www.liebertpub.com/doi/10.1089/cyber.2017.0239. Acesso em: 14 jan. 2022.

HAIR, J. F. J.; BLACK, W. C.; BABIN, B. J.; ANDERSON, R. E.; TATHAM, R. L. **Análise multivariada de dados**. 6. ed. Porto Alegre: Bookman, 2009. v. 232

HAMID, H. A.; YUSOF, M. M.; DALI, N. R. S. M. The influence of security control management and social factors in deterring security misbehaviour. **International Journal of Recent Technology and Engineering**, *[S. l.]*, v. 8, n. 1, p. 144–150, 2019. Disponível em: https://oarep.usim.edu.my/jspui/handle/123456789/1369

HE, W.; ASH, I.; ANWAR, M.; LI, L.; YUAN, X.; XU, L.; TIAN, X. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. **Journal of Intellectual Capital**, *[S. l.]*, v. 21, n. 2, p. 203–213, 2019. DOI: 10.1108/JIC-05-2019-0112. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/JIC-05-2019-0112/full/html. Acesso em: 06 jan. 2022.

HINA, S.; SELVAM, D. D. D. P.; LOWRY, P. B. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. **Computers and Security**, *[S. l.]*, v. 87, 2019. DOI: 10.1016/j.cose.2019.101594. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404818308320?via%3Dihub, Acesso em: 14 jan. 2022.

HONG, Y.; FURNELL, S. Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. **Journal of Computer Information Systems**, *[S. l.]*, 2019. DOI: 10.1080/08874417.2019.1683781. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08874417.2019.1683781. Acesso em: 05 jan. 2022.

HOOPER, V.; BLUNT, C. Factors influencing the information security behaviour of IT employees. **Behaviour and Information Technology**, *[S. l.]*, v. 39, n. 8, p. 862–874, 2020. DOI: 10.1080/0144929X.2019.1623322. Disponível em: https://www.tandfonline.com/doi/full/10.1080/0144929X.2019.1623322. Acesso em: 06 jan.

2022.

HOUSE, D.; RAJA, M. K. Phishing: message appraisal and the exploration of fear and self-confidence. **Behaviour and Information Technology**, *[S. l.]*, v. 39, n. 11, p. 1204–1224, 2020. DOI: 10.1080/0144929X.2019.1657180. Disponível em: https://www.tandfonline.com/doi/full/10.1080/0144929X.2019.1657180. Acesso em: 28 jan. 2022.

HWANG, I.; KIM, D.; KIM, T.; KIM, S. Why not comply with information security? An empirical approach for the causes of non-compliance. **Online Information Review**, *[S. l.]*, v. 41, n. 1, p. 2–18, 2017. a. DOI: 10.1108/OIR-11-2015-0358. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85010904453&doi=10.1108%2fOIR-11-2015-0358&partnerID=40&md5=d974659502c5a4bb6c5877bb936df85c. Acesso em: 08 jan. 2021.

HWANG, I.; KIM, S.; REBMAN, C. Impact of regulatory focus on security technostress and organizational outcomes: the moderating effect of security technostress inhibitors. **Information Technology and People**, *[S. l.]*, 2021. DOI: 10.1108/ITP-05-2019-0239. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ITP-05-2019-0239/full/html. Acesso em: 18 jan. 2022.

HWANG, I.; WAKEFIELD, R.; KIM, S.; KIM, T. Security Awareness: The First Step in Information Security Compliance Behavior. **Journal of Computer Information Systems**, *[S. l.]*, v. 61, n. 4, p. 345–356, 2021. DOI: 10.1080/08874417.2019.1650676. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08874417.2019.1650676. Acesso em: 24 jan. 2022.

IBM SECURITY. **Relátorio de Custo da Violação de Dados 2022**. [s.l: s.n.]. Disponível em: https://www.ibm.com/security/data-breach.

ISACA, INFORMATION SYSTEMS AUDITAND CONTROL ASSOCIATION. **COBIT 5 for Information Security.** Rolling Meadows, 2012. Disponível em: https://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf.

ISO/IEC 27000. **INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. ISO/IEC 27000: information technology:** security techniques: information security management systems: overview and vocabulary , 2014.

JAEGER, L.; ECKHARDT, A. Eyes wide open: The role of situational information security awareness for security-related behaviour. **Information Systems Journal**, *[S. l.]*, 2020. DOI: 10.1111/isj.12317. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/isj.12317. Acesso em: 05 jan. 2022.

JANSEN, J.; VAN SCHAIK, P. Comparing three models to explain precautionary online behavioural intentions. **Information and Computer Security**, *[S. l.]*, v. 25, n. 2, p. 165–180, 2017. DOI: 10.1108/ICS-03-2017-0018. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020724766&doi=10.1108%2fICS-03-2017-0018&partnerID=40&md5=e9abe67c1ae47a2c9bea31017cafc120. Acesso em: 08 jan. 2022.

JANSEN, J.; VAN SCHAIK, P. Testing a model of precautionary online behaviour: The case of online banking. **Computers in Human Behavior**, *[S. l.]*, v. 87, p. 371–383, 2018. a. DOI: 10.1016/j.chb.2018.05.010. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049317489&doi=10.1016%2fj.chb.2018.05.010&partnerID=40&md5=a4a44aa1cd3753248244d47c5844a606. Acesso em: 10 jan. 2022.

JANSEN, J.; VAN SCHAIK, P. Persuading end users to act cautiously online: a fear appeals study on phishing. **Information and Computer Security**, *[S. l.]*, v. 26, n. 3, p. 264–276, 2018. b. DOI: 10.1108/ICS-03-2018-0038. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2018-0038/full/html. Acesso em: 14 jan. 2022.

JANSEN, J.; VAN SCHAIK, P. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. **International Journal of Human Computer Studies**, *[S. l.]*, v. 123, p. 40–55, 2019. DOI: 10.1016/j.ijhcs.2018.10.004. Disponível em: https://www.sciencedirect.com/science/article/pii/S1071581918306293?via%3Dihub. Acesso em: 08 jan. 2022.

JANSEN, Jurjen; VEENSTRA, Sander; ZUURVEEN, Renske; STOL, Wouter. Guarding against online threats : why entrepreneurs take protective measures. **Behaviour & Information Technology**, *[S. l.]*, v. 3001, 2016. DOI: 10.1080/0144929X.2016.1160287. Disponível em: https://www.tandfonline.com/doi/full/10.1080/0144929X.2016.1160287

JIANG, H.; TSOHOU, A.; SIPONEN, M.; LI, Y. Examining the side effects of organizational Internet monitoring on employees. **Internet Research**, *[S. l.]*, v. 30, n. 6, p. 1613–1630, 2020. DOI: 10.1108/INTR-08-2019-0360. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/INTR-08-2019-0360/full/html. Acesso em: 14 jan. 2022.

JOHNSTON, A. C.; WARKENTIN, M.; DENNIS, A. R.; SIPONEN, M. Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. **Decision Sciences**, *[S. l.]*, v. 50, n. 2, p. 245–284, 2019. DOI: 10.1111/deci.12328. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/deci.12328. Acesso em: 05 jan. 2022.

KARJALAINEN, M.; SIPONEN, M.; SARKER, S. Toward a stage theory of the development of employees' information security behavior. **Computers and Security**, *[S. l.]*, v. 93, 2020. DOI: 10.1016/j.cose.2020.101782. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820300675?via%3Dihub. Acesso em: 14 jan. 2022.

KEARNEY, W. D.; KRUGER, H. A. Can perceptual differences account for enigmatic information security behaviour in an organisation? **Computers and Security**, *[S. l.]*, v. 61, p. 46–58, 2016. DOI: 10.1016/j.cose.2016.05.006. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404816300645?via%3Dihub

KHAN, H. U.; ALSHARE, K. A. Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. **Journal of Organizational**

Computing and Electronic Commerce, *[S. l.]*, v. 29, n. 1, p. 4–23, 2019. DOI: 10.1080/10919392.2019.1552743. Disponível em: https://www.tandfonline.com/doi/full/10.1080/10919392.2019.1552743. Acesso em: 22 jan. 2022.

KHATIB, R.; BARKI, H. How different rewards tend to influence employee non-compliance with information security policies. **Information and Computer Security**, *[S. l.]*, 2021. DOI: 10.1108/ICS-01-2021-0008. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-01-2021-0008/full/html. Acesso em: 12 jan. 2022.

KI-ARIES, D.; FAILY, S. Persona-centred information security awareness. **Computers and Security**, *[S. l.]*, v. 70, p. 663–674, 2017. DOI: 10.1016/j.cose.2017.08.001. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404817301566?via%3Dihub. Acesso em: 14 jan. 2022.

KIM, B.; LEE, D. Y.; KIM, B. Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. **Behaviour and Information Technology**, *[S. l.]*, v. 39, n. 11, p. 1156–1175, 2020. DOI: 10.1080/0144929X.2019.1653992. Disponível em: https://www.tandfonline.com/doi/full/10.1080/0144929X.2019.1653992. Acesso em: 14 jan. 2022.

KIM, H. L.; HAN, J. Do employees in a “good” company comply better with information security policy? A corporate social responsibility perspective. **Information Technology and People**, *[S. l.]*, v. 32, n. 4, p. 858–875, 2019. DOI: 10.1108/ITP-09-2017-0298. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ITP-09-2017-0298/full/html. Acesso em: 06 jan. 2022.

KIM, S. S.; KIM, Y. J. The effect of compliance knowledge and compliance support systems on information security compliance behavior. **Journal of Knowledge Management**, *[S. l.]*, v. 21, n. 4, p. 986–1010, 2017. DOI: 10.1108/JKM-08-2016-0353. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/JKM-08-2016-0353/full/html. Acesso em: 14 jan. 2022.

KITCHENHAM, B.; BRERETON, O. P.; BUDGEN, D.; TURNER, M.; BAILEY, J.; LINKMAN, S.. Systematic literature reviews in software engineering – A systematic literature review. **Information and Software Technology**, *[S. l.]*, v. 51, n. 1, p. 7–15, 2009. DOI: 10.1016/j.infsof.2008.09.009. Disponível em: http://dx.doi.org/10.1016/j.infsof.2008.09.009. Acesso em: 12 setembro. 2021.

KOLOSENI, D. N.; LEE, C. Y.; GAN, M. L. Understanding information security behaviours of Tanzanian government employees: A health belief model perspective. **International Journal of Technology and Human Interaction**, *[S. l.]*, v. 15, n. 1, p. 15–32, 2019. DOI: 10.4018/IJTHI.2019010102 Disponível em: https://www.igi-global.com/gateway/article/214928. Acesso em: 14 jan. 2022.

KOOHANG, A.; NORD, J. H.; SANDOVAL, Z. V.; PALISZKIEWICZ, J. Reliability, Validity, and Strength of a Unified Model for Information Security Policy Compliance. **Journal of Computer Information Systems**, *[S. l.]*, 2020. DOI:

10.1080/08874417.2020.1779151. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1779151. Acesso em: 14 jan. 2022.

LANDIS, J. R;; KOCH, G. G. An application of hierarchical kappa-type statistics in the assessment of majority agreement among multiple observers. **Biometrics**, *[S. l.]*, p. 363–374, 1977. Disponível em: https://www.jstor.org/stable/2529786?origin=crossref. Acesso em: 07 jul. 2022.

LANKTON, N. K.; STIVASON, C.; GURUNG, A. Information protection behaviors: morality and organizational criticality. **Information and Computer Security**, *[S. l.]*, v. 27, n. 3, p. 468–488, 2019. DOI: 10.1108/ICS-07-2018-0092. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2018-0092/full/html. Acesso em: 14 jan. 2022.

LEERING, A.; VAN DE WIJNGAERT, L.; NIKOU, S. More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors. **Behaviour and Information Technology**, *[S. l.]*, 2020. DOI: 10.1080/0144929X.2020.1822444. Disponível em: https://www.tandfonline.com/doi/full/10.1080/0144929X.2020.1822444. Acesso em: 08 jan. 2022.

LEMAY, D. J.; BASNET, R. B.; DOLECK, T. Examining the relationship between threat and coping appraisal in phishing detection among college students. **Journal of Internet Services and Information Security**, *[S. l.]*, v. 10, n. 1, p. 38–49, 2020. DOI: 10.22667/JISIS.2020.02.29.038. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://isyou.info/jisis/vol10/no1/jisis-2020-vol10-no1-03.pdf. Acesso em: 30 jan. 2022.

LETICA, I. B. Some correlates of risky user behavior and ICT security awareness of secondary school students. **International Journal of Electrical and Computer Engineering Systems**, *[S. l.]*, v. 10, n. 2, p. 85–89, 2019. DOI: 10.32985/ijeces.10.2.4. Disponível em: http://www.etfos.unios.hr/ijeces/papers/some-correlates-of-risky-user-behavior-and-ict-security-awareness-of-secondary-school-students/. Acesso em: 06 jan. 2022.

LI, L.; HE, W.; XU, L.; ASH, I.; ANWAR, M.; YUAN, X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. **International Journal of Information Management**, *[S. l.]*, v. 45, p. 13–24, 2019. DOI: 10.1016/j.ijinfomgt.2018.10.017. Disponível em: https://www.sciencedirect.com/science/article/pii/S0268401218302093?via%3Dihub. Acesso em: 14 jan. 2022.

LIU, C.; WANG, N.; LIANG, H. Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. **International Journal of Information Management**, *[S. l.]*, v. 54, 2020. DOI: 10.1016/j.ijinfomgt.2020.102152. Disponível em: https://www.sciencedirect.com/science/article/pii/S0268401219302877?via%3Dihub. Acesso em: 14 jan. 2022.

MAKERI, Y. A. The strategy detection on information security in corporate organizations on crucial asset. **International Journal on Informatics Visualization**, *[S. l.]*, v. 4, n. 1, p. 35–

39, 2020. DOI: 10.30630/joiv.4.1.280. Disponível em: http://joiv.org/index.php/joiv/article/view/280. Acesso em: 30 jan. 2022.

MALATJI, M.; MARNEWICK, A.; VON SOLMS, S. Validation of a socio-technical management process for optimising cybersecurity practices. **Computers and Security**, *[S. l.]*, v. 95, 2020. DOI: 10.1016/j.cose.2020.101846. Disponível em: https://www.sciencedirect.com/science/article/pii/S016740482030119X?via%3Dihub. Acesso em: 08 jan. 2022.

MAMONOV, S.; BENBUNAN-FICH, R. The impact of information security threat awareness on privacy-protective behaviors. **Computers in Human Behavior**, *[S. l.]*, v. 83, p. 32–44, 2018. DOI: 10.1016/j.chb.2018.01.028. Disponível em: https://www.sciencedirect.com/science/article/pii/S0747563218300347?via%3Dihub Acesso em: 03 fev. 2022.

MARCHAND, P. RATINAUD, P.. Les primaires socialistes pour l'élection présidentielle française (septembre-octobre 2011). **L'analyse de similitude appliquée aux corpus textuels**, *[S. l.]*, p. 687–699, 2012.

MCCORMAC, A.; CALIC, D.; PARSONS, K.; BUTAVICIUS, M.; PATTINSON, M.; LILLIE, M. The effect of resilience and job stress on information security awareness. **Information and Computer Security**, *[S. l.]*, v. 26, n. 3, p. 277–289, 2018. DOI: 10.1108/ICS-03-2018-0032. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2018-0032/full/html. Acesso em: 28 jan. 2022.

MCCORMAC, A.; ZWAANS, T.; PARSONS, K.; CALIC, D.; BUTAVICIUS, M.; PATTINSON, M. Individual differences and Information Security Awareness. **Computers in Human Behavior**, *[S. l.]*, v. 69, p. 151–156, 2017. a. DOI: 10.1016/j.chb.2016.11.065. Disponível em: http://dx.doi.org/10.1016/j.chb.2016.11.065. Acesso em: 05 jan. 2021.

MCGILL, T.; THOMPSON, N. Exploring potential gender differences in information security and privacy. **Information and Computer Security**, *[S. l.]*, v. 29, n. 5, p. 850–865, 2021. DOI: 10.1108/ICS-07-2020-0125. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2020-0125/full/html. Acesso em: 28 jan. 2022.

MD AZMI, N. A. A.; TEOH, A. P.; VAFAEI-ZADEH, A.; HANIFAH, H. Predicting information security culture among employees of telecommunication companies in an emerging market. **Information and Computer Security**, *[S. l.]*, v. 29, n. 5, p. 866–882, 2021. DOI: 10.1108/ICS-02-2021-0020. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-02-2021-0020/full/html. Acesso em: 05 jan. 2022.

MENARD, P.; BOTT, G. J.; CROSSLER, R. E. User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. **Journal of Management Information Systems**, *[S. l.]*, v. 34, n. 4, p. 1203–1230, 2017. DOI: 10.1080/07421222.2017.1394083. Disponível em: https://www.tandfonline.com/doi/full/10.1080/07421222.2017.1394083. Acesso em: 08 jan. 2022.

MENARD, Philip; WARKENTIN, Merrill; LOWRY, Paul Benjamin. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. **Computers and Security**, *[S. l.]*, v. 75, p. 147–166, 2018. DOI: 10.1016/j.cose.2018.01.020. Disponível em: https://doi.org/10.1016/j.cose.2018.01.020.Acesso em: 12 jan. 2022.

MERHI, M. I.; AHLUWALIA, P. Examining the impact of deterrence factors and norms on resistance to Information Systems Security. **Computers in Human Behavior**, *[S. l.]*, v. 92, p. 37–46, 2019. DOI: 10.1016/j.chb.2018.10.031. Disponível em: https://www.sciencedirect.com/science/article/pii/S0747563218305211?via%3Dihub. Acesso em: 14 jan. 2022.

MERMOUD, A.; KEUPP, M. M.; HUGUENIN, K.; PALMIÉ, M.; PERCIA DAVID, D. To share or not to share: A behavioral perspective on human participation in security information sharing. **Journal of Cybersecurity**, *[S. l.]*, v. 5, n. 1, 2019. DOI: 10.1093/cybsec/tyz006. Disponível em: https://academic.oup.com/cybersecurity/article/5/1/tyz006/5554880?login=true. Acesso em: 05 jan. 2022.

MUTCHLER, L. A. Response awareness and instructional self-efficacy: influences on intent. **Information and Computer Security**, *[S. l.]*, v. 26, n. 4, p. 489–507, 2019. DOI: 10.1108/ICS-05-2018-0061. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-05-2018-0061/full/html. Acesso em: 14 jan. 2022.

NASIRPOURI S., F.; BIROS, D. Understanding Employee Information Security Policy Compliance from Role Theory Perspective. **Journal of Computer Information Systems**, *[S. l.]*, v. 61, n. 6, p. 571–580, 2021. DOI: 10.1080/08874417.2020.1845584. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1845584. Acesso em: 08 jan. 2022.

NEL, F.; DREVIN, L. Key elements of an information security culture in organisations. **Information and Computer Security**, *[S. l.]*, v. 27, n. 2, p. 146–164, 2019. DOI: 10.1108/ICS-12-2016-0095. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2016-0095/full/html Acesso em: 22 jan. 2022.

NOOR, M. U. Indonesian millennial awareness to privacy and personal data protection on the internet. **DESIDOC Journal of Library and Information Technology**, *[S. l.]*, v. 40, n. 2, p. 431–436, 2020. DOI: 10.14429/djlit.40.02.14969. Disponível em: https://publications.drdo.gov.in/ojs/index.php/djlit/article/view/14969. Acesso em: 14 jan. 2022.

OGBANUFE, O. Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. **Computers and Security**, *[S. l.]*, v. 108, 2021. DOI: 10.1016/j.cose.2021.102340. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404821001644?via%3Dihub Acesso em: 30 jan. 2022.

OGBANUFE, O.; CROSSLER, R. E.; BIROS, D. Exploring stewardship: A precursor to voluntary security behaviors. **Computers and Security**, *[S. l.]*, v. 109, 2021. DOI: 10.1016/j.cose.2021.102397. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404821002212?via%3Dihub, Acesso em: 05 jan. 2022.

ORAZI, D. C.; JOHNSTON, A. C.; WARKENTIN, M. Integrating construal-level theory in designing fear appeals in IS security research. **Communications of the Association for Information Systems**, *[S. l.]*, v. 45, n. 1, p. 397–410, 2019. DOI: 10.17705/1CAIS.04522. Disponível em: https://aisel.aisnet.org/cais/vol45/iss1/22/. Acesso em: 15 jan. 2022.

PARDAL, Luís; LOPES, Eugênia soares. **Métodos e técnicas de investigação social**. Porto - Portugal: Areal, 2011.

PARK, E. H.; KIM, J.; WILES, L. L.; PARK, Y. S. Factors affecting intention to disclose patients' health information. **Computers and Security**, *[S. l.]*, v. 87, 2019. DOI: 10.1016/j.cose.2018.05.003. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404818304917?via%3Dihub. Acesso em: 30 jan. 2022.

PARK, M.; CHAI, S. Comparing the effects of two methods of education (online versus offline) and gender on information security behaviors. **Asia Pacific Journal of Information Systems**, *[S. l.]*, v. 30, n. 2, p. 308–327, 2020. DOI: 10.14329/apjis.2020.30.2.308. Disponível em: http://www.apjis.or.kr/common/sub/currentissue_view.asp?UID=5188&GotoPage=1. Acesso em: 30 jan. 2022.

PARSONS, K.; CALIC, D.; PATTINSON, M.; BUTAVICIUS, Ms; MCCORMAC, A.; ZWAANS, T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. **Computers and Security**, *[S. l.]*, v. 66, p. 40–51, 2017. DOI: 10.1016/j.cose.2017.01.004. Disponível em: http://dx.doi.org/10.1016/j.cose.2017.01.004. Acesso em: 10 out. 2021.

PATTINSON, M.; BUTAVICIUS, M.; LILLIE, M.; CICCARELLO, B.; PARSONS, K.; CALIC, D.; MCCORMAC, A. Matching training to individual learning styles improves information security awareness. **Information and Computer Security**, *[S. l.]*, v. 28, n. 1, p. 1–14, 2019. DOI: 10.1108/ICS-01-2019-0022. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-01-2019-0022/full/html. Acesso em: 20 fev. 2022.

PESTANA, M. H.; GAGEIRO, J. N. **Análise de dados para ciências sociais:** a complementaridade do SPSS. Lisboa: Sílabo, 2008.

PORTE, M.S.; TRINDADE, J. D. R.. Barreiras tecnológicas : um fator limitador na acessibilidade das pessoas com deficiência Technological barriers : a limiting factor in the accessibility of people with disabilities. *[S. l.]*, p. 1–18, 2019. DOI: 10.35699/1983-3652.2021.32563.

PORTE, Marcelo; SAUR-AMARAL, Irina. Pesquisa em auditoria : principais temas *. *[S. l.]*, p. 41–59, 2018. DOI: 10.1590/1808-057x201804410. Disponível em:

https://periodicos.ufmg.br/index.php/textolivre/article/view/32563, Acesso em: 22 jan. 2022.

QAZI, W.; RAZA, S. A.; KHAN, K. A. The contradiction between self-protection and self-presentation on knowledge sharing behaviour: Evidence from higher education students in Pakistan. **International Journal of Knowledge and Learning**, *[S. l.]*, v. 13, n. 3, p. 246–271, 2020. DOI: 10.1504/IJKL.2020.109910. Disponível em: https://ideas.repec.org/a/ids/ijklea/v13y2020i3p246-271.html. Acesso em: 14 jan. 2022.

RAJAB, M.; EYDGAHI, A. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. **Computers and Security**, *[S. l.]*, v. 80, p. 211–223, 2019. DOI: 10.1016/j.cose.2018.09.016. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404818311325?via%3Dihub. Acesso em: 18 jan. 2022.

REINERT, M. Alceste une méthodologie d'analyse des données textuelles et une application: Aurelia De Gerard De Nerval. **Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique**, *[S. l.]*, v. 26, n.1, p. 24–54, 1990. Disponível em: https://journals.sagepub.com/doi/10.1177/075910639002600103, Acesso em: 08 jan. 2022.

RICHARDSON, Roberto Jarry. **Pesquisa social: métodos e técnicas**. 3. ed. São Paulo: Atlas, 2009.

ROGERS, Ronald W. A protection motivation theory of fear appeals and attitude change. **The journal of psychology**, *[S. l.]*, v. 91, n. 1, p. 93–114, 1975.

ROGERS, Ronald W. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. **Social psychophysiology: A sourcebook**, *[S. l.]*, p. 153–176, 1983. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/00223980.1975.9915803. Acesso em: 30 jan. 2022.

SAFA, N. S.; MAPLE, C. Human errors in the information security realm – and how to fix them. **Computer Fraud and Security**, *[S. l.]*, v. 2016, n. 9, p. 17–20, 2016. DOI: 10.1016/S1361-3723(16)30073-2. Disponível em: https://www.sciencedirect.com/science/article/pii/S1361372316300732?via%3Dihub. Acesso em: 14 jan. 2022.

SAFA, N. S.; MAPLE, C.; FURNELL, S.; AZAD, M. A.; PERERA, C.; DABBAGH, M.; SOOKHAK, M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. **Future Generation Computer Systems**, *[S. l.]*, v. 97, p. 587–597, 2019. DOI: 10.1016/j.future.2019.03.024. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X18331285?via%3Dihub. Acesso em: 30 jan. 2022.

SAFA, N. S.; MAPLE, C.; WATSON, T.; FURNELL, S. Information security collaboration formation in organisations. **IET Information Security**, *[S. l.]*, v. 12, n. 3, p. 238–245, 2018. a. DOI: 10.1049/iet-ifs.2017.0257. Disponível em: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ifs.2017.0257. Acesso em: 14 jan. 2022.

SAFA, N. S.; MAPLE, C.; WATSON, T.; VON SOLMS, R. Motivation and opportunity based model to reduce information security insider threats in organisations. **Journal of Information Security and Applications**, *[S. l.]*, v. 40, p. 247–257, 2018. b. DOI: 10.1016/j.jisa.2017.11.001. Disponível em: https://www.sciencedirect.com/science/article/pii/S2214212617302600?via%3Dihub. Acesso em: 08 jan. 2022.

SAFA, N. S.; SOOKHAK, M.; VON SOLMS, R.; FURNELL, S.; GHANI, N. A.; HERAWAN, T. Information security conscious care behaviour formation in organizations. **Computers & Security**, *[S. l.]*, v. 53, p. 65–78, 2015. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404815000863?via%3Dihub. Acesso em: 18 jan. 2022.

SAFA, N. S.; VON SOLMS, R. Computers in Human Behavior An information security knowledge sharing model in organizations. **Computers in Human Behavior**, *[S. l.]*, v. 57, n. 2016, p. 442–451, 2016. b. DOI: 10.1016/j.chb.2015.12.037. Disponível em: http://dx.doi.org/10.1016/j.chb.2015.12.037. Acesso em: 10 jan. 2021.

SAFA, S. N.; VON SOLMS, R.; FURNELL, S. Information security policy compliance model in organizations. **Computers and Security**, *[S. l.]*, v. 56, p. 1–13, 2016. DOI: 10.1016/j.cose.2015.10.006. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84954106648&doi=10.1016%2fj.chb.2015.12.037&partnerID=40&md5=7644d1b633827cf08a854f954cc6157c. Acesso em: 15 dez 2021.

SAMPAIO, R. F.; MANCINI, M. C. Estudos de revisão sistemática: um guia para síntese. **Revista Brasileira de Fisioterapia**, *[S. l.]*, v. 11, p. 83–89, 2007.
SAMPIERE, H.; COLLADO, C. F.; LUCIO, M. P. B. **Metodologia de pesquisa**. 5. ed. Porto Alegre: Penso, 2013.

SANTANA, J. C. S. **A segurança da informação na ciência da informação no brasil**. 2021. UFBA, *[S. l.]*, 2021.

SANTOS, R. B.; SILVA, T. B. .. Information and communications security management. Ergonomic assessment to evaluate unsafe behaviors | Gestão da segurança da informação e comunicações. Análise ergonômica para avaliação de comportamentos inseguros. **Revista Digital de Biblioteconomia e Ciencia da Informacao**, *[S. l.]*, v. 19, 2021. DOI: 10.20396/rdbci.v19i00.8665529. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8665529. Acesso em: 15 jan. 2022.

SARKAR, S.; VANCE, A.; RAMESH, B.; DEMESTIHAS, M.; WU, D. T. The influence of professional subculture on information security policy violations: A field study in a healthcare context. **Information Systems Research**, *[S. l.]*, v. 31, n. 4, p. 1240–1259, 2020. DOI: 10.1287/isre.2020.0941. Disponível em: https://pubsonline.informs.org/doi/10.1287/isre.2020.0941. Acesso em: 08 jan. 2022.

SCHUETZ, S. W.; BENJAMIN LOWRY, P.; PIENTA, D. A.; BENNETT THATCHER, J. The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security. **Journal of Management Information Systems**, *[S. l.]*, v. 37, n. 3, p. 723–757, 2020. DOI: 10.1080/07421222.2020.1790187.

SCOPUS. **Content Coverage Guide.** Elsevier B.V., , 2017. Disponível em: https://www.elsevier.com/__data/assets/pdf_file/0007/69451/0597-Scopus-Content-Coverage-Guide-US-LETTER-v4-HI-singles-no-ticks.pdf. Acesso em 15 jan. 2022.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 2. ed. Rio de Janeiro: Campus, 2014.

SHADBAD, F. N.; BIROS, D. Technostress and its influence on employee information security policy compliance. **Information Technology and People**, *[S. l.]*, 2020. DOI: 10.1108/ITP-09-2020-0610. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ITP-09-2020-0610/full/html. Acesso em: 28 jan. 2022.

SNYMAN, D.; KRUGER, H. The application of behavioural thresholds to analyse collective behaviour in information security. **Information and Computer Security**, *[S. l.]*, v. 25, n. 2, p. 152–164, 2017. a. DOI: 10.1108/ICS-03-2017-0015. Diponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020697801&doi=10.1108%2fICS-03-2017-0015&partnerID=40&md5=b1df6af7ce1afc61f2df7fe6f5aac64d. Acesso em: 04 jan. 2022.

SNYMAN, D. P.; KRUGER, H. Collective information security behaviour: a technology-driven framework. **Information and Computer Security**, *[S. l.]*, v. 29, n. 4, p. 589–603, 2021. DOI: 10.1108/ICS-11-2020-0180. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-11-2020-0180/full/html. Acesso em: 14 jan. 2022.

SNYMAN, D. P.; KRUGER, H.; KEARNEY, W. D. I shall, we shall, and all others will: paradoxical information security behaviour. **Information and Computer Security**, *[S. l.]*, v. 26, n. 3, p. 290–305, 2018. DOI: 10.1108/ICS-03-2018-0034. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2018-0034/full/html. Acesso em: 22 jan. 2022.

SNYMAN, Dirk; KRUGER, Hennie. The application of behavioural thresholds to analyse collective behaviour in information security. **Information and Computer Security**, *[S. l.]*, v. 25, n. 2, p. 152–164, 2017. b. DOI: 10.1108/ICS-03-2017-0015. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2017-0015/full/html. Acesso em: 18 jan. 2022.

SOHRABI SAFA, Nader; VON SOLMS, Rossouw; FURNELL, Steven. Information security policy compliance model in organizations. **Computers and Security**, *[S. l.]*, v. 56, p. 1–13, 2016. DOI: 10.1016/j.cose.2015.10.006. Disponível em: http://dx.doi.org/10.1016/j.cose.2015.10.006. Acesso em: 04 jan. 2022.

SOLOMON, G.; BROWN, I. The influence of organisational culture and information security culture on employee compliance behaviour. **Journal of Enterprise Information Management**, *[S. l.]*, 2020. DOI: 10.1108/JEIM-08-2019-0217. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/JEIM-08-2019-0217/full/html. Acesso em:18 jan. 2022.

SOMMESTAD, T. Work-related groups and information security policy compliance. **Information and Computer Security**, *[S. l.]*, v. 26, n. 5, p. 533–550, 2018. DOI: 10.1108/ICS-08-2017-0054. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-08-2017-0054/full/html, Acesso em: 13 jan. 2022.

SOUSA, Yuri Sá Oliveira. O Uso do Software Iramuteq : Fundamentos de Lexicometria para Pesquisas Qualitativas. **Estudos e Pesquisas em Psicologia**, *[S. l.]*, v. 21, n. 4, p. 1541–1560, 2021. DOI: 10.12957/epp.2021.64034. Disponível em: https://www.redalyc.org/journal/4518/451873480014/html/. Acesso em: 14 jan. 2022.

STAFFORD, T.; DEITZ, G.; LI, Y. The role of internal audit and user training in information security policy compliance. **Managerial Auditing Journal**, *[S. l.]*, v. 33, n. 4, p. 410–424, 2018. DOI: 10.1108/MAJ-07-2017-1596. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/MAJ-07-2017-1596/full/html, Acesso em: 20 jan. 2022.

STEFANIUK, T. Training in shaping employee information security awareness. **Entrepreneurship and Sustainability Issues**, *[S. l.]*, v. 7, n. 3, p. 1832–1846, 2020. DOI: 10.9770/jesi.2020.7.3(26). Disponível em: https://jssidoi.org/jesi/article/492 Acesso em: 22 jan. 2022.

STEWART, H.; JÜRJENS, J. Information security management and the human aspect in organizations. **Information and Computer Security**, *[S. l.]*, v. 25, n. 5, p. 494–534, 2017. DOI: 10.1108/ICS-07-2016-0054. Diponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85033226176&doi=10.1108%2fICS-07-2016-0054&partnerID=40&md5=2d7254e8e73aa4095e580c464e57fe24. Acesso em: 10 jan. 2022.

SYMANTEC. **ISTR - Internet Security Threat Report**. , 2019.

TAVAKOL, M. ..; DENNICK, R. Making sense of Cronbach's alpha. **International Journal of Medical Education**, *[S. l.]*, v. 2, p. 53–55, 2011. DOI: https://dx.doi.org/10.5116/ijme.4dfb.8dfd. Disponível em: https://www.ijme.net/archive/2/cronbachs-alpha/. Acesso em 05 jan. 2022.

TOPA, I.; KARYDA, M. From theory to practice: guidelines for enhancing information security management. **Information and Computer Security**, *[S. l.]*, v. 27, n. 3, p. 326–342, 2019. DOI: 10.1108/ICS-09-2018-0108. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-09-2018-0108/full/html, Acesso em: 08 jan. 2022.

TRANG, S.; NASTJUK, I. Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. **Computers and Security**, *[S. l.]*, v. 104, 2021. DOI: 10.1016/j.cose.2021.102222. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404821000468?via%3Dihub. Acesso em: 22 fev. 2022.

TRIVIÑOS, Augusto Nibaldo Silva. **Introdução à pesquisa em ciências sociais: a pesquisa**

qualitativa em educação. São Paulo: Atlas, 1987.

UCHENDU, B.; NURSE, J. R. C.; BADA, M.; FURNELL, S. Developing a cyber security culture: Current practices and future needs. **Computers and Security**, *[S. l.]*, v. 109, 2021. DOI: 10.1016/j.cose.2021.102387. Disponível em: https://www.sciencedirect.com/science/article/pii/S016740482100211X?via%3Dihub. Acesso em: 08 jan. 2022.

VAN DER KLEIJ, R.; WIJN, R.; HOF, T. An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. **Computers and Security**, *[S. l.]*, v. 97, 2020. DOI: 10.1016/j.cose.2020.101970. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820302431?via%3Dihub. Acesso em: 25 jan. 2022.

VAN SCHAIK, P.; JESKE, D.; ONIBOKUN, J.; COVENTRY, L.; JANSEN, J.; KUSEV, P. Risk perceptions of cyber-security and precautionary behaviour. **Computers in Human Behavior**, *[S. l.]*, v. 75, p. 547–559, 2017. DOI: 10.1016/j.chb.2017.05.038. Disponível em: https://www.sciencedirect.com/science/article/pii/S074756321730359X?via%3Dihub. Acesso em: 14 jan. 2022.

VAN SLYKE, C.; BELANGER, F. Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective. **Computers and Security**, *[S. l.]*, v. 99, 2020. DOI: 10.1016/j.cose.2020.102064. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820303370?via%3Dihub. Acesso em: 30 jan. 2022.

VEDADI, A.; WARKENTIN, M.; DENNIS, A. Herd behavior in information security decision-making. **Information and Management**, *[S. l.]*, v. 58, n. 8, 2021. DOI: 10.1016/j.im.2021.103526. Disponível em: https://www.sciencedirect.com/science/article/pii/S0378720621001002?via%3Dihub. Acesso em: 05 jan. 2022.

VEIGA, A. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. **Information and Computer Security**, *[S. l.]*, v. 26, n. 5, p. 584–612, 2018. DOI: 10.1108/ICS-08-2017-0056. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-08-2017-0056/full/html. Acesso em: 30 jan. 2022.

VEIGA, A.; ASTAKHOVA, L. V.; BOTHA, A.; HERSELMAN, M. Defining organisational information security culture—Perspectives from academia and industry. **Computers and Security**, *[S. l.]*, v. 92, 2020. DOI: 10.1016/j.cose.2020.101713. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820300018?via%3Dihub. Acesso em: 14 jan. 2022.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 7. ed. São Paulo: Atlas, 2006.

WALL, J. D.; PALVIA, P.; D'ARCY, J. Theorizing the Behavioral Effects of Control Complementarity in Security Control Portfolios. **Information Systems Frontiers**, *[S. l.]*,

2021. DOI: 10.1007/s10796-021-10113-z. Disponível em: https://link.springer.com/article/10.1007/s10796-021-10113-z. Acesso em: 18 jan. 2022.

WIAFE, I.; KORANTENG, F. N.; WIAFE, A.; OBENG, E. N.; YAOKUMAH, W. The role of norms in information security policy compliance. **Information and Computer Security**, *[S. l.]*, v. 28, n. 5, p. 743–761, 2020. DOI: 10.1108/ICS-08-2019-0095. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/ICS-08-2019-0095/full/html. Acesso em: 30 jan. 2022.

WILEY, A.; MCCORMAC, A.; CALIC, D. More than the individual: Examining the relationship between culture and Information Security Awareness. **Computers and Security**, *[S. l.]*, v. 88, 2020. DOI: 10.1016/j.cose.2019.101640. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404819301841?via%3Dihub. Acesso em: 14 jan. 2022.

XU, F.; WARKENTIN, M. Integrating elaboration likelihood model and herd theory in information security message persuasiveness. **Computers and Security**, *[S. l.]*, v. 98, 2020. DOI: 10.1016/j.cose.2020.102009. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820302820?via%3Dihub. Acesso em: 14 jan. 2022.

XU, Z.; GUO, K. It ain't my business: a coping perspective on employee effortful security behavior. **Journal of Enterprise Information Management**, *[S. l.]*, v. 32, n. 5, p. 824–842, 2019. DOI: 10.1108/JEIM-10-2018-0229. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/JEIM-10-2018-0229/full/html. Acesso em: 22 jan. 2022.

YENG, P. K.; SZEKERES, A.; YANG, B.; SNEKKENES, E. A. Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: Systematic mapping study. **JMIR Human Factors**, *[S. l.]*, v. 8, n. 2, 2021. DOI: 10.2196/17604. Disponível em: https://humanfactors.jmir.org/2021/2/e17604. Acesso em: 14 mar. 2022.

YUPANQUI, J. R. A.; ORÉ, S. B. Information Security Policies: A systematic review of theories explaining their compliance | Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. **RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao**, *[S. l.]*, v. 2017, n. 25, p. 112–134, 2017. DOI: 10.17013/risti.25.112-134. Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85041588835&doi=10.17013%2fristi.25.112-134&partnerID=40&md5=b5ae0e5985bed999a042a951c9e9d6d6. Acesso em: 10 jan. 2021.

YUPANQUI, J. R. A.; ORÉ, S. B. Políticas de Seguridad de la Información: Revisión Revisión Sistemática de las Teorías que Explican su Cumplimiento. **RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação Políticas de Seguridad de la Información**, *[S. l.]*, n. 2003, p. 1–15, 2018.

ZHEN, J.; XIE, Z.; DONG, K. Positive emotions and employees' protection-motivated behaviours: A moderated mediation model. **Journal of Business Economics and Management**, *[S. l.]*, v. 21, n. 5, p. 1466–1485, 2020. a. DOI: 10.3846/jbem.2020.13169. Disponível em: https://journals.vilniustech.lt/index.php/JBEM/article/view/13169 Acesso em:

29 jan. 2022.

ZHEN, J.; XIE, Z.; DONG, K. Relationship between information security behavior and satisfaction degree of psychological needs and the mediation effect of team effectiveness and organizational commitment. **Revista Argentina de Clinica Psicologica**, *[S. l.]*, v. 29, n. 1, p. 442–452, 2020. b. DOI: 10.24205/03276716.2020.60. Disponível em: https://www.revistaclinicapsicologica.com/article.php?doi=10.24205/03276716.2020.60. Acesso em: 12 fev. 2022.

ZWILLING, M.; KLIEN, G.; LESJAK, D.; WIECHETEK, Ł.; CETIN, F.; BASIM, H. N. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. **Journal of Computer Information Systems**, *[S. l.]*, 2020. DOI: 10.1080/08874417.2020.1712269. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1712269. Acesso em: 14 jan. 2022.

APÊNDICE A – Roteiro da entrevista com especialistas

PESQUISA SOBRE COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO NAS UNIVERSIDADES FEDERAIS

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Este é um convite para senhor(a) participar da pesquisa intitulada “COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO: estudo aplicado as Universidades Federais do Brasil", desenvolvida pela doutoranda Sueny Léda Araújo Ribeiro, do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, sob orientação do Prof. Dr. Wagner Junqueira de Araújo, da Universidade Federal da Paraíba e do coorientação Prof. Dr. Marcelo de Santana Porte, da Universidade Federal do Sul e Sudeste do Pará. As informações serão utilizadas estritamente para fins acadêmicos, podendo os resultados serem publicados em eventos ou periódicos científicos, sempre sem fins lucrativos e resguardando a identidade dos respondentes.

Agradecemos sua contribuição!

1 - A universidade possui uma(s) política(s) ou procedimentos de segurança da informação? Ex: Política de controle de acesso lógico e físico à informação e aos recursos de processamento da informação; política de mesa limpa/tela limpa para os recursos de processamento da informação; política de classificação da informação. Ex.: sigilosa, ostensiva, pessoal; acordos de confidencialidade ou acordo de não divulgação que reflitam as necessidades da organização para a proteção da informação; termo de responsabilidade que oriente os funcionários sobre a responsabilidade pelas informações que manuseiam.

2 Quais os controles de segurança da informação relacionados ao comportamento humano são utilizados pela universidade? Ex: sistemas utilizados exigem senhas alfanuméricas e que sejam trocadas com frequência ou controle de acesso físico aos ambientes

4 A instituição informa periodicamente os funcionários sobre as questões de violações de segurança da informação por meio de campanhas de conscientização (e-mail, folheto / seminário / workshops? Como eles funcionam?

5 Existe programas de treinamento em conscientização da segurança da informação?

6 Existe(m) alguma(s) ação(es) de conscientização em segurança da informação desenvolvidas pela universidade? Como: Informar periodicamente sobre as questões de violações de segurança da informação por meio de campanhas de conscientização (e-mail, folheto / seminário / workshops).

7 A universidade possui ponto de contato (responsável definido) onde os funcionários podem se reportar quando são vítimas de incidentes de segurança da informação?

8 Quais os incidentes de seguranças ocorrem com mais frequência?

9 Quais são os principais motivos para ocorrência desses incidentes?

10 Os servidores são instruídos a notificar sobre quaisquer fragilidades de segurança da informação nos sistemas/serviços o mais rápido possível?

APÊNDICE B – Questionário aplicado aos gestores

PESQUISA SOBRE COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO NAS UNIVERSIDADES FEDERAIS

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Este é um convite para senhor(a) participar da pesquisa intitulada "COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO: estudo aplicado as Universidades Federais do Brasil", desenvolvida pela doutoranda Sueny Léda Araújo Ribeiro, do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, sob orientação do Prof. Dr. Wagner Junqueira de Araújo, da Universidade Federal da Paraíba e do coorientação Prof. Dr. Marcelo de Santana Porte, da Universidade Federal do Sul e Sudeste do Pará. As informações serão utilizadas estritamente para fins acadêmicos, podendo os resultados serem publicados em eventos ou periódicos científicos, sempre sem fins lucrativos e resguardando a identidade dos respondentes.

Agradecemos sua contribuição!

1 Quais desses instrumentos de controle existem na sua instituição? (Marque quantas opções forem necessárias).
( ) Política de segurança da informação
( ) Controle de acesso físico ao ambiente de trabalho
( ) Política para uso de correio eletrônico
( ) Política de Senhas
( ) Capacitação em conscientização da segurança da informação
( ) Campanhas de conscientização em segurança da informação.
( ) Termo de responsabilidade e confidencialidade dando ciência do conhecimento das normas e suas principais responsabilidades em relação à segurança da informação.
( ) Política de Classificação da Informação
( ) Política de Mesa Limpa/Tela Limpa

2 Quais incidentes de segurança relacionados aos aspectos humanos ocorrem com mais frequência na sua instituição?
( ) Phishing
( ) Engenharia Social
( ) Defacement
( ) Acesso indevido por compartilhamento de senhas
( ) Acesso indevido a rede sem fio por terceirizados com senhas de alunos
( ) Ransomware
( ) Não há mapeamento ainda.
( ) Outros. Quais?

3 Quais os canais de comunicação para informar incidentes de segurança ou denúncias de quebra de segurança pela comunidade acadêmica? (Pode marcar mais de uma opção)

( ) E-mail
( ) Telefone
( ) Site institucional
( ) Sistema interno de chamados
( ) Redes sociais
( ) Não existe ponto de contato

4 O servidor é responsabilizado pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso.

Nunca	Raramente	Ocasionalmente	Quase sempre	Sempre
01	02	03	04	05

APÊNDICE C – Questionário aplicado aos servidores

PESQUISA SOBRE COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO NAS UNIVERSIDADES FEDERAIS

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Este é um convite para senhor(a) participar da pesquisa intitulada "COMPORTAMENTO HUMANO EM SEGURANÇA DA INFORMAÇÃO: estudo aplicado as Universidades Federais do Brasil", desenvolvida pela doutoranda Sueny Léda Araújo Ribeiro, do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, sob orientação do Prof. Dr. Wagner Junqueira de Araújo, da Universidade Federal da Paraíba e do coorientação Prof. Dr. Marcelo de Santana Porte, da Universidade Federal do Sul e Sudeste do Pará. As informações serão utilizadas estritamente para fins acadêmicos, podendo os resultados serem publicados em eventos ou periódicos científicos, sempre sem fins lucrativos e resguardando a identidade dos respondentes.

Agradecemos sua contribuição!

Perfil do respondente
Você aceita participar dessa pesquisa? ( ) Sim Não ( )
(Responda apenas se for Servidor Técnico-Administrativo ou Docente ativos de Universidade Federal (UF).

1 Você está vinculado a qual Universidade Federal? (Apenas SIGLA)

2 Qual seu sexo?
( ) Masculino ( ) Feminino
( ) Prefiro não declarar ( )Outro_____
3 Qual sua idade? _____
4 Qual sua categoria profissional?
( ) Técnico Administrativo ( ) Docente
5 Qual seu tempo de serviço? _____
6 Qual seu nível de escolaridade?
( ) Graduação ( ) Especialização
( ) Mestrado ( ) Doutorado
( ) Pós-Doutorado ( ) Outro Qual?_____

Avaliação da Ameaça
Avaliação da ameaça - avalia o nível de perigo vinculado a um evento de segurança da informação.
Para as questões dessa seção, indique o quanto você concorda ou discorda das afirmações. 1 (Discordo totalmente), 2 (Discordo parcialmente), 3 (Indiferente), 4 (Concordo parcialmente) e 5 (Concordo totalmente).

7 Eu sei que minha instituição pode estar vulnerável a violações de segurança se eu não aderir às suas Políticas de Segurança da Informação (PSI).

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

8 Posso ser vítima de um ataque malicioso se não cumprir as Políticas de Segurança da Informação (PSI) da minha instituição.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

9 Em termos de riscos à segurança da informação na UFPB, a vulnerabilidade do meu computador e dados é muito alta.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

10 Informações importantes ou recursos de computação podem ser danificados devido à minha negligência em relação às Políticas de Segurança da Informação (PSI).

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

11 Na minha opinião, proteger as informações da minha instituição é importante.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

12 Eu entendo que ter alguém violando ou danificando os recursos de informação no trabalho é muito perigoso.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

13 Para mim, tomar precauções de segurança da informação é fácil.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

14 A UFPB disciplina os funcionários que violam as regras de segurança da informação

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

15 Se eu fosse pego violando as políticas de segurança da informação da UFPB, seria severamente punido.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

Avaliação de enfrentamento

Avaliação de enfrentamento - avalia uma determinada estratégia de enfrentamento para mitigar ou evitar um evento de segurança ameaçador.

Para as questões dessa seção, indique o quanto você concorda ou discorda das afirmações. 1 (Discordo totalmente), 2 (Discordo parcialmente), 3 (Indiferente), 4 (Concordo parcialmente) e 5 (Concordo totalmente).

16 Em minha instituição, os esforços para garantir a segurança das informações confidenciais são eficazes.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

17 Em minha instituição, as medidas de segurança disponíveis para proteger as informações de trabalho contra violações de segurança são eficazes.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

18 As medidas preventivas de que disponho na minha instituição para lidar com conteúdos maliciosos são importantes.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

19 Medidas de segurança em minha instituição evitam que hackers tenham acesso a informações pessoais ou educacionais confidenciais.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente

01	02	03	04	05

20 Eu acredito que tenho as competências necessárias para me proteger de violações de segurança da informação.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

21 Acredito que desenvolvi a capacidade de impedir que as pessoas obtenham minhas informações confidenciais.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

22 Acredito que está sob meu controle me proteger de violações de segurança da informação.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

23 Posso ativar as medidas de segurança em meu computador da UFPB, mas apenas quando tenho manuais para referência.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

24 Seguir as regras de segurança é demorado.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

25 Cumprir as regras de segurança requer muito esforço mental.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

26 Cumprir as regras de segurança exigiria iniciar um novo hábito.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

27 O custo de implementação de medidas excede os benefícios de não as aplicar.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

28 Meus colegas acham que devo seguir as políticas de segurança da informação da UFPB.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

29 Meu gestor recomenda que devo seguir as políticas de segurança da informação da UFPB.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

30 A alta administração recomenda que devo seguir as políticas de segurança da informação da UFPB.

Discordo totalmente	**Discordo parcialmente**	**Indiferente**	**Concordo parcialmente**	**Concordo totalmente**
01	02	03	04	05

31 Acredito que meus colegas implementam medidas de segurança para se proteger contra as ameaças à segurança da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

32 Acredito que meu gestor implementa medidas de segurança para se proteger contra as ameaças à segurança da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

33 Acredito que a alta administração implementa as medidas de segurança para se proteger contra as ameaças à segurança da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

Conscientização e Capacitação
Conscientização- reflete a consciência das responsabilidades com a segurança da informação e os meios pelos quais essas responsabilidades são realizadas.
Capacitação - treinamento realizado em diferentes formas de apresentação.

34 Tenho conhecimento do setor que devo me reportar caso tenha conhecimento ou sofra algum incidente de segurança da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

35 Se eu perceber algum comportamento suspeito, eu reportarei ao setor competente.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

36 Se eu perceber que meu colega não cumpre as regras de segurança, não praticarei nenhuma ação sobre isso.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

37 Se eu souber de algum incidente de segurança da informação, reportarei ao setor competente.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

38 Minha instituição informa periodicamente sobre as questões de violações de segurança da informação por meio de campanhas de conscientização (e-mail, folheto / seminário / workshop).

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

39 Minha instituição me mantém atualizado sobre violações de segurança da informação e medidas preventivas.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

40 Minha instituição continua instruindo os funcionários sobre suas responsabilidades de segurança de computador.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

41 Eu nem sempre clico em links de e-mail só porque eles vieram de pessoas conhecidas.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

42 Eu clico em links de e-mail enviado por pessoas desconhecidas, se eu entender que a informação seja interessante.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

43 Eu não abro e-mail se o remetente for um desconhecido.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

44 Uso diferentes senhas para acessar contas pessoais e do trabalho.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

45 Troco minhas senhas com frequência.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

46 Compartilho minhas senhas com meus colegas de trabalho.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

47 Uso combinações de letras, números e símbolos para minhas senhas do trabalho.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

48 Bloqueio a tela do computador por meio de senha antes de me ausentar da minha estação de trabalho.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

49 Minha instituição possui um programa de capacitação constante para que eu me mantenha informado sobre atualização das políticas e de procedimentos de segurança da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

50 Os programas de capacitação em segurança da informação da minha instituição me mantêm bem informado contra ameaças à segurança.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

51 Os programas de capacitação em segurança da informação da minha instituição contribuem para que eu desenvolva habilidades necessárias para adotar um comportamento protetor.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

Políticas e controles de segurança da informação

52 Pretendo cumprir os requisitos das Políticas de Segurança da Informação da minha instituição no futuro.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

53 Pretendo cumprir minhas responsabilidades em relação às Políticas de Segurança da Informação no futuro.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

54 É minha intenção continuar a cumprir as Políticas de Segurança da Informação institucionais.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

55 A Política de Segurança da Informação da minha instituição influencia nas minhas rotinas de trabalho.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

56 Minha instituição garante que as Políticas de Segurança da Informação estejam disponíveis para todos os funcionários.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

57 Acredito que minha instituição tenha estabelecido regras de conduta para o uso de recursos de informática.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

58 Minha instituição tem diretrizes específicas que regem o que os funcionários têm permissão para fazer com seus computadores.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

59 Acredito que minha instituição definiu códigos de conduta explicando o que devemos e não devemos fazer em relação à segurança da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

ANEXO A - PARECER CONSUBSTANCIADO DO CEP

CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA - CCS/UFPB

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: COMPORTAMENTO EM SEGURANÇA DA INFORMAÇÃO: estudo de caso na Universidade Federal da Paraíba ¿ Brasil e da Universidade de Aveiro - Portugal

Pesquisador: SUENY LEDA ARAUJO RIBEIRO

Área Temática:

Versão: 2

CAAE: 52700021.1.0000.5188

Instituição Proponente: Universidade Federal da Paraíba

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.148.542

Apresentação do Projeto:

Trata-se de um protocolo de pesquisa egresso do PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO, do CENTRO DE CIÊNCIAS SOCIAIS APLICADAS, da UNIVERSIDADE FEDERAL DA PARAÍBA, da aluna SUENY LEDA ARAUJO RIBEIRO, sob orientação do Prof. Dr. Wagner Junqueira de Araújo.

1 INTRODUÇÃO

Esta seção consiste na exposição dos aspectos gerais da proposta de pesquisa, de modo a contextualizar e delimitar o tema, o problema e as hipóteses formuladas, descrição dos objetivos geral e específicos, justificativa da pesquisa e, por fim, a organização da estrutura da pesquisa.

1.1 TEMA DE PESQUISA

As organizações, crescentemente, veem a informação como um dos seus ativos mais valiosos (BUNKER, 2012; LEIDNER, 2010, tradução nossa), constituindo-se como um elemento essencial para o desenvolvimento da sociedade, sendo responsável pelas transformações tecnológicas, administrativas e organizacionais. Tendo em vista sua importância como insumo, a informação requer cuidados específicos que considerem sua origem, criação, tratamento, disponibilização e uso, uma vez que, ao longo do seu ciclo de vida, diversos fatores podem emergir, dentre eles, a

necessidade da manutenção da segurança dos ativos informacionais.

Os ativos informacionais correspondem aos elementos que asseguram os processos de negócio de uma determinada organização, sendo de relevância para o seu desenvolvimento, requerendo um gerenciamento preciso que possa coordenar toda a complexidade que gira em torno do ciclo de vida das informações necessárias aos negócios (ARAÚJO, 2016).

Perante a dimensionalidade desses ativos na operação dos mercados de bens e serviços, na dinâmica organizacional, as informações são rotineiramente trocadas, compradas, encontradas, geradas e aplicadas ao trabalho, configurando-se como importante constituinte da expansão organizacional. Em vista disso, a gestão dos ativos informacionais precisa considerar a aplicabilidade da segurança da informação como um dos procedimentos essenciais de sua estratégia para a proteção das informações das corporações.

Ainda, segundo Bunker (2012, tradução nossa) dada a importância da informação para o funcionamento eficaz e desenvolvimento estratégico dos seus negócios, as organizações veem cada vez mais a segurança da informação como uma prioridade. Visto que, à medida que a importância da informação cresce, o mesmo acontece com os incentivos para o acesso e o abuso à informação cometidos por hackers, descontentes, criminosos e terroristas (DOHERTY; TAJUDDIN, 2018, tradução nossa).

Nessa conjuntura, por representar um conceito amplo, a segurança da informação tem sido estudada por múltiplas áreas, tanto nas ciências exatas (estudando a tecnologia), como nas ciências sociais (estudando o comportamento humano e os processos). Dentre as áreas das ciências sociais preocupadas com a segurança da informação, em contexto de pesquisa, inclusive a Ciência da Informação, que no campo da gestão do conhecimento, procura estabelecer seus estudos de segurança centrados das dimensões de processos e pessoas (ARAÚJO, 2014).

As pesquisas nessas ciências, com base nas necessidades organizacionais, ou do indivíduo, estruturaram a segurança da informação como uma disciplina, que abrange ações necessárias, que buscam garantir, conforme necessidades específicas, a preservação da informação com base em três propriedades: confidencialidade, integridade e disponibilidade (INFORMATION SYSTEMS AUDITAND CONTROL ASSOCIATION, 2012, tradução nossa; SÊMOLA, (2014). Essas propriedades representam a sobrevivência de qualquer organização, cuja interferência, direta ou indireta, em algum de seus processos, pode acarretar grandes prejuízos. Assim, ressalta-se a necessidade de uma gestão da segurança da informação que contemple, de forma eficiente, os diversos tipos de informações que são criadas, manuseadas e/ou protegidas pelas organizações.

Nas últimas décadas, diversas organizações têm se concentrado nas soluções baseadas em tecnologia para abordar a segurança da informação, como por exemplo: anti-virus, antimalware, antispam, anti-phishing, anti-spyware, firewall, autenticação e sistemas de detecção de intrusão. No entanto, Safa et al (2015, tradução nossa) argumentam que essa abordagem não garante a seguridade do negócio no contexto da gestão da segurança da informação, destacando que a tecnologia, unicamente como equipamento tecnológico e componentes lógicos computacionais, não é capaz de estabelecer a proteção da informação contra ameaças, evidenciando que falhas humanas devem ser consideradas.

Doherty e Tajuddin (2018, tradução nossa) destacam que incidentes, relacionados à segurança da informação, como violações de confidencialidade, fraude de computador, utilização indevida dos sistemas de informação, e infecções por vírus ou software disruptivo, são comumente identificados, em vez de problemas técnicos. Nesse sentido, Safa, Von Solms e Furnell (2016, tradução nossa) esclarecem que para a garantia de um ambiente seguro para a informação, os aspectos humanos devem ser tomados em consideração, além dos aspectos tecnológicos, para que possa haver uma efetiva gestão da segurança da informação, cuja raiz das falhas dos usuários da informação são, essencialmente, a falta de conscientização de segurança da informação, ignorância, negligência, apatia, dano e resistência.

Nesse contexto, embora as pessoas sejam frequentemente referidas como o elo mais fraco na segurança da informação, são exatamente as pessoas que podem desempenhar um papel essencial na salvaguarda da informação (CONNOLLY et al., 2017; DANG-PHAM; PITTAYACHAWAN; BRUNO, 2017a; JANSEN; VAN SCHAIK, 2018; PARSONS et al., 2017; SAFA; VON SOLMS; FURNELL, 2016; SAMPAIO; MANCINI, 2007; SNYMAN; KRUGER, 2017). Entretanto, para que ocorra a prática de um comportamento preventivo, é necessário que os indivíduos estejam conscientes dos riscos e vulnerabilidades, bem como capacitados para o enfrentamento de possíveis ameaças. Nessas circunstâncias, é imprescindível uma abordagem do comportamento humano em segurança da informação (JANSEN; VAN SCHAIK, 2018, tradução nossa).

Nessa perspectiva, sabendo-se que a Ciência da Informação está direcionada aos problemas da efetiva comunicação entre os seres humanos e os registros – no contexto social, institucional/organizacional ou individual – referente às necessidades de informação Saracevic (1996), e compreendendo que a segurança da informação corresponde a uma disciplina inserida nessa área do conhecimento, no campo da gestão, um estudo referente à abordagem do comportamento humano em segurança da informação poderá representar novos direcionamentos teóricos e práticos para soluções de problemas evidenciados no contexto real das necessidades

informacionais em organizações.

1.2 PROBLEMA E HIPÓTESES DA PESQUISA

De acordo com estudos recentes da área de tecnologia da informação, uma proteção da segurança da informação baseada apenas em uma perspectiva tecnológica, culmina em uma abordagem incompleta, demonstrando a necessidade de uma visão ampla com base em uma abordagem interdisciplinar, na qual o fator humano é considerado como principal componente de processos estratégicos organizacionais de segurança da informação (YUPANQUI; ORÉ, 2018, tradução nossa).

Ainda nesse sentido, a tecnologia da informação trouxe muitas vantagens para as organizações, no entanto, a segurança da informação permanece como uma grande preocupação para os sistemas organizacionais que dependem dessa tecnologia. Os usuários, intencionalmente ou por negligência, são uma grande fonte potencial de risco para os ativos de informação. A falta de consciência, assim como a negligência, resistência, desobediência, apatia e malícia são as causas principais dos incidentes de segurança da informação nas mais diversas instituições.

Nesse contexto, em ambiente organizacional, as ameaças internas atraíram a atenção de vários especialistas nesse domínio, em que, com base em suas observações exploratórias, foram identificadas duas considerações particularmente importantes: a motivação e a oportunidade (SAFA et al., 2018, tradução nossa). A partir desses aspectos, tornou-se possível analisar de forma direcionada os comportamentos de usuários da informação organizacional. Nesse sentido, em relação à segurança da informação, torna-se salutar estudar o comportamento dos usuários/funcionários observando suas motivações perante um possível comportamento preventivo em organizações, sejam nas dimensões públicas ou privadas.

3 PROCEDIMENTOS METODOLÓGICOS

Nesta seção, serão apresentados os fundamentos e procedimentos metodológicos estabelecidos para o desenvolvimento da proposta da pesquisa, cujas ideias principais estão identificadas neste projeto. A sua estrutura, encontra-se organizada conforme a lógica da pesquisa científica com a apresentação da caracterização da pesquisa, com descrição da tipologia, abordagem e estratégia que serão utilizadas, bem como a apresentação dos contextos e sujeitos da pesquisa, as técnicas de coleta de dados, e a descrição dos métodos de análise dos dados e a trajetória da pesquisa.

3.1 CARACTERIZAÇÃO DA PESQUISA

Com o intuito de alcançar o objetivo da pesquisa em estabelecer uma análise comparativa e

relacional entre aspectos comportamentais em segurança da informação com grupos de servidores culturalmente diferenciados, bem como responder ao questionamento da identificação dos aspectos comportamentais nesses grupos, a pesquisa proposta se caracterizará como aplicada, cujos objetivos a classificarão como pesquisa descritiva, que se apoiará em uma abordagem quantitativa, com uma estratégia de investigação definida no estudo de casos múltiplos.

A caracterização da pesquisa como de natureza aplicada, refere-se a sua necessidade em investigar a complexa dinâmica do funcionamento universitário e a circulação da informação produzida, manipulada e disseminada por essa instituição, tendo como principal elemento o comportamento de servidores perante a segurança dos ativos informacionais. A pesquisa aplicada permite que o conhecimento gerado a partir da análise de determinada problemática em condições da realidade, pode ser direcionado para a solução de problemas específicos do cotidiano. De acordo com a proposta da pesquisa, em seu objetivo específico de desenvolver um modelo de comportamento preventivo para universidades sob a perspectiva da Teoria da Motivação de Proteção, tem-se o intuito de poder contribuir com uma solução prática para a problemática condição da segurança dos ativos de informação de universidades diante da atuação dos servidores em saber manipular esses ativos conforme suas especificidades e cuidados exigidos.

A pesquisa descritiva se dá pela necessidade de atingir os objetivos específicos de:

verificar os requisitos legais aplicados à segurança da informação na UFPB-BR e UA-PT;

compreender como os requisitos legais influenciam o comportamento em segurança dos servidores;

identificar quais os controles formais e informais são utilizados pelos servidores, relacionados ao comportamento humano; e investigar as relações entre, gravidade percebida, vulnerabilidade percebida; e eficácia de resposta, autoeficácia, custo de reposta com o comportamento seguro. A pesquisa descritiva busca descrever as características de determinada população, a partir de uma série de informações sobre o que se deseja pesquisar, além de exigir uma precisa delimitação de técnicas, métodos e teorias que orientarão a coleta e interpretação dos dados (GIL, 2012; TRIVIÑOS, 1987).

Para que a pesquisa consiga alcançar seu objetivo de contribuir com uma solução prática no tocante à segurança dos ativos informacionais de universidades conforme o comportamento de seus servidores, será necessário que a pesquisa proposta assuma o caráter de uma pesquisa descritiva para que possa reunir um conjunto de informações que auxilie na construção e examinação dos fatos e fenômenos que serão verificados. Ou seja, a pesquisa descritiva busca

descrever as características de determinada população, a partir de uma série de informações sobre o que se deseja pesquisar, além de exigir uma precisa delimitação de técnicas, métodos e teorias que orientarão a coleta e a interpretação dos dados (TRIVIÑOS, 1987; GIL, 2012).

Nessa perspectiva, a pesquisa descritiva também irá contribuir para o alcance dos objetivos que buscam verificar os requisitos legais que direcionam a segurança da informação nas universidades que serão estudadas, compreender se esses requisitos influenciam o comportamento dos servidores em segurança da informação, identificar os controles formais e informais que se relacionam ao comportamento humano, e investigar os aspectos relacionais como: gravidade percebida, vulnerabilidade percebida , eficácia de resposta, autoeficácia, custo de resposta com a intenção de comportamento preventivo.

Como abordagem, optou-se pela pesquisa quantitativa perante a exigência de um estudo de verificação não observável – como o objetivo da pesquisa descritiva – de modo que possa ajudar no desenvolvimento de uma investigação organizada, em parte, por um exame crítico das informações, evitando-se ao máximo a geração de imprecisões (TRIVIÑOS, 1987).

Quanto ao método, a proposta de pesquisa pode ser considerada um estudo de casos múltiplos, uma vez que se trata de uma comparação entre comportamentos em segurança da informação em duas instituições públicas de países diferentes. Nessa perspectiva, para Godoi, Bandeira-de-Melo e Silva (2010), os estudos de casos múltiplos são muito usados em pesquisas comparativas cross-cultural, que buscam estudar como pessoas de diferentes países, regiões ou culturas se apropriam de determinados conceitos e significados que são orientadores de seu comportamento. Para esses autores, os estudos de casos múltiplos além de permitir a comparação, possibilita a obtenção de resultados mais robustos.

Segundo Yin (1994), os estudos de casos podem ser baseados em uma mistura de provas quantitativas e qualitativas; e representam uma importante estratégia para pesquisar acontecimentos contemporâneos, inseridos em um contexto real, sobre o qual o investigador tem pouco ou nenhum controle. O autor adverte que o pesquisador deve estar preparado para fazer uso de várias fontes de evidências, que precisam convergir, oferecendo, dessa maneira, condições para se afirmar fidedignidade e validade dos achados por meio de triangulações de informações, dados, evidências, e mesmo, de teorias.

Ainda de acordo com Yin (1994), nos estudos de casos múltiplos, a análise deve seguir um experimento cruzado, ou seja, deve-se conduzir cada estudo de caso individualmente e, em seguida, fazer o cruzamento dos resultados. No entanto, conforme o autor um ponto negativo do estudo de casos múltiplos é o fato do estudo implicar muito tempo do pesquisador, além possíveis

Investimentos financeiros.

3.2 CONTEXTO DA PESQUISA

O contexto da pesquisa consiste em duas universidades públicas localizadas em países lusófonos pertencentes a continentes distintos, mas com passado comum: a Universidade Federal da Paraíba (UFPB), estado da Paraíba, Brasil, e a Universidade de Aveiro (UA), cidade de Aveiro, Portugal. O Brasil, por ter sido colonizado por portugueses, foi influenciado por muitas semelhanças culturais. No entanto, existe também diversas diferenças marcantes entre os dois países – como o posicionamento geográfico e desenvolvimento histórico-social – que exercem, de forma significativa, influência sobre a cultura de cada país, e por sua vez, no comportamento de seus indivíduos (PIRES; MACÊDO, 2006).

A Universidade Federal da Paraíba foi criada em 1955, como Universidade da Paraíba, por meio da Lei estadual nº. 1.366, de 02 de dezembro de 1955. Inicialmente seu surgimento ocorreu com a junção de algumas escolas superiores. Posteriormente, com a sua federalização, aprovada e promulgada pela Lei nº. 3.835 de 13 de dezembro de 1960, transformou-se em Universidade Federal da Paraíba, incorporando as estruturas universitárias das cidades de João Pessoa e Campina Grande. A partir de sua federalização, a UFPB desenvolveu uma crescente estrutura multicampi, distinguindo-se, nesse aspecto, das demais universidades federais do sistema de ensino superior do Brasil que, em geral, têm suas atividades concentradas num só espaço urbano. Essa singularidade expressou-se por sua atuação em sete campi implantados nas cidades de João Pessoa, Campina Grande, Areia, Bananeiras, Patos, Sousa e Cajazeiras. A Lei nº. 10.419 de 09 de abril de 2002 criou, por desmembramento da UFPB, a Universidade Federal de Campina Grande (UFCG), com sede e foro na cidade de Campina Grande, Paraíba. A UFPB ficou composta legalmente, a partir de então, pelos campi de João Pessoa (capital), Areia e Bananeiras. Posteriormente foi criado um campus, no Litoral Norte do Estado, abrangendo os municípios de Mamanguape e Rio Tinto (UNIVERSIDADE FEDERAL DA PARAÍBA, 2015, 2018).

Concernente aos campi e aos centros, a UFPB está estruturada da seguinte forma:

Campus I, na cidade de João Pessoa, compreendendo os seguintes Centros: Centro de Ciências Exatas e da Natureza (CCEN); Centro de Ciências Humanas, Letras e Artes (CCHLA); Centro de Ciências Médicas (CCM); Centro de Ciências da Saúde (CCS); Centro de Ciências Sociais Aplicadas (CCSA); Centro de Educação (CE); Centro de Tecnologia (CT); Centro de Ciências Jurídicas (CCJ) e Centro de Tecnologia e Desenvolvimento Regional (CTDR); Campus II, na cidade de Areia, compreendendo o Centro de Ciências Agrárias (CCA); Campus III, na cidade de Bananeiras, abrangendo o Centro de Ciências Humanas, Sociais e Agrárias (CCHSA); e o

Campus IV, nas cidades de Mamanguape e Rio Tinto, com o Centro de Ciências Aplicadas e Educação (CCAE).

De acordo com o Relatório de Gestão, ano de 2018, a UFPB é composta por 31.752 alunos de graduação, 4.750 alunos de pós-graduação, 2.862 docentes, 3.491 servidores técnicoadministrativos, 128 cursos de graduação, 110 cursos de pós-graduação (72 mestrados e 38 doutorados), duas escolas de ensino médio e profissionalizante, dentre outras unidades e critérios quantificáveis (UNIVERSIDADE FEDERAL DA PARAÍBA, 2018). A Figura 15, ilustra a estrutura organizacional da UFPB.

A Universidade de Aveiro é uma fundação pública com regime de direito privado que tem como missão a intervenção e desenvolvimento da formação em graduação e pós-graduação (ensino), pesquisa e cooperação com a sociedade (extensão). Foi criada em 15 de dezembro de 1973, mas somente foi aberta ao público entre os anos de 1974 e 1975 com os cursos de Eletrônica e Telecomunicações, com os primeiros 46 alunos. O objetivo inicial da UA foi a criação de cursos que se destacavam em áreas determinadas como inovadoras para época, que não eram exploradas pelas instituições de ensino superior tradicionais, e em domínios com correspondência na estrutura produtiva regional e nacional. Em 1975/1976 foi criado o curso de Estudos do Ambiente, bem como diversos cursos de formação de professores: Ciências da Natureza, Matemática, Inglês-Português e Francês-Português (UNIVERSIDADE DE AVEIRO, 2019).

Entre os anos de 1977 e 1978, com o acréscimo incipiente da população discente nos cursos de bacharelado, a instituição os substituiu por cursos de licenciatura, no âmbito da primeira restruturação pedagógica realizada na Universidade de Aveiro. Durante a década de 1980, ocorreu a fase de consolidação da universidade, em que foram definidos o Regulamento Interno e a criação dos órgãos fundamentais, bem como a conclusão do processo de aquisição dos terrenos para implantação do Campus. Em 24 de setembro de 1988, foi consolidada a estrutura orgânica da UA, com a homologação, em junho de 1989, dos Estatutos da Universidade (UNIVERSIDADE DE AVEIRO, 2019).

Nesse período, aos cursos iniciais foram acrescidas áreas inovadoras como Ambiente, Gestão Industrial, Música, Turismo, Materiais, Química Industrial e Novas Tecnologias.

Durante a década de 1990, ocorreu uma nova fase de evolução da UA, em que foram redefinidas novas prioridades como a Internacionalização e a Cooperação, nomeadamente com a participação em Programas Europeus, no reforço das relações com países de expressão portuguesa e latina, na participação em redes e consórcios de universidades internacionais e na

assinatura de protocolos com instituições, organismos e empresas do país e do estrangeiro. (UNIVERSIDADE DE AVEIRO, 2019).

Atualmente, a cooperação com a sociedade é reforçada pela intervenção da UA na promoção de transferência do conhecimento, tecnologia e inovação em conjunto com o campo empresarial. Paralelamente, ocorre o avanço, afirmativo, na dinamização de programas de formação continuada e de ensino a distância que assumem uma importância crescente na diferenciação de públicos e na satisfação das suas necessidades de formação. Nesse contexto, com o dinamismo do corpo de docentes e de pesquisadores, a UA é reconhecida como a universidade portuguesa com o maior número de projetos de pesquisa reconhecidos internacionalmente (UNIVERSIDADE DE AVEIRO, 2019).

A estrutura organizacional da Universidade de Aveiro, tem por base uma estrutura matricial que integra os subsistemas de ensino universitário e politécnico, que são representados em uma permanente interação entre unidades, serviços e demais estruturas, privilegiando a interdisciplinaridade, flexibilidade, organização, gestão por atividades, objetivos e a abertura à sociedade com estreita ligação ao meio empresarial envolvente (UNIVERSIDADE DE AVEIRO, 2019).

A Universidade de Aveiro integra o Campus Universitário de Santiago e o Campus do Crasto, em Aveiro e os polos de ensino de Águeda (Escola Superior de Tecnologia e Gestão de Águeda) e de Oliveira de Azeméis (Escola Superior de Design, Gestão e Tecnologias da Produção Aveiro Norte), formando o trio de cidades UA (UNIVERSIDADE DE AVEIRO, 2019).

Quanto à gestão institucional, a UA é regida por normativos e documentos estratégicos, como Estatutos Académicos e Administrativos, Plano Estratégico, Plano de Atividades, Relatório de Contas e Gestão, Manual da Qualidade, Manual de Pessoal, Balanço Social e Gestão de Riscos de Corrupção e Infrações Conexas (UNIVERSIDADE DE AVEIRO, 2019).

Em relação a sua estrutura, a UA ocupa 150 hectares onde estão situados 45 edifícios compostos por 20 (vinte) departamentos e escolas, além de quatro bibliotecas. Atualmente, cerca de 13 mil estudantes estão matriculados, distribuídos entre os cursos de licenciatura, mestrado e doutorado (UNIVERSIDADE DE AVEIRO, 2019).

De acordo com a Universidade de Aveiro (2019), para o desenvolvimento de suas atividades acadêmicas e administrativas, a universidade dispõe de mais de mil docentes, 650 técnicos de administração e gestão e 152 pesquisadores. Com oferta de 45 licenciaturas, 60 mestrados, 12 (doze) mestrados integrados e 51 programas de doutorado. Nesse contexto, a UA desenvolve 433 projetos nacionais e 95 projetos internacionais com base nas 22 unidades de

pesquisa distribuídas em suas instalações. A Figura 16, ilustra a organização da UA.

O processo de seleção pela Universidade Federal da Paraíba e Universidade de Aveiro, baseou-se em aspectos que consideraram tanto fatores pessoais como fatores técnicos que são favoráveis ao estabelecimento de uma análise comparativa de noções comportamentais em segurança da informação fundamentado na Teoria da Motivação de Proteção em sistemas culturais distintos, com evidência em um estudo transcultural.

De acordo com Carvalho e Borges (2012), a seleção por organizações em pesquisas que contemplam contextos de países diferentes, requer um desafio complementar, pelo fato dos processos organizacionais sofrerem influência substancial tanto do ambiente externo quanto do ambiente interno, o que implica em afirmar que a variação dessa influência é muito maior – em comparação com um mesmo contexto cultural de um único país – ao se considerar organizações que são atuantes em diferentes países, cuja variação é determinada pelas diferenças geográficas e históricas, pelos tipos e níveis de desenvolvimento industrial, sistemas de legislação, relações de trabalho e sistemas sociais e econômicos. Essa relação de aspectos técnicos foi definitiva para a escolha desse contexto de pesquisa devido à abrangência que essas variações irão proporcionar no momento da identificação dos fatores comportamentais. Ou seja, poderá permitir uma identificação ampla de fatores que contribuirá com a elaboração do modelo de comportamento preventivo. A diversificação de comportamento auxiliará na classificação de condutas preventivas perante uma dada ameaça aos ativos informacionais específicos de universidades, podendo, até mesmo, servir de modelo básico para mediações de ações de proteção em universidades atuantes em outras localidades do mundo, visto que a base das estruturas organizacionais universitárias são similares perante suas missões de ensino, pesquisa e extensão. Para que seja possível esse intuito, as investigações que compreendem a transculturalidade, necessitam que a pesquisa trabalhe com organizações que sejam equiparadas, por isso a opção de análise em universidades públicas, em países que possuam alguma semelhança em termos de história, e grau de desenvolvimento do setor de ensino superior (CARVALHO; BORGES, 2012).

3.3 UNIVERSO E AMOSTRA DA PESQUISA

O universo, ou população, da pesquisa consiste no total de elementos que apresentam as características comuns que corresponderão ao objeto de investigação (PARDAL; LOPES, 2011; VERGARA, 2006). Para a pesquisa proposta neste projeto, o universo será constituído pelos servidores (professores, pesquisadores e técnico-administrativos) que criam, manipulam e disseminam os ativos de informação, atuantes na estrutura subsequente ao reitor e vice-reitor, da

Universidade Federal da Paraíba (UFPB/Brasil) e Universidade de Aveiro (UA/Portugal).

Concernente à amostra, é importante considerar que a pesquisa proposta irá trabalhar com duas dimensões de abordagens: pesquisa quantitativa e pesquisa qualitativa, condição que exigirá da pesquisa o trabalho com dois tipos de amostras. A amostra, ou população amostral, corresponde a uma parte do universo escolhido, seguindo a sua seleção a partir de determinado critério de representatividade (VERGARA, 2006).

Em relação à pesquisa deste projeto, o critério de representativa que será conferido para o estabelecimento da amostra se fundamentará no sistema da amostra aleatória ou probabilística para a pesquisa quantitativa. Segundo Pardal e Lopes (2011, p. 56) "uma amostra probabilística é aquela que, recorrendo ao acaso, permite que cada um dos elementos do universo tenha probabilidade de integrar a amostra". Nesse sentido, a amostra probabilística corresponderá à totalidade de servidores que responderem ao questionário, e o retornarem à pesquisa, cuja validade se estabelecerá a partir da aplicação de cálculos estatísticos.

3.4 TÉCNICAS DE COLETA DE DADOS

Com o intuito de alcançar os objetivos propostos pela pesquisa apresentada neste projeto, será utilizada a estratégia de triangulação de técnicas de coleta de dados por permitir a combinação de múltiplas técnicas de pesquisa aptas à incorporar as dimensões qualitativas e quantitativas do objeto de estudo, de forma que consiga atender tanto aos requisitos do método qualitativo, de modo a sustentar a representatividade e diversidade dos posicionamentos dos grupos sociais que constituem o universo da pesquisa, quanto aos requisitos do método quantitativo, referente ao entendimento da magnitude e eficiência dos sistemas em pesquisa (AZEVEDO et al., 2013; BOUCHARD, 1976; GARNELO, 2006; HOPPER; HOQUE, 2006).

A pesquisa documental será utilizada com o intuito de atingir o objetivo específico de verificar as orientações legais aplicadas à segurança da informação na UFPB-BR e UA-PT.

Segundo Chizzotti (1991), documento pode ser definido como: qualquer informação sob a forma de textos, imagens, sons, sinais, entre outros, contida em um suporte material (papel, madeira, tecido, pedra), fixados por técnicas especiais como impressão, gravação, pintura, incrustação, entre outros. Qualsquer informações orais (diálogo, exposições, aula, reportagens faladas), tornam-se documentos quando transcritas em suporte material. A noção de documento corresponde a uma informação organizada sistematicamente, comunicada de diferentes maneiras (oral, escrita, visual ou gestualmente) e registrada em material durável.

A pesquisa documental recorre a materiais que ainda não receberam tratamento analítico, tais como: documentos oficiais, reportagem de jornais, contratos, relatórios, entre

Proteção. Por categorias, entende-se que são as rubricas sob as quais serão organizados os elementos do conteúdo, conforme grupos de relação de sentido (LAVILLE; DIONNE, 1999).

3.5 MÉTODO DE ANÁLISE DOS DADOS

Com base nessa primeira análise, serão aplicadas as técnicas da teoria das probabilidades, com o objetivo de estabelecer proposições probabilísticas do universo de pesquisa, a partir do estudo da amostra aleatória da pesquisa quantitativa. Nesse sentido, serão realizadas comparações dos cruzamentos de informações, de modo a testar as hipóteses. Ou seja, procedimento que permitirá gerar possíveis conclusões do universo de pesquisa, com base em comparações entre os resultados das amostras.

Os dados a serem coletados da ferramenta de formulários do Google e das cópias impressas do questionário serão transcritos diretamente para uma base de dados do Statistical Package for the Social Sciences (SPSS), versão 22, software utilizado em todas as análises estatísticas deste projeto de tese. Com o intuito de se realizar uma análise confiável e consistente, é fundamental que os dados coletados e inseridos na base de dados não possuam anomalias e/ou discrepâncias que os comprometam. Dessa forma, será necessário realizar uma inspeção criteriosa da base de dados, identificando as inconsistências e procedendo com as medidas necessárias para sua adequação. Aqui, será verificada, por exemplo, a existência de respostas em branco ou sem valores estabelecidos e a presença de respostas excessivas em uma mesma escala.Após a "limpeza dos dados", o coeficiente alfa de Cronbach, que avalia o grau de consistência entre múltiplas medidas de uma variável (HAIR et al., 2005), será usado com o intuito de estimar a confiabilidade do instrumento de pesquisa. Em geral, considera-se satisfatório um instrumento de pesquisa que obtenha alfa superior ou igual a 0.700 (HAIR et al., 2005). Depois de confirmada a confiabilidade do questionário, se dará início à análise descritiva, que tem como objetivo "sintetizar uma série de valores de mesma natureza, permitindo dessa forma que se tenha uma visão global da variação desses valores" (GUEDES et al., 2006). Serão aplicados testes gráficos (histogramas e outros), medidas de posição (moda, média, mediana e percentis) e medidas de dispersão (amplitude, variância e desvio-padrão). Em seguida, será realizada a análise de correlação dos construtos. O coeficiente de correlação de Pearson representa o grau de dependência linear entre duas variáveis.

Critério de Inclusão:

Para esta pesquisa estão incluídos todos os servidores ativos da Universidade Federal da Paraíba e Universidade de Aveiro.

Critério de Exclusão:

Todos os servidores da Universidade Federal da Paraíba e Universidade de Aveiro que não responderem ao questionário on-line.

Objetivo da Pesquisa:

Na avaliação dos objetivos apresentados os mesmos estão coerentes com o propósito do estudo:

Objetivo Primário:

Analisar o comportamento em segurança da informação dos servidores da Universidade Federal da Paraíba -UFPB/Brasil e da Universidade de Aveiro- UA/Portugal, sob a ótica da teoria de motivação de proteção.

Objetivos Secundários:

a) Verificar os requisitos legais aplicados à segurança da informação na UFPB-BR e UA-PT;
b) Compreender como os requisitos legais influenciam o comportamento em segurança da informação dos servidores da UFPB-BR e UA-PT;

c) Identificar quais os controles formais e informais são utilizados pelos servidores da UFPB-BR e da UA-PT, relacionados ao comportamento humano;

d) Identificar as causas de conformidade ou não conformidade dos servidores com a segurança da informação;

e) Desenvolver um modelo de comportamento preventivo para as universidades, baseado na teoria de motivação de proteção.

Avaliação dos Riscos e Benefícios:

Na avaliação dos riscos e benefícios apresentados estão coerentes com a Resolução 466/2012 CNS, item V "Toda pesquisa com seres humanos envolve riscos em tipos e gradações variadas. Quanto maiores e mais evidentes os riscos, maiores devem ser os cuidados para minimizá-los e a proteção oferecida pelo Sistema CEP/CONEP aos participantes.

No Item II.4 - benefícios da pesquisa - proveito direto ou indireto, imediato ou posterior, auferido pelo participante e/ou sua comunidade em decorrência de sua participação na pesquisa.

Riscos:

Não existem riscos que sejam previsíveis com relação à pesquisa, no entanto é preciso considerar a ocorrência de situações de constrangimento do participante ao responder o questionário. Se os servidor se sentir constrangido em algum momento ao responder ao questionário on-line, poderá desistir em qualquer tempo.

Benefícios:

Os benefícios da pesquisa proposta estão na conscientização sobre Segurança da Informação nas Universidades envolvidas -bem como em motivar os gestores a criar uma cultura de segurança da informação, por meio da implementação de ações de segurança da informação, relacionadas a dimensão humana.

Comentários e Considerações sobre a Pesquisa:

O presente projeto apresenta coerência científica, mostrando relevância para a academia, haja vista a ampliação do conhecimento, onde se busca, principalmente, analisar o comportamento em segurança da informação dos servidores da Universidade Federal da Paraíba -UFPB/Brasil e da Universidade de AveiroUA/Portugal, sob a ótica da teoria de motivação de proteção.

Considerações sobre os Termos de apresentação obrigatória:

Todos os Termos de Apresentação Obrigatória, foram anexados tempestivamente.

Recomendações:

RECOMENDAMOS QUE, CASO OCORRA QUALQUER ALTERAÇÃO NO PROJETO (MUDANÇA NO TÍTULO, NA AMOSTRA OU QUALQUER OUTRA), A PESQUISADORA RESPONSÁVEL DEVERÁ SUBMETER EMENDA SOLICITANDO TAL(IS) ALTERAÇÃO(ÕES), ANEXANDO OS DOCUMENTOS NECESSÁRIOS.

RECOMENDAMOS TAMBÉM QUE AO TÉRMINO DA PESQUISA A PESQUISADORA RESPONSÁVEL

CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA - CCS/UFPB

Continuação do Parecer: 5.146.542

UNIVERSIDADE FEDERAL DA PARAÍBA, RELATÓRIO FINAL E DOCUMENTO DEVOLUTIVO COMPROVANDO QUE OS DADOS FORAM DIVULGADOS JUNTO À INSTITUIÇÃO ONDE OS MESMOS FORAM COLETADOS, AMBOS EM PDF, VIA PLATAFORMA BRASIL, ATRAVÉS DE NOTIFICAÇÃO, PARA OBTENÇÃO DA CERTIDÃO DEFINITIVA.

Conclusões ou Pendências e Lista de Inadequações:

TENDO EM VISTA O CUMPRIMENTO DAS PENDÊNCIAS ELENCADAS NO PARECER ANTERIOR E A NÃO OBSERVÂNCIA DE NENHUM IMPEDIMENTO ÉTICO, SOMOS DE PARECER FAVORÁVEL A EXECUÇÃO DO PRESENTE PROJETO, DA FORMA COMO SE APRESENTA, SALVO MELHOR JUÍZO.

Considerações Finais a critério do CEP:

Certifico que o Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba – CEP/CCS aprovou a execução do referido projeto de pesquisa. Outrossim, informo que a autorização para posterior publicação fica condicionada à submissão do Relatório Final na Plataforma Brasil, via Notificação, para fins de apreciação e aprovação por este egrégio Comitê.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1838772.pdf	26/11/2021 11:25:42		Aceito
Outros	CARTA_RESPOSTA_COMPROVANDO_O_ATENDIMENTO_DAS_PENDENCIAS.docx	26/11/2021 11:20:31	SUENY LEDA ARAUJO RIBEIRO	Aceito
Outros	Questionario.docx	26/11/2021 11:19:19	SUENY LEDA ARAUJO RIBEIRO	Aceito
Projeto Detalhado / Brochura Investigador	PROJETO_DE_TESE.docx	26/11/2021 11:18:44	SUENY LEDA ARAUJO RIBEIRO	Aceito
Cronograma	Cronograma.docx	26/11/2021 11:15:58	SUENY LEDA ARAUJO RIBEIRO	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE.pdf	26/11/2021 10:13:20	SUENY LEDA ARAUJO RIBEIRO	Aceito

Endereço: Prédio da Reitoria da UFPB ¿ 1º Andar
Bairro: Cidade Universitária CEP: 58.051-900
UF: PB Município: JOAO PESSOA
Telefone: (83)3216-7791 Fax: (83)3216-7791 E-mail: comitedeetica@ccs.ufpb.br

CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA - CCS/UFPB

Continuação do Parecer: 5.148.542

Folha de Rosto	FolhaCentro.pdf	19/10/2021 19:28:09	SUENY LEDA ARAUJO RIBEIRO	Aceito
Outros	Ata_qualificacao.pdf	07/10/2021 17:19:56	SUENY LEDA ARAUJO RIBEIRO	Aceito
Outros	Certidao_PPGCI.pdf	07/10/2021 17:19:26	SUENY LEDA ARAUJO RIBEIRO	Aceito
Outros	Autorizacao_UA.pdf	07/10/2021 17:18:37	SUENY LEDA ARAUJO RIBEIRO	Aceito
Declaração de concordância	Autorizacao_UFPB.pdf	07/10/2021 17:17:44	SUENY LEDA ARAUJO RIBEIRO	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

JOAO PESSOA, 06 de Dezembro de 2021

Assinado por:
Eliane Marques Duarte de Sousa
(Coordenador(a))

Endereço: Prédio da Reitoria da UFPB ¿ 1º Andar
Bairro: Cidade Universitária **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** comitedeetica@ccs.ufpb.br