PROJETO DE GRADUAÇÃO

PERCEPÇÃO DE SEGURANÇA DIGITAL EM AMBIENTES DE TRABALHO: UMA ANÁLISE DE FATORES HUMANOS VIA PLS-SEM E IPMA

Por,
VITÓRIA OTT ROSEK
19/0039485

Brasília, 29 de junho de 2025.

UNIVERSIDADE DE BRASILIA

FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia
Departamento de Engenharia de Produção

PROJETO DE GRADUAÇÃO

PERCEPÇÃO DE SEGURANÇA DIGITAL EM AMBIENTES DE TRABALHO: UMA ANÁLISE DE FATORES HUMANOS VIA PLS-SEM E IPMA

Por,

VITÓRIA OTT ROSEK
19/0039485

Relatório submetido como requisito parcial para
obtenção do grau de Engenheiro de Produção

Banca Examinadora

Prof. Ari Melo Mariano, Ph.D.
UnB/ EPR(Orientador) _____

Prof. Dra. Márcia Terezinha Longen
Zindel EPR/FT/UnB _____

Prof. Dra. Maíra Rocha Santos
Adm/FACE/UnB _____

Brasília, 29 de junho de 2025.

Dedico este trabalho aos meus pais, por todo amor
e pelas oportunidades ao longo da jornada.

Tudo o que fizerem, façam de todo o coração, como para o Senhor, não para os homens.

Colossenses 3:23

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer a Deus, pois tudo o que tenho e sou é por causa dele. É Ele quem me capacita, me dá sabedoria e alegria para viver cada dia.

Em segundo lugar, agradeço à minha família. Sei que família a gente não escolhe, mas, se pudesse, eu os escolheria infinitas vezes. Aos meus pais, por sempre me apoiarem em tudo e serem meu porto seguro. Minha mãe, sempre tão amorosa e presente, você é a melhor mãe que eu poderia ter. Meu pai, que sempre me incentivou em tudo, principalmente nos estudos, é, para mim, um exemplo de dedicação e inteligência.

Lembro até hoje da história do funil, na qual, se olharmos do lado largo para o estreito, vemos pouca coisa; mas, se olharmos do lado estreito para o largo, conseguimos enxergar mais. Nossa visão se amplia com educação, e o conhecimento nos permite compreender melhor o mundo.

Ao meu irmão Henrique, que também é meu grande amigo, obrigada por estar sempre comigo, da infância à vida adulta. À minha cunhada Anne, que entrou depois na família, mas se tornou como uma irmã para mim. Aos meus parentes do Sul, distantes geograficamente, mas sempre próximos no coração.

Agradecimento especial aos meus professores do ensino primário, secundário e médio. Por vocês, sempre fui muito acolhida e incentivada. Vocês despertaram em mim o desejo de aprender e acreditaram no meu potencial mesmo quando eu não acreditava. Também me prepararam para o PAS, pelo qual consegui ingressar na UnB, uma universidade tão conceituada e pela qual serei eternamente grata.

Aos professores da graduação, sempre dispostos a me auxiliar com paciência e dedicação. Cada aula, cada orientação e cada conversa contribuíram não apenas para minha formação acadêmica, mas também pessoal.

Em especial, agradeço ao meu professor orientador, Ari Mariano, que, desde as primeiras disciplinas da graduação, já despertava em mim o desejo de tê-lo como orientador. Você torna o difícil fácil e ensina com clareza e entusiasmo. Obrigada por todo o apoio ao longo da universidade e, especialmente, nesses dois semestres de Projeto de Graduação. Sem você, este trabalho não seria possível.

Aos meus amigos da faculdade, sejam os que foram temporários, mas importantes, ou os que permanecem desde o primeiro semestre, com 17 anos de idade: Ana Beatriz, Amanda, Lucas Magno e Marina, obrigada por tornarem a jornada universitária mais leve.

Aos meus amigos da escola, carinhosamente apelidados de Amis, com quem posso ser eu mesma. E, à Mariana e à Maíra, amigas de outras fases da vida: vocês são minha segunda família.

Aos colegas do Centro Acadêmico e da Atlética, com quem compartilhei momentos de descanso e descontração entre as aulas, seja jogando sinuca ou participando de competições esportivas pelo time feminino. Esses momentos foram importantes para recarregar minhas energias ao longo da graduação.

Ao Grupo Gestão, Empresa Júnior de Engenharia de Produção, e a todas as pessoas incríveis que encontrei nesse percurso. Vocês me ensinaram a aprender sempre — e a me divertir no processo.

Ao meu diretor, Fabian, que compartilhou comigo sua paixão por cibersegurança e vive em prol da missão de construir um mundo digital mais seguro para todos. Obrigada por me apresentar uma área tão desafiadora, fascinante e necessária.

Agradeço também aos participantes da pesquisa, que contribuíram com generosidade para a construção deste trabalho.

A todos que, de alguma forma, estão presentes nestes agradecimentos, meu muito obrigada. Espero, um dia, poder retribuir o que recebi com tanto carinho.

RESUMO

Com o avanço da digitalização, a cibersegurança tornou-se um fator essencial nas organizações e a crescente dependência de ambientes digitais de trabalho demanda que os colaboradores adotem comportamentos seguros para mitigar riscos cibernéticos. Deste modo, o problema desta pesquisa foi compreender quais são os principais fatores que influenciam na percepção de segurança dos trabalhadores em um contexto de ambientes de trabalho digitais. Deste modo, o objetivo geral deste estudo foi estruturar recomendações práticas que contribuam para a melhoria da segurança digital nas organizações e fortalecimento da percepção de cibersegurança entre os colaboradores. Para alcançar o objetivo proposto, foi realizada uma pesquisa quantitativa de caráter explicativo por meio de equações estruturais, com 119 respondentes. O estudo foi uma adaptação do modelo de Saeed (2023). O modelo apresentado foi validado estatisticamente e o objetivo foi alcançado revelando que o fator mais relevante para a Percepção de Segurança foi o Suporte e Treinamento Organizacional, seguido por Gerenciamento de Segurança e Infraestrutura e Gerenciamento de Senhas, com 7,06% e 4,38% de influência na percepção de segurança, respectivamente. Os resultados foram utilizados para propor ações práticas baseadas em ferramentas da Engenharia de Produção, visando fortalecer a cultura de segurança digital nas organizações.

Palavras-chave: Cibersegurança, Fatores Humanos, Percepção de Segurança, PLS-SEM, Brasil.

ABSTRACT

With the advancement of digitalization, cybersecurity has become an essential factor in organizations, and the increasing reliance on digital work environments requires employees to adopt secure behaviors to mitigate cyber risks. Thus, the problem addressed in this research was to understand the main factors that influence workers' security perception in the context of digital work environments. The general objective of this study was to structure practical recommendations that contribute to improving digital security management in organizations and strengthening employees' perception of cybersecurity. To achieve this goal, an explanatory quantitative study was conducted using structural equation modeling (PLS-SEM), with a sample of 119 respondents. The study was based on an adaptation of the model proposed by Saeed (2023). The model was statistically validated, and the objective was achieved by revealing that the most relevant factor for the perception of security was Organizational Support and Training, followed by Infrastructure and Security Management and Password Management, with 7.06% and 4.38% influence on security perception, respectively. The results were used to propose practical actions based on Production Engineering tools, aiming to strengthen the digital security culture within organizations.

Keywords: Cybersecurity, Human Factors, Security Perception, PLS-SEM, Brazil.

SUMÁRIO

1. INTRODUÇÃO 14
1.1. PROBLEMA DA PESQUISA 15
1.2. JUSTIFICATIVA 15
1.3. OBJETIVOS 15
1.3.1. Objetivo Geral 15
1.3.2. Objetivos específicos 15
1.4. ESTRUTURA DOS CAPÍTULOS 16
2. REVISÃO DA LITERATURA (TEMAC) 17
2.1. PREPARAÇÃO DA PESQUISA 17
2.2. APRESENTAÇÃO E INTERRELAÇÃO DOS DADOS 18
2.3. DETALHAMENTO, MODELO INTEGRADOR E VALIDAÇÃO POR EVIDÊNCIAS 25
3. REFERENCIAL TEÓRICO 30
3.1. *CYBERSECURITY* 30
3.2. ENGENHARIA SOCIAL E COMPORTAMENTO HUMANO 31
3.3. MODELO E HIPÓTESE 33
3.3.1. Gerenciamento de Senhas 33
3.3.2. Gerenciamento de Segurança de Infraestrutura 34
3.3.3. Gerenciamento de E-mail 34
3.3.4. Política de Segurança Organizacional 35
3.3.5. Suporte e Treinamento Organizacional 35
3.3.6. Percepção de Segurança 35
4. MÉTODOS 39
4.1. TIPO DA PESQUISA 39
4.2. LOCAL DE PESQUISA 39
4.3. OBJETO DE ESTUDO 39
4.4. INSTRUMENTO DE COLETA DE DADOS 39

4.5. AMOSTRA 41
4.6. PROCEDIMENTO DE COLETA DE DADOS 42
4.7. TRATAMENTO DE DADOS 42
5. RESULTADOS 43
5.1. DESCRIÇÃO DA AMOSTRA 43
5.2. CÁLCULO DO MODELO 45
6. ANÁLISE E DISCUSSÃO DAS HIPÓTESES 53
6.1. DISCUSSÃO DAS HIPÓTESES 53
6.2. IMPLICAÇÕES PRÁTICAS 55
7. CONSIDERAÇÕES FINAIS, LIMITAÇÕES E FUTURAS LINHAS DE PESQUISA 64
8. REFERÊNCIAS BIBLIOGRÁFICAS 65
APÊNDICES 69
APENDICE A: INSTRUMENTO DE COLETA DE DADOS 69

LISTA DE FIGURAS

Figura 1 – Etapas TEMAC 17
Figura 2 – Mapa de coocorrência 19
Figura 3 – Publicação ano a ano indexada em *Web Of Science* 20
Figura 4 – Autores que mais publicaram 22
Figura 5 – Autores mais citados 23
Figura 6 – Publicação por países em *Web of Science* 23
Figura 7 – Presença das ODSs nas publicações em *Web of Science* 24
Figura 8 – Palavras mais frequentes nos títulos dos artigos 25
Figura 9 – Mapa de *Cocitation* 26
Figura 10 – Mapa de *Coupling* 27
Figura 11 – Modelo integrador 29
Figura 12 – Modelo teórico de SAEED 38
Figura 13 – Metodologia PLS 42
Figura 14 – Distribuição por gêneros da amostra 43
Figura 15 – Distribuição por faixa etária da amostra 44
Figura 16 – Distribuição por área de atuação da amostra 44
Figura 17 – Etapas de avaliação dos modelos 45
Figura 18 – Modelo estrutural 46
Figura 19 – Modelo Inicial de Confiabilidade de Item 47
Figura 20 – Modelo Final de Confiabilidade de Item 48
Figura 21 – Gráfico Importância VS Desempenho 56
Figura 22 – Ciclo PDCA 62

LISTA DE QUADROS

Quadro 1 – String de busca 18
Quadro 2 – Artigos mais citados 21
Quadro 3 – Artigos selecionados 28
Quadro 4 – Variáveis identificadas 32
Quadro 5 – Simulação HyveSystems 34
Quadro 6 – Construtos e Subconstrutos 37
Quadro 7 – Instrumento de Coleta (Questionário) 41
Quadro 8 – Matriz SWOT 58
Quadro 9 – SIPOC 60
Quadro 10 – KPIs 61

LISTA DE TABELAS

Tabela 1 – Indicadores da Confiabilidade Interna e Variância Média Extraída 49
Tabela 2 – Resultados Fornell-Larcker 50
Tabela 3 – Testes de Hipóteses 51

1. INTRODUÇÃO

A digitalização foi identificada como uma das principais tendências de mudança na sociedade como um todo e nas organizações. Adotar tecnologias digitais no ambiente de trabalho leva a mudanças no ambiente digital, devido à inserção de novas ferramentas tecnológicas (PARVIAINEN *et al.* 2017).

No início do século XX1, o mundo testemunhou a quarta revolução industrial, bem como a transformação digital do mundo dos negócios. A digitalização é muitas vezes considerada a força por trás da quarta revolução industrial, comumente denominada de Indústria 4.0, segundo exposto no trabalho de Ghobakhloo (2020).

Além disso, o acontecimento da pandemia do COVID-19 teve como provável consequência a aceleração da digitalização dos modelos de negócios e acelerou a necessidade de mudança em uma série de setores da economia (AMANKWAH-AMOAH *et al.* 2021). Tornou-se evidente, nos últimos tempos, que a pandemia do COVID-19 alterou fundamentalmente a operação de muitas organizações e empresas no mundo todo. A variedade de medidas tomadas durante a pandemia (como por exemplo, distanciamento social, quarentenas e lockdowns) forçou empresas a adaptar seus modelos de negócios, o que resultou na aceleração da digitalização no ambiente de trabalho (SOSTERO *et al.* 2020).

A crescente digitalização nos ambientes de trabalho gerou uma migração de serviços para a internet e mudanças para trabalho e operações remotas. Segundo Sostero (*et al.* 2020), essa migração, por sua vez, resultou em preocupações relacionadas à segurança, à privacidade e à capacidade de resistir a ameaças de ataques cibernéticos e hackers, ou mesmo a interrupções de internet.

Nesse contexto de adaptação de trabalhos tradicionais para ambientes de trabalho digitais, a cibersegurança surge como fator que corrobora com a digitalização dos ambientes de trabalho. Segundo Parviainen (*et al.* 2017), preocupações com segurança e insuficiência técnica, juntamente com a falta de uma estratégia de digitalização, são os obstáculos mais típicos para a digitalização nas organizações.

Desta maneira, compreender os fatores que influenciam a percepção de segurança dos trabalhadores e sua disposição para adotar comportamentos de cibersegurança é essencial em um contexto marcado por ambientes de trabalho digitais e pela crescente digitalização das organizações.

1.1. PROBLEMA DA PESQUISA

A pesquisa busca responder a seguinte questão: Quais são os principais fatores que influenciam na percepção de segurança dos trabalhadores em um contexto de ambientes de trabalhos digitais?

1.2. JUSTIFICATIVA

Do ponto de vista social, a pesquisa é relevante por tratar de um tema que afeta diretamente a segurança e a integridade de pessoas e organizações no ambiente digital. Em um cenário onde as ameaças cibernéticas estão cada vez mais frequentes e complexas, compreender como os colaboradores percebem e reagem às práticas de segurança é essencial para reduzir riscos operacionais, preservar a continuidade dos serviços e proteger dados de pessoas e empresas. Além disso, promover uma cultura com olhar voltado à cibersegurança contribui para relações de trabalho mais seguras e diminuição de prejuízos causados por falhas humanas.

A justificativa científica está respaldada pelo crescente número de publicações (no *Web of Science*), o que significa aumento no interesse sobre os fatores humanos envolvidos na segurança da informação. A evolução do volume de publicações aponta para uma expansão na pesquisa sobre esse tema, muito impulsionada pela digitalização dos ambientes de trabalho e crescente sofisticação dos ataques cibernéticos.

No campo da Engenharia de Produção, o tema é pertinente porque entender quais fatores influenciam a percepção de segurança dos colaboradores ajuda a identificar falhas de comportamento que podem afetar os processos, a produtividade e a gestão de riscos das organizações. Dessa forma, é possível explorar e propor soluções baseadas em ferramentas clássicas da área, como SIPOC, indicadores de desempenho (KPIs), planos de desenvolvimento individual (PDI) e o ciclo PDCA com intuito de estruturar, medir e aprimorar comportamentos digitais seguros no dia a dia do trabalho. Ao juntar os resultados da pesquisa com metodologias práticas consolidadas da Engenharia de Produção, o estudo contribui diretamente para reduzir vulnerabilidades humanas e fortalecer a cultura de segurança cibernética nas organizações.

1.3. OBJETIVOS

1.3.1. Objetivo Geral

O presente estudo tem por objetivo estruturar recomendações práticas que contribuam para a melhoria da gestão de segurança digital nas organizações e para o fortalecimento da percepção de cibersegurança entre os colaboradores.

1.3.2. Objetivos específicos

A fim de alcançar o objetivo geral, foi necessário dividi-lo em objetivos específicos:

- Delimitar o conceito de cibersegurança;
- Identificar os fatores humanos na cibersegurança;
- Consolidar o fatores encontrados na literatura em um modelo estrutural;

- Validar estatisticamente o modelo de pesquisa selecionado;
- Calcular fatores que mais influenciam a percepção de segurança.

1.4. ESTRUTURA DOS CAPÍTULOS

O presente estudo está estruturado da seguinte forma: o Capítulo 2 apresenta a revisão bibliográfica do tema estudado, por meio da Teoria do Enfoque Meta-Analítico Consolidado (TEMAC). O Capítulo 3 traz o referencial teórico, abordando conceitos relacionados à segurança da informação e aos fatores humanos na cibersegurança, além do modelo adotado neste trabalho. O Capítulo 4 descreve a metodologia utilizada na pesquisa. O Capítulo 5 apresenta os resultados e a validação do modelo. O Capítulo 6 aprofunda a análise das hipóteses e propõe implicações práticas para o tema. Por fim, o Capítulo 7 expõe as considerações finais, limitações do estudo e sugestões para pesquisas futuras.

2. REVISÃO DA LITERATURA (TEMAC)

Com a chegada da internet, a quantidade e disponibilidade de informações aumentou exponencialmente. Para uma pesquisa de qualidade, surge o desafio de identificar quais são as pesquisas mais relevantes, dentre um número cada vez maior de publicações disponíveis (Albrecht, Gurzki & Woisetschläger, 2017).

Dessa maneira, justifica-se a utilização de um método de revisão sistemático integrador de literatura, o TEMAC, que possui como principal objetivo melhorar a interação entre diferentes bases de dados e pesquisadores (Mariano e Rocha, 2017). O TEMAC (Teoria do Enfoque Meta-Analítico Consolidado) é uma teoria que mistura duas abordagens: a revisão da literatura e a bibliometria. Utiliza-se a qualificação da ciência por meio do Fator de Impacto, para observar quais revistas e periódicos são mais relevantes, levando em consideração também o número de citações das publicações.

A Revisão Bibliográfica serve para resgatar conhecimentos do passado para que uma nova publicação não seja igual à outras já publicadas e para que essa nova publicação tenha tido como embasamento os trabalhos mais relevantes acerca do assunto a ser aprofundado. O Enfoque Meta-Analítico busca o equilíbrio entre a análise qualitativa e quantitativa para mapear a literatura sobre o tema escolhido.

O TEMAC é dividido em três etapas: 1) Preparação da pesquisa, 2) Apresentação e interrelação dos dados e 3) Detalhamento, modelo integrador e validação por evidências, como pode ser observado na Figura 1 a seguir, de Mariano e Rocha:

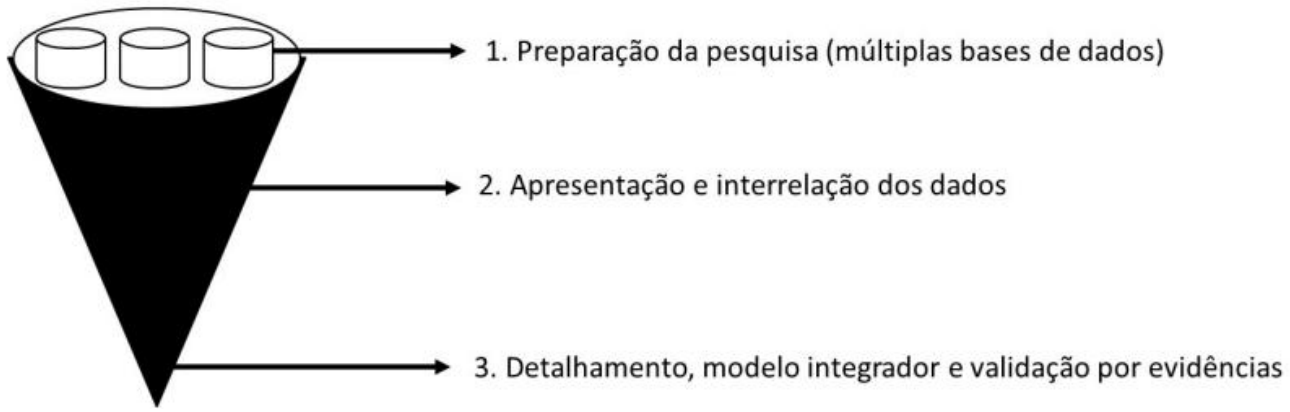


Figura 1 – Etapas TEMAC
Fonte – Mariano e Rocha (2017)

2.1. PREPARAÇÃO DA PESQUISA

Na primeira etapa, Preparação da pesquisa, as palavras-chave utilizadas na busca 1 foram *"Human Factors"* e *"Cybersecurity"* adicionando o operador lógico booleano *"AND"*. A base de dados utilizada foi *Web Of Science* (WoS), no período de todos os anos e foram encontrados 300 registros no total.

Busca	String de busca	Período	Tipo de documento	Áreas	Total de registros
1	*"Human Factors" AND "Cybersecurity"*	Todos os anos	Todos	Todas	300

Quadro 1 – String de busca
Fonte – Autoria Própria (2024)

2.2. APRESENTAÇÃO E INTERRELAÇÃO DOS DADOS

Na segunda etapa, Apresentação e interrelação dos dados, ordenou-se a busca pela data, do mais antigo para o mais recente. O registro mais antigo encontrado na busca é o trabalho dos autores Kc Claffy, Marina Fomenkov, Ethan Katz-Bassett, Robert Beverly, Beverly Cox e Matthew Luckie, publicado em Outubro de 2009, "The Workshop on Active Internet Measurements (AIMS) Report". Na publicação, os autores defendem a importância da coleta de dados no setor de redes, tendo em vista que os dados são absolutamente necessários para esse setor progredir, assim como acontece em qualquer outra ciência de sistemas complexos. Dessa forma, foi realizado um Workshop de colaboração com o intuito de maximizar os benefícios da pesquisa com um custo mínimo e os resultados, *insights* e recomendações encontrados no evento estão descritos no relatório dos autores.

No mapa de coocorrência de palavras-chave, observado na figura 2, pode-se perceber a mudança na temática ao longo dos anos, entre 2019 e 2021. Em 2019, *"Usable Security"*, *"Cyber Security"* e *"Decision-Making"* eram os temas mais importantes no período, e grande parte dos trabalhos tinham como preocupação o treinamento e a conscientização dos usuários, já que um dos elos mais fracos em ataques cibernéticos é justamente o comportamento humano. Além disso, discorrem sobre o processo de tomada de decisão como um dos fatores humanos que influencia na cibersegurança dos usuários.

Em 2020, *"Human Factors", "Internet Of Things", "Social Cybersecurity"* foram as palavras-chave com maior coocorrência e trouxeram o papel da interação humana em ataques cibernéticos. Nesse período, começam a aparecer com mais frequência os temas de 2FA (*Two Factor Authentication*), E-mails de SPAM e ataques de *phishing* que aproveitam-se de vulnerabilidades humanas e fatores comportamentais.

Em 2021, "*Behavior*", "*Systems*", "*Social Engineering*", "*Impact*", "*Policy*", "*Cyber Hygiene*" foram os temas que mais apareceram no período. Nas publicações, aparece o impacto da engenharia social e exploração da vulnerabilidade no comportamento humano e a utilização da persuasão e fatores emocionais para sucesso nos ataques cibernéticos. Além disso, enfatiza a perspectiva das características cognitivas do usuário (fator humano) nos sistemas de tecnologia, visto que é geralmente considerado a parte mais fraca do sistema e, portanto, mais vulnerável à ataques. Aparecem também os riscos das ameaças internas *(Insider threats)*, que são justamente usuários internos à organização que apresentam risco à cibersegurança do negócio, seja intencionalmente ou de maneira não intencional. Nesse contexto, o tema de *phishing* continua a

aparecer e surge também o conceito de higiene cibernética, que é a realização de adaptações nos sistemas para mitigar atividades online arriscadas.

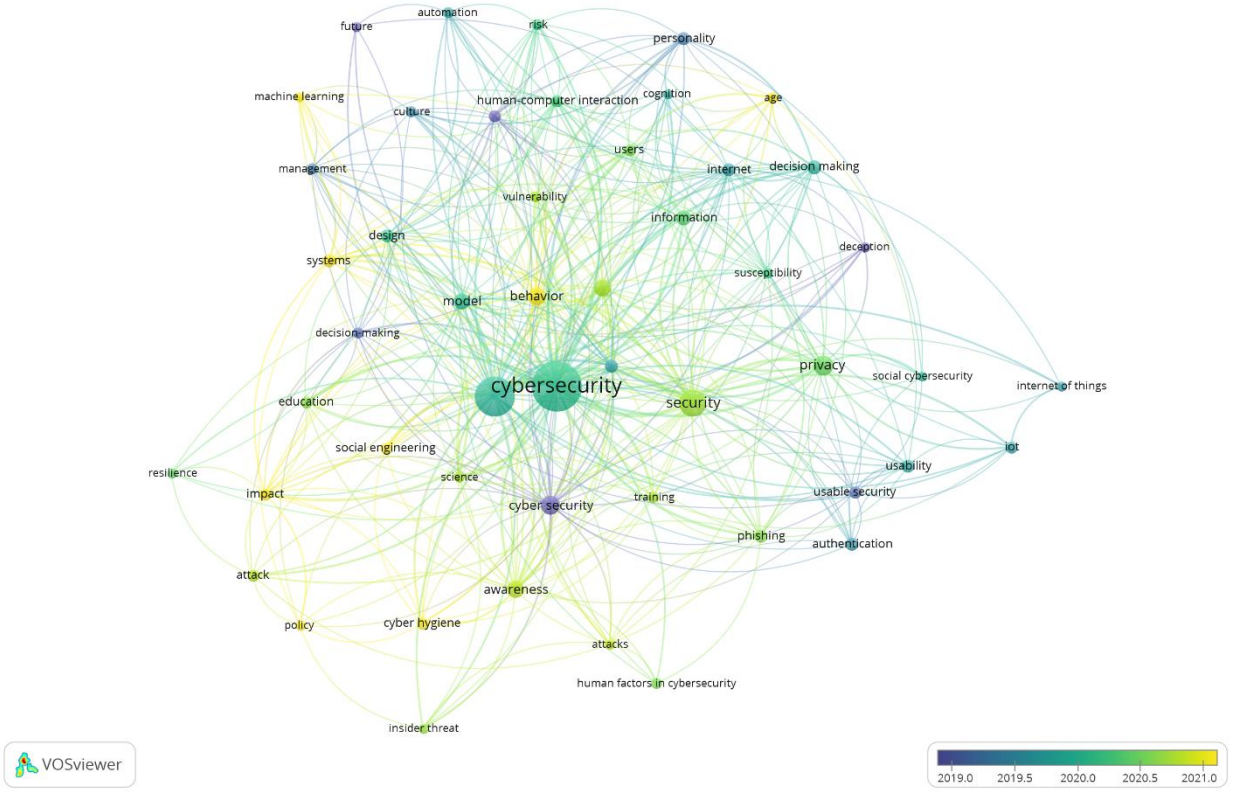


Figura 2 – Mapa de coocorrência

Fonte – *VOSvierwer* 1.6.18

Em relação aos registros ano a ano, observa-se na figura 3 que a quantidade de publicações possui uma tendência positiva, além de o tema ter começado a receber maior destaque a partir do ano de 2018.



Figura 3 – Publicação ano a ano indexada em *Web Of Science*

Fonte – Própria. Extraída de *Web Of Science*.

No período da pandemia (2020), houve uma queda no número de artigos publicados, mesmo assim ainda se manteve uma quantidade considerável de publicações, o que pode ser explicado pela relevância do tema cibersegurança em um contexto de migração do trabalho presencial para o formato do *home-office.*

Foram selecionados os cinco artigos com maior quantidade de citações no período indicado (quadro 2).

Autor	Título do artigo	Contribuições	Citações
Canfield, Casey Inez; Fischhoff, Baruch; Davis, Alex et al. (2016)	Quantifying Phishing Susceptibility for Detection and Behavior Decisions	Artigo com análises quantitativas do comportamento humano à ataques de *pishing* e traz como possível intervenção o feedback aos usuários com pior performance no estudo (aqueles mais suscetíveis aos *phishing*).	77
Pierce, James et al. (2019)	Smart Home Security Cameras and Shifting Lines of Creepiness A Design-Led Inquiry	Nesse artigo, o autor foca em câmeras de segurança domésticas inteligentes e suas questões de privacidade e segurança, pois essas câmeras funcionam por meio de aplicativos que contém informações digitais que podem ser vazadas.	70
Acar, Yasemin; Fahl, Sascha; Mazurek, Michelle	You Are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy	Os autores destacam a importância de melhorar a facilidade de uso das ferramentas de segurança para não só usuários finais, mas também para os	60

Autor	Título do artigo	Contribuições	Citações
L. et al. (2016)		próprios desenvolvedores responsáveis pela segurança dos softwares, pois eles também são suscetíveis aos fatores humanos.	
Evans, Mark; Maglaras, Leandros A.; He, Ying; Janicke, Helge et. al. (2016)	Human behaviour as an aspect of cybersecurity assurance	Os autores propõem um *framework* com técnicas e processos a serem seguidos para garantia da segurança cibernética levando em consideração os gaps de segurança identificados referentes aos fatores humanos.	55
Wen, Zikai Alex; Lin, Zhiqiu; Chen, Rowena; Andersen, Erik et al. (2019)	What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation	Nesse artigo, os autores discorrem acerca de um aplicativo, chamado What.Hack. Esse aplicativo ensina os conceitos teóricos de *phishing*, mas também realiza simulações práticas de ataques reais. Como contribuições, demonstram que o jogo é mais envolvente e eficaz do que treinamentos convencionais.	50

Quadro 2 – Artigos mais citados

Fonte - Autoria Própria (2024).

Pode-se observar que dois dos artigos mais citados centram-se em ataques de *phishing* e enfatizam a importância de feedbacks e treinamentos para prevenção desse tipo de ataque, ataque que explora a engenharia social como brecha para invasões cibernéticas em usuários comuns e organizações. A maior parte das publicações foca nos usuários finais, mas também temos a terceira publicação, que é mais voltada para os desenvolvedores de software como parte crucial na segurança digital.

O autor que mais publicou foi Proctor, com 6 trabalhos (figura 4).

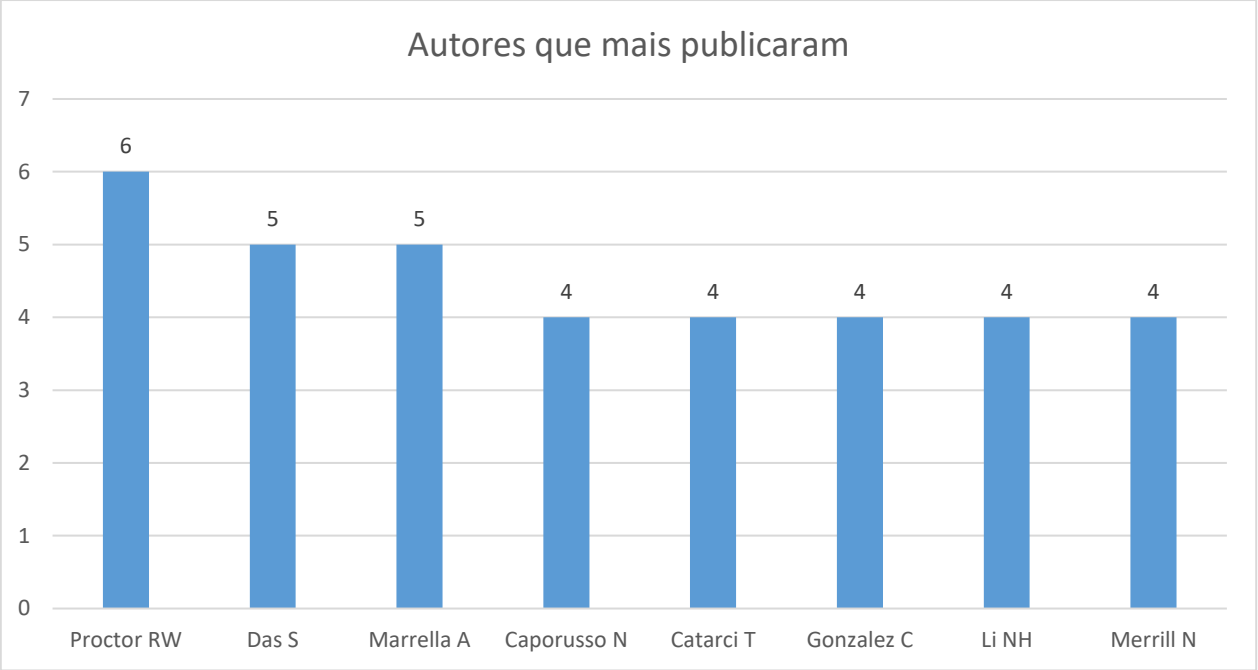


Figura 4 – Autores que mais publicaram
Fonte – Própria. Extraída de *Web Of Science*.

Proctor possui dois trabalhos focados em aplicativos móveis e dois em ataques de *phishing* por meio de páginas da Web. Em seus outros dois trabalhos, discorre sobre a tomada de decisão e IoT e seus fatores humanos na segurança digital. Já na parte de autores mais citados (figura 5), Proctor também lidera o ranking, o que mostra sua importância e relevância tanto em quantidade de artigos publicados quanto em quantidade de citações em relação ao tema de *cybersecurity.*

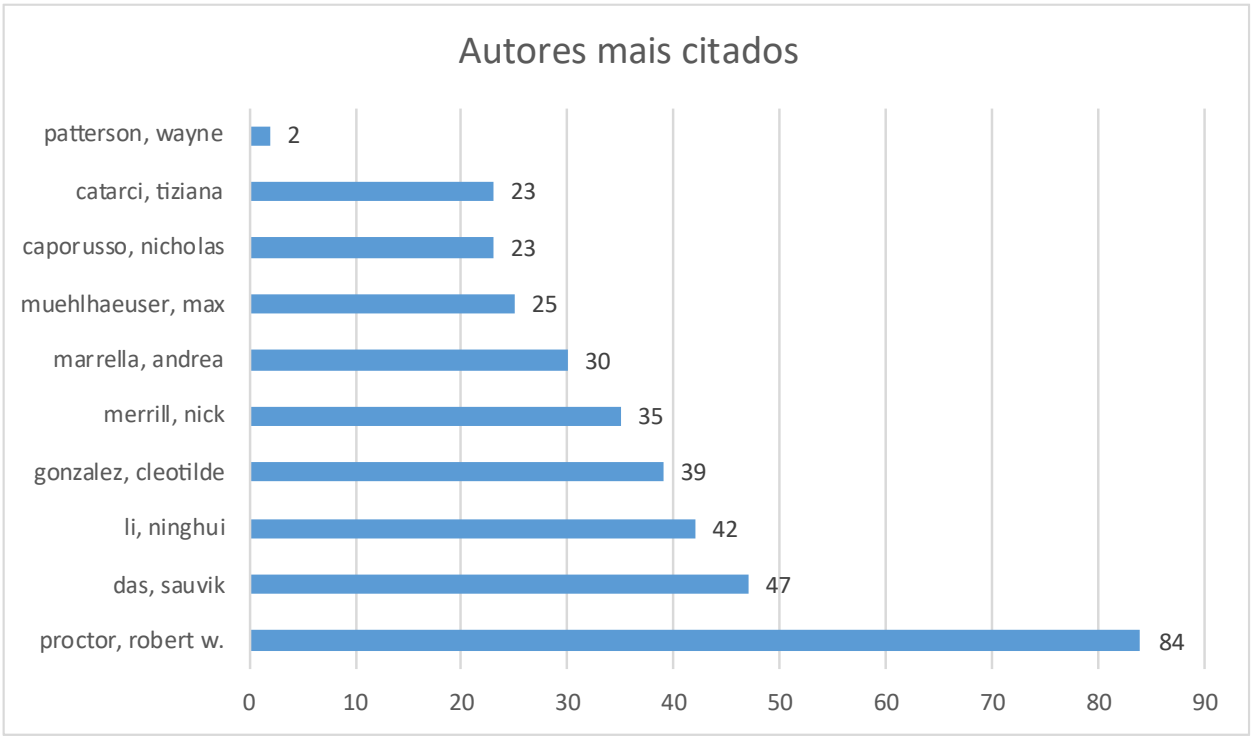


Figura 5 – Autores mais citados
Fonte – Própria. Extraída de *Web Of Science*.

Entre os países que mais publicaram estão Estados Unidos (48%), com 144 publicações, Inglaterra (12,65%) com 38 publicações e Alemanha (7,33%), com 22 publicações. O Brasil encontra-se na 42ª posição, com apenas uma publicação.



Figura 6 – Publicação por países em *Web of Science*
Fonte – Própria. Extraída de *Web of Science*.

Percebe-se que os EUA lideram o ranking de países com maior número de publicações, com mais de cem publicações a mais que os países seguintes, o que mostra que este país está oferecendo contribuições científicas na área.

Os ODSs (Objetivos de Desenvolvimento Sustentável) mais presentes nas publicações são 03) Saúde e Bem Estar (presente em 25 publicações), 11) Cidades e Comunidades Sustentáveis (presente em 9 publicações) e 04) Educação de Qualidade (presente em 8 publicações). Entretanto, em mais de 80% das publicações não contém menção à nenhuma dos 17 ODSs.

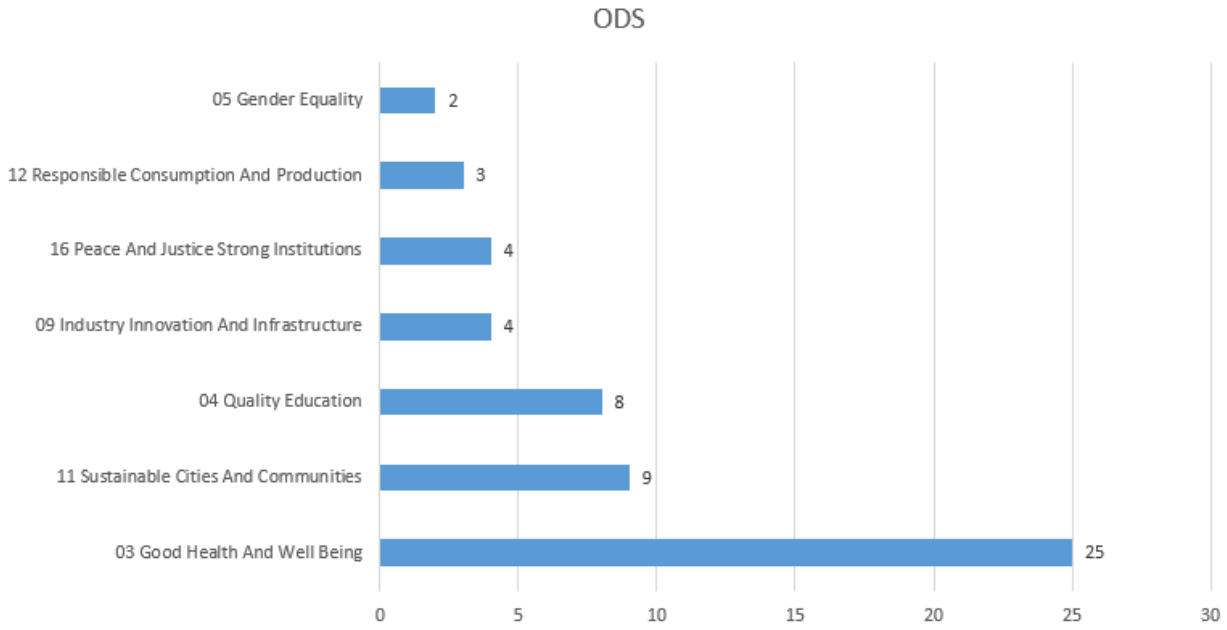


Figura 7 – Presença das ODSs nas publicações em *Web of Science*
Fonte – Própria. Extraída de *Web of Science*.

Foi realizada a consolidação das palavras que aparecem com mais frequência nos títulos das publicações. Como pode ser observado na Figura 8, as palavras mais frequentes foram *training, role, security, design* e *survey.*

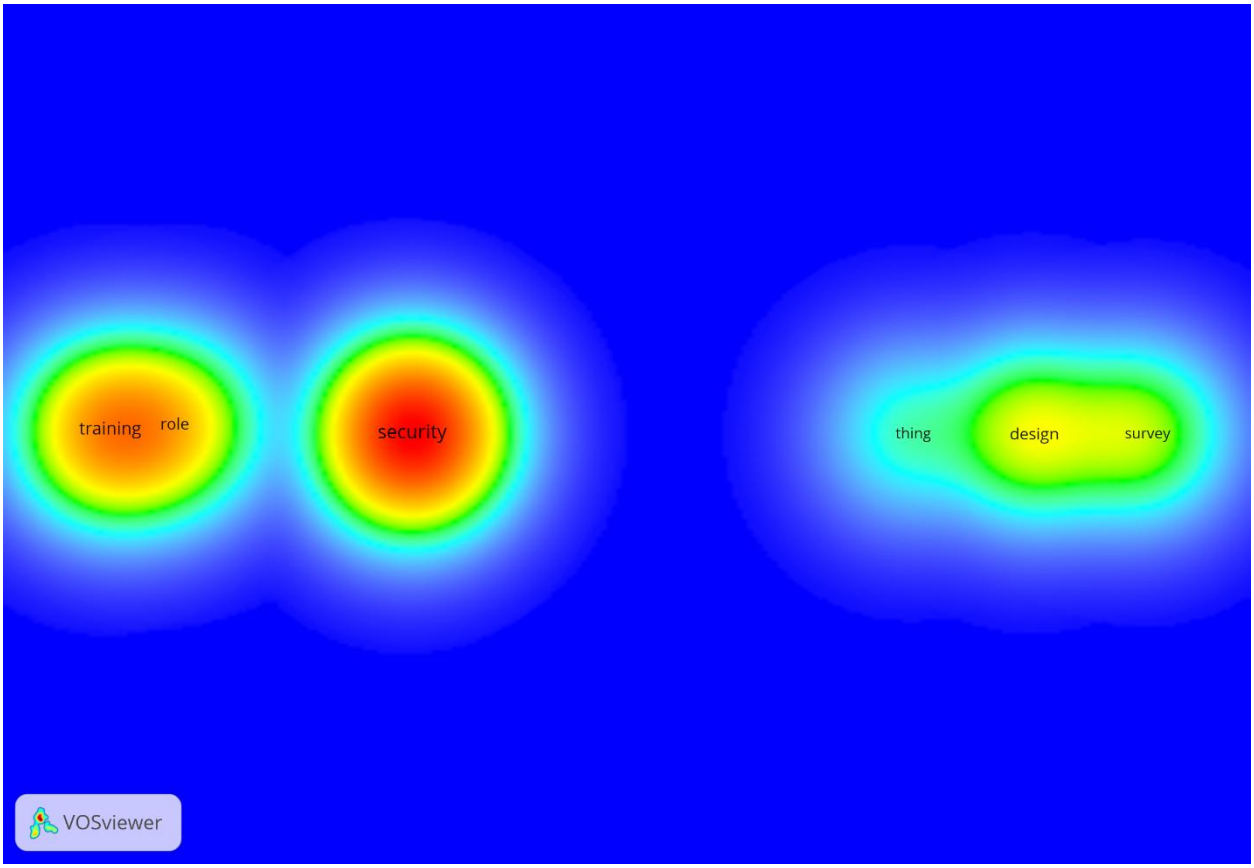


Figura 8 – Palavras mais frequentes nos títulos dos artigos
Fonte – Própria. Extraída de *Web Of Science*.

As palavras encontradas no mapa de calor (figura 8) retificam os resultados encontrados anteriormente, com o treinamento e conscientização como um dos fatores mais importantes para prevenção de ataques que utilizam engenharia social e exploram vulnerabilidades humanas. Também se destacam o *design* e facilidade de uso (tecnologias *user friendly*) como fatores relevantes na cibersegurança.

2.3. DETALHAMENTO, MODELO INTEGRADOR E VALIDAÇÃO POR EVIDÊNCIAS

A terceira etapa inicia-se com o detalhamento da pesquisa por meio dos mapas de *cocitation* e *coupling*. De acordo com Mariano e Rocha (2017), a análise de cocitação apresenta artigos que são citados juntos e, portanto, podem possuir semelhança entre os estudos. Já a análise de *coupling* traz quais frentes de pesquisa foram mais abordadas por meio de um acoplamento bibliográfico, além de seus anos de publicação, levando em consideração os três últimos anos.

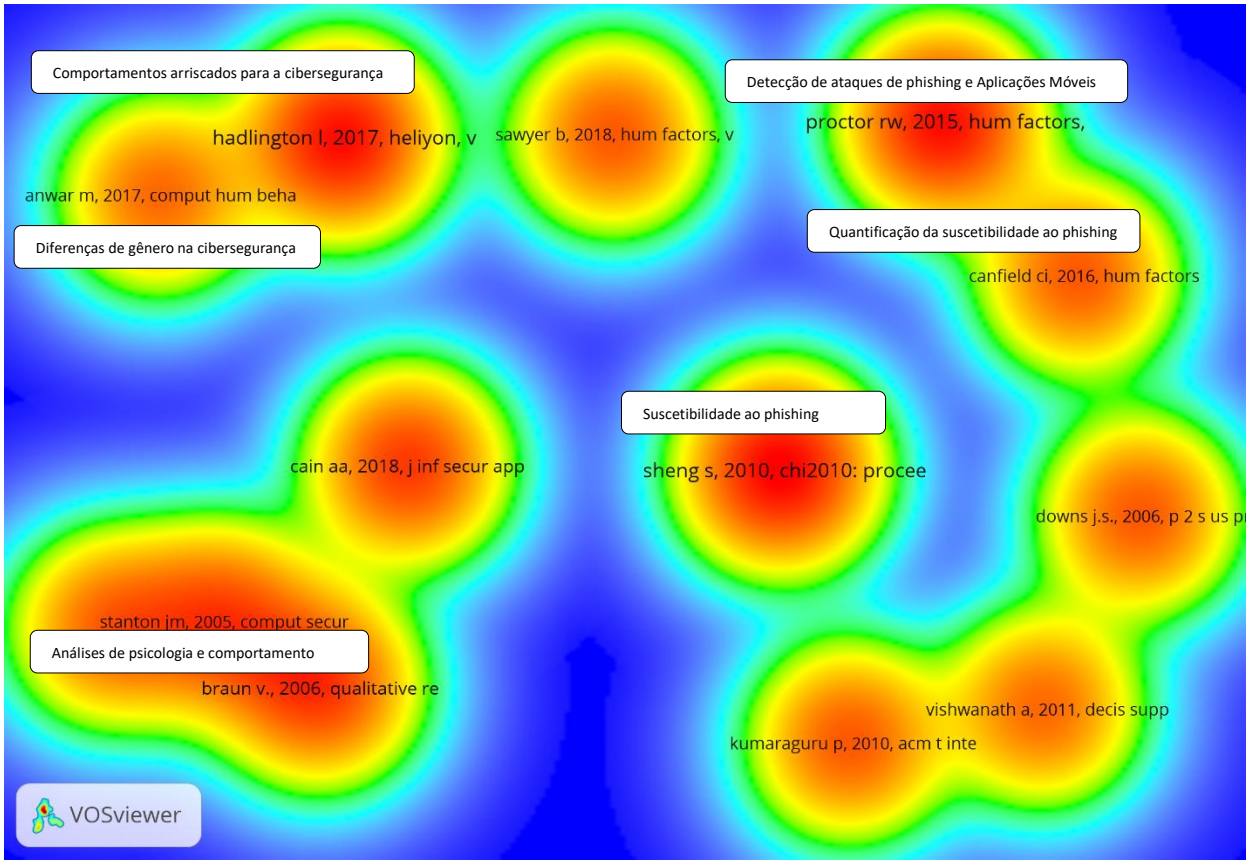


Figura 9 – Mapa de *Cocitation*
Fonte – Própria. Extraída do *Vosviewer*

O primeiro Cluster é formado por trabalhos que trazem o vício em internet, impulsividade e comportamentos considerados arriscados na cibersegurança (Hadlington et al., 2017) e diferenças de gênero na cibersegurança (Anwar et al., 2017).

O segundo Cluster contempla trabalhos com foco em análises do comportamento do usuário (Stanton et al., 2005) e análises qualitativas em psicologia (Braun et al., 2006).

O terceiro Cluster traz o tema de suscetibilidade aos ataques de *phishing* por meio de uma análise demográfica (Sheng et al., 2010).

O quarto Cluster também traz enfoque aos ataques de *phishing* e o comportamento humano e tomada de decisões como fatores explorados por esses ataques (Proctor et. al., 2015, Canfield et al., 2016).

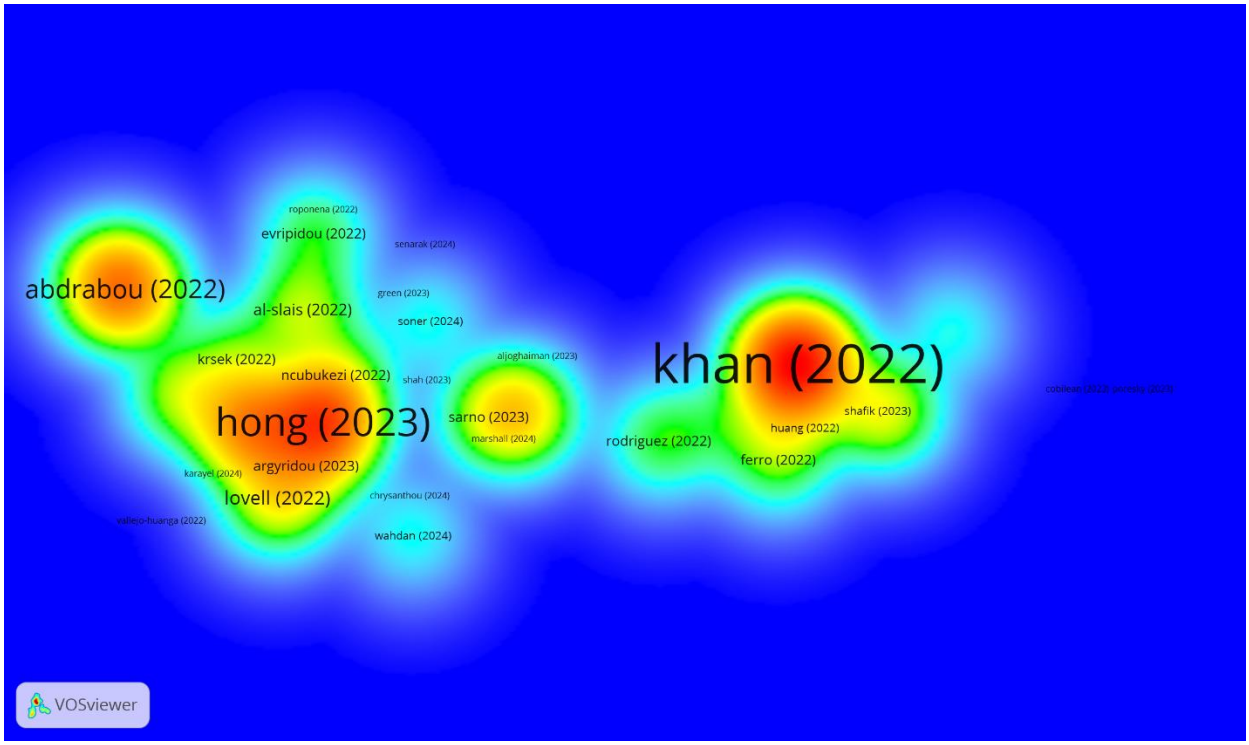


Figura 10 – Mapa de *Coupling*
Fonte – Própria. Extraída do *Vosviewer*

Na análise de *coupling*, o primeiro cluster representado por Abdrabou (2022) discorre acerca da reutilização de senhas como fator de risco à segurança digital e a traz um modelo de detecção de senhas reutilizadas com o principal objetivo de prevenir essa reutilização.

No segundo cluster aparece em destaque o trabalho de Hong (2023), que traz um modelo com as variáveis de conhecimento, atitude e comportamento e como esses fatores relacionam-se na cibersegurança. Também discorre acerca da influência social no ambiente de trabalho, que é capaz de remodelar a atitude das pessoas de maneira negativa, oferecendo mais riscos cibernéticos.

O terceiro cluster é representado pelo trabalho de Khan (2022). Nessa publicação, o autor comenta a crescente utilização de *Insider threats*, no caso do artigo, os *Insider Threats* não intencionais, como vetor para ataques cibernéticos.

A partir das três etapas e análise das publicações, foram reunidos os trabalhos mais condizentes com o tema. Além disso, foi realizado o *Snowballing*, que consiste na seleção de outros documentos a partir de citações presentes na seleção inicial (referências bibliográficas). Dessa maneira, foram selecionados 12 artigos (Quadro 3).

Autor/Ano	Artigo	Motivo da inclusão
Canfield; Fischhoff; Davis, et al. (2016)	Quantifying Phishing Susceptibility for Detection and Behavior Decisions	Um dos trabalhos mais citados e de acordo com o tema
Acar; Fahl; Mazurek et al. (2016)	You Are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy	Um dos trabalhos mais citados e de acordo com o tema
Evans; Maglaras; He; Janicke et. al. (2016)	Human behaviour as an aspect of cybersecurity assurance	Um dos trabalhos mais citados e de acordo com o tema
Wen; Lin; Chen; Andersen et al. (2019)	What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation	Um dos trabalhos mais citados e de acordo com o tema
Proctor; Chen et al. (2015)	The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace	Publicação de um dos autores mais citados e com mais publicações (Proctor, RW) e de acordo com o tema
Xiong; Proctor; Yang; Li et al. (2019)	Embedding Training Within Warnings Improves Skills of Identifying Phishing Webpages	Publicação de um dos autores mais citados e com mais publicações (Proctor, RW) e de acordo com o tema
Chong; Xiong; Proctor et al. (2019)	Human Factors in the Privacy and Security of the Internet of Things	Publicação de um dos autores mais citados e com mais publicações (Proctor, RW) e de acordo com o tema
Hadlington et al. (2017)	Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours	*Cocitation*
Stanton et al. (2005)	Analysis of end user security behaviors.	*Cocitation*
Khan; Houghton; Sharples et al. (2022)	Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks	*Coupling*
Welk et al.(2015)	Will the “Phisher-Men” Reel You In?: Assessing individual differences in a phishing detection task.	*Snowballing*
Uebelacker; Quiel et al. (2014)	The social engineering personality framework.	*Snowballing*

Quadro 3 – Artigos selecionados

Fonte – Autoria Própria (2024).

A partir do quadro 3, os 12 artigos foram estudados com o intuito de gerar o modelo integrador do estudo (Figura 11).

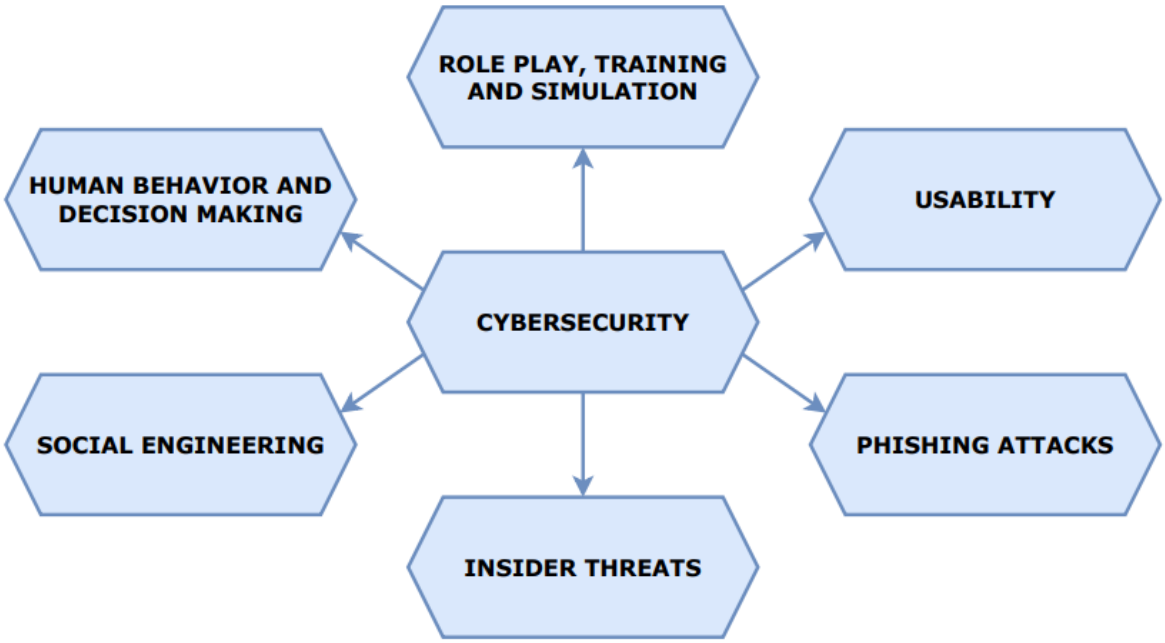


Figura 11 – Modelo integrador
Fonte – Autoria Própria (2024).

Pode-se perceber que as categorias do modelo integrador possuem forte relação entre si. O comportamento humano e a tomada de decisão são uns dos elos mais fracos em um sistema de cibersegurança e são uns dos principais fatores explorados pelos cibercriminosos. Esses criminosos utilizam técnicas de engenharia social para se beneficiar de vulnerabilidades humanas e de comportamento, sendo um dos principais vetores de incidentes cibernéticos os ataques de phishing, normalmente por meio de Insider threats não intencionais, que clicam em um link ou arquivo infectado e podem comprometer a segurança digital de uma organização inteira.

Dessa forma, algumas possíveis soluções mencionadas pelos estudos são melhorar a usabilidade nos sistemas de tecnologia, tanto para usuários finais quanto para desenvolvedores e focar em treinamentos e simulações de ataques para conscientizar os usuários e prevenir o sucesso nessas invasões, destacando a importância da educação cibernética no contexto atual.

3. REFERENCIAL TEÓRICO

O presente capítulo tem como objetivo apresentar os dados mais relevantes encontrados por meio do TEMAC e sua conexão com os Fatores Humanos na Cibersegurança. A partir da pesquisa realizada na etapa de Revisão da Literatura, tornou-se possível construir o embasamento teórico e o aprofundamento do tema escolhido.

3.1. *CYBERSECURITY*

Os ataques cibernéticos representam um dos efeitos globais de maior relevância e mais desestabilizadores na infraestrutura de tecnologia que permeia nossas vidas atualmente. A globalização e digitalização tornaram escaláveis tanto a propensão quanto a gravidade do cibercrime. Os impactos do cibercrime foram estimados em 945 bilhões de dólares na economia global, só em 2020 (Smith *et al*. 2020).

Vulnerabilidades cibernéticas trazem riscos significativos às corporações, sejam elas organizações privadas ou governamentais. Alguns exemplos desses riscos são interrupções na operação, vazamento ou sequestro de dados, perda de privacidade e prejuízos financeiros, além de perda de reputação (Sheehan *et al.* 2019).

Segundo o relatório *"The Second Annual Cost of Cyber Crime Study",* feito pelo Ponemon Institute, 98% das organizações tiveram experiência com ataques relacionados à *malwares*, 70% com ataques relacionados à *phishing* e engenharia social, 63% com ataques relacionados à códigos maliciosos, 55% com ataques relacionados à *botnets*, 50% com ataques relacionados à roubo de dispositivos e 41% com ataques relacionados à *insiders* maliciosos (Ponemon Institute, 2016).

Tendo em vista os dados apresentados acima, percebe-se a relevância do cibercrime no contexto de um ambiente globalizado e digitalizado e os diversos prejuízos decorrentes da exploração de vulnerabilidades cibernéticas em organizações.

Nesse contexto, as organizações prezam por criar um ambiente seguro. Esse ambiente seguro se trata de um esforço conjunto entre usuários e organizações (que também estão divididas em equipe de risco/segurança e os colaboradores). Cada um destes atores por sua vez deve observar duas diferentes perspectivas relacionadas à segurança cibernética: a. a primeira são as questões técnicas e um b. segundo aspecto, de comportamental ou não técnico, apropriadamente referido como o fator humano (Onumo *et al*. 2018).

Apesar do fator humano ser o maior responsável pelos crimes cibernéticos, os estudos sobre ele são menores. Chanda *et al.* (2025) explicam que os fatores humanos são explorados em aproximadamente 54% das violações de dados organizacionais.

Assim, os usuários finais dentro das organizações têm sido frequentemente vistos como o elo mais fraco da segurança cibernética por apresentarem alguns comportamentos inseguros, como a criação de senhas

fracas, acesso a links de *phishing* ou o compartilhamento de informações em redes vulneráveis, expondo os sistemas a riscos (Zimmermann *et al.* 2024). Essas ações são realizadas por meio do que se conhece como Engenharia Social.

3.2. ENGENHARIA SOCIAL E COMPORTAMENTO HUMANO

A Engenharia Social é a uma grande ameaça cibernética porque ela explora o elo mais fraco em qualquer sistema de segurança, que é o elemento humano. Uma organização pode possuir excelentes sistemas de segurança, mas as pessoas sempre estão envolvidas em parte da operação. Dessa maneira, se as pessoas não possuem uma higiene de segurança cibernética, podem colocar toda uma organização em risco e tornar todo o sistema vulnerável à ataques que utilizam engenharia social (Long, 2013).

Tendo em vista o contexto e importância global da cibersegurança e seus fatores humanos, surgem modelos para mensurar o comportamento humano na cibersegurança. Para identificar os fatores que mais influenciam o comportamento na cibersegurança, foram levantadas as variáveis mais recorrentes na revisão da literatura, disponível no Quadro 4.

Variável	Definição	Fonte(s)
Gerenciamento de Senhas	Criação, reutilização, armazenamento e compartilhamento de senhas	Saeed (2023)
Gerenciamento de Infraestrutura de Segurança	Infraestrutura referente à antivírus, firewall, anti-spyware, scripting, aplicações e bloqueio de tela	Saeed (2023)
Gerenciamento de E-mail	Abertura de E-mails desconhecidos, como anexos e links suspeitos	Saeed (2023), Tam et al. (2022)
Política de Segurança Organizacional e Política de segurança da informação e compliance	Políticas de segurança das organizações, como processos a serem seguidos para uma melhor segurança	Saeed (2023), Nawankpa et al. (2023)
Suporte e treinamento organizacional	Suporte da equipe técnica e treinamentos de cibersegurança	Saeed (2023)
Percepção de Segurança	Percepção do usuário em relação à segurança	Saeed (2023)
Trabalho Remoto	Trabalho remoto realizado fora do ambiente do escritório/ sede da organização	Nawankpa et al. (2023)
Tomada de providências baseada em segurança	Tomada de ações de precaução relacionadas à segurança cibernética	Nawankpa et al. (2023)
Conscientização de segurança	Reconhecimento e conscientização de práticas de segurança pelo usuário	Nawankpa et al. (2023), Tam et al. (2022)
Práticas e comportamento em cibersegurança	Práticas como atualizações, utilização de antivírus, abertura de E-mails desconhecidos, checagem de URLs e HTTPSs, mudança de senhas e utilização de 2FA (Two-factor Atuthentication)	Alanazi et al (2022)
Intenção de práticas de cibersegurança	Intenção do usuário em adotar práticas de cibersegurança	Alanazi et al (2022), Tam et al. (2022)
Atitude em relação à práticas de cibersegurança	Atitude em relação às práticas, se elas são benéficas ao usuário, desagradáveis ou inúteis	Alanazi et al (2022), Tam et al. (2022)
Normas subjetivas (influência social)	O que as outras pessoas acreditam e esperam do comportamento do usuário	Alanazi et al (2022), Tam et al. (2022)
Percepção de controle de comportamento (auto eficácia e controlabilidade)	Facilidade, confiança e presença de recursos para seguimento de práticas de segurança	Alanazi et al (2022), Tam et al. (2022)

Variável	Definição	Fonte(s)
Percpepção e conscientização sobre ameaças cibernéticas	Conhecimento da existência de cyber threats e riscos online e da importância de práticas de cibersegurança	Alanazi et al (2022), Tam et al. (2022)
Nível de habilidades na internet e conhecimento informativo	O quanto o usuário possui habilidades onlines e conhecimentos acerca de segurança da informação	Alanazi et al (2022)
Conhecimento de ameaças cibernéticas	Conhecimento dos conceitos de E-mail Worm, Trojan Horse, E-mail Spam, Phishing, DoS (Denial-of-service), Engenharia Social e Incidentes de Segurança	Alanazi et al (2022)
Congruência de valores subjetivos	Sentimentos em relação à empresa de trabalho, sentimento de pertencimento ao time e importância na empresa	Tam et al. (2022)
Satisfação em relação ao trabalho	Nível de satisfação geral em relação ao trabalho, felicidade, satisfação e vontade de permanência no mesmo	Tam et al. (2022)

Quadro 4 – Variáveis identificadas
Fonte – Autoria Própria (2024).

Nifakos et al. 2024 explicam que compreender a Engenharia Social tornou-se indispensável para uma compreensão mais ampla dos riscos cibernéticos decorrentes de comportamentos humanos inseguros, algo que os métodos tradicionais de avaliação de risco, focados no perfil de segurança dos sistemas de TI, não abordavam plenamente.

Para compreender esse processo, muitos trabalhos, como os apresentados no Quadro 4, fazem a utilização de TPB (*Theory of Planned Behavior*), teoria que assume que certas variáveis afetam a intenção de comportamento de um indivíduo. Essa teoria, proposta por Ajzen (2002), parte da ideia de que a intenção de agir de uma pessoa é influenciada por três fatores: sua atitude em relação ao comportamento, a pressão social percebida (norma subjetiva) e o quanto ela acredita que tem controle sobre a ação (controle comportamental percebido) Nesse caso em específico, referem-se à intenção de comportamento do usuário em relação a práticas preventivas de cibersegurança . No contexto deste trabalho, isso significa entender o que leva os colaboradores a possuirem uma percepção positiva em segurança da informação e adotarem comportamentos seguros no ambiente digital. A TPB tem sido amplamente usada em pesquisas de segurança da informação justamente por ajudar a analisar como esses fatores influenciam diretamente práticas de cibersegurança no dia a dia das organizações.

O modelo que mais se adequa ao estudo é o modelo de Saaed (2023), visto que ele analisa uma maior quantidade de variáveis relevantes, como por exemplo, o gerenciamento de E-mails e suporte e treinamento organizacional, fatores que estiveram muito presentes na revisão da literatura por meio do TEMAC. Além disso, o modelo é baseado na Teoria do Comportamento Planejado (TPB) e combina fatores organizacionais e comportamentais, o que ajuda a entender melhor o que influencia o a percepção de segurança e o

comportamento seguro dos colaboradores em ambientes digitais de trabalho. Por esses motivos, ele foi escolhido como base para a construção do modelo deste trabalho.

3.3. MODELO E HIPÓTESE

A partir da adaptação do modelo de Saaed (2023), este trabalho seis cinco construtos relacionados ao comportamento de Segurança da Informação de Trabalhadores em um contexto de Ambientes de Trabalho Digitais:

1. Gerenciamento de Senhas;
2. Gerenciamento de Segurança de Infraestrutura;
3. Gerenciamento de E-mail;
4. Política de Segurança Organizacional;
5. Suporte e Treinamento Organizacional;
6. Percepção de Segurança.

A seguir estão dispostas explicações e definições, além das hipóteses a respeito de cada um dos construtos. Cada hipótese é uma afirmação que será testada nas etapas subsequentes.

3.3.1. Gerenciamento de Senhas

Um gerenciamento de senhas efetivo é de suma importância para uma melhor segurança digital. A empresa de cibersegurança HiveSystems (2024) simulou quanto tempo leva para um hacker descobrir sua senha, a depender de algumas variáveis na senha, como presença de números, letras minúsculas, maiúsculas e símbolos, além da quantidade de caracteres. Segundo a simulação feita pela empresa, senhas pequenas e pouco complexas são facilmente (e até instantaneamente) descobertas por cibercriminosos e aumentam o risco de ataques cibernéticos, invasões e vazamento de dados.

Quanto tempo leva para um hacker descobrir sua senha?					
Número de caracteres	**Apenas números**	**Letras minúsculas**	**Minúsculas e Maiúsculas**	**Números, letras minúsculas e maiúsculas**	**Números, letras minúsculas, maiúsculas e símbolos**
4	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
5	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
6	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
7	Instantaneamente	Instantaneamente	2 segundos	7 segundos	31 segundos
8	Instantaneamente	Instantaneamente	2 minutos	7 minutos	39 segundos
9	Instantaneamente	10 segundos	1 hora	7 horas	2 dias
10	Instantaneamente	4 minutos	3 dias	3 semanas	5 meses

Quanto tempo leva para um hacker descobrir sua senha?					
Número de caracteres	**Apenas números**	**Letras minúsculas**	**Minúsculas e Maiúsculas**	**Números, letras minúsculas e maiúsculas**	**Números, letras minúsculas, maiúsculas e símbolos**
11	Instantaneamente	2 horas	5 meses	3 anos	34 anos
12	2 segundos	2 dias	24 anos	200 anos	3 mil anos
13	19 segundos	2 meses	1 mil anos	12 mil anos	202 mil anos
14	3 minutos	4 anos	64 mil anos	750 mil anos	16 milhões de anos
15	32 minutos	100 anos	3 milhões de anos	46 milhões de anos	1 bilhão de anos
16	5 horas	3 mil anos	173 milhões de anos	3 bilhões de anos	92 bilhões de anos
17	2 dias	69 mil anos	9 bilhões de anos	179 bilhões de anos	7 trilhões de anos
18	3 semanas	2 milhões de anos	467 bilhões de anos	11 trilhões de anos	438 trilhões de anos

Quadro 5 – Simulação HyveSystems
Fonte – Adaptado de HyveSystems (2024)

Além da simulação da HiveSystems, que evidencia a fragilidade de senhas fracas frente a ataques, a literatura científica também destaca que o gerenciamento de senhas vai muito além do conhecimento técnico. Segundo Tam, Glassman e Vandenwauver (2010), os usuários geralmente sabem o que torna uma senha forte ou fraca, mas ainda assim mantêm hábitos inseguros por priorizarem a conveniência. Comportamentos como reutilizar senhas, anotar em papéis ou compartilhar com colegas são motivados não pela ignorância, mas pela sensação de que os riscos não os afetam diretamente. Esse comportamento é um reflexo do *trade-off* entre segurança e conveniência/ usabilidade, que impacta a percepção individual sobre segurança digital. Assim, um gerenciamento de senhas é essencial para assegurar uma maior percepção da segurança na hipótese 1:

H1: Um gerenciamento de senhas efetivo leva a uma positiva percepção da segurança.

3.3.2. Gerenciamento de Segurança de Infraestrutura

Segundo o *National Institute of Standards and Technology* a resiliência de uma infraestrutura refere-se à capacidade de uma organização antecipar, resistir, adaptar-se e/ou recuperar rapidamente de qualquer ataque cibernético, atividades cibercriminosas, vandalismo cibernético, sabotagem cibernética, espionagem cibernética, acidentes, ameaças que ocorrem naturalmente ou falha de infraestrutura induzida por erro humano (NIST, 2020). Dessa maneira, um gerenciamento da segurança da infraestrutura é de suma importância para uma maior segurança cibernética, gerando a hipótese 2:

H2: Um gerenciamento de recursos de infraestrutura de segurança efetivo leva a uma positiva percepção da segurança.

3.3.3. Gerenciamento de E-mail

Segundo o Dr. Markus Jakobsson, pesquisador de segurança e cientista principal de consumo na Paypal, *phishing* é uma forma de engenharia social em que um invasor, também conhecido como *phisher*, realiza tentativas de recuperar de maneira fraudulenta as credenciais de usuários legítimos ou outras credenciais sensíveis imitando comunicações eletrônicas confiáveis. Essas comunicações são feitas com mais frequência através de E-mails que direcionam os usuários para sites fraudulentos que, por sua vez, coletam as credenciais desejadas. Existem diversos tipos de ataques de *phishing*: *Deceptive Phishing*, no qual são enviados E-mails em massa com um *call to action* para clicar em links maliciosos, *Spear Phishing*, que consiste em um phishing focado e direcionado a uma única pessoa, departamento ou organização e o *Content-Injection Phishing*, no qual o cibercriminoso insere conteúdos maliciosos em um website legitimo. Nesse sentido, o gerenciamento de E-mail é um fator relevante na segurança cibernética, já que é um dos principais vetores de ataques de *phishing* (JAKOBSSON, 2006).

Tendo em vista que o E-mail é um dos principais vetores de ataques de phishing, como exposto acima, um gerenciamento de E-mail é essencial na cibersegurança, gerando a hipótese 3:

H3: Um gerenciamento de atividades de E-mail apropriado leva a uma positiva percepção da segurança.

3.3.4. Política de Segurança Organizacional

As políticas são especialmente importantes para a segurança dos sistemas de informação, pois fornecem os modelos e processos necessários para implementar práticas seguras em uma organização (VON SOLMS, 2004). O principal objetivo da política é fornecer gerenciamento, direção e suporte para segurança da informação de acordo com os requisitos da operação de cada negócio e conformidade com regulamentos e leis relevantes (ISO/IEC, 2005), como por exemplo, a LGPD (Lei Geral de Proteção de Dados), em vigor no Brasil.

Dessa forma, uma boa política de segurança organizacional é relevante percepção de segurança das organizações, gerando a hipótese 4:

H4: Políticas de segurança organizacionais levam a uma positiva percepção da segurança.

3.3.5. Suporte e Treinamento Organizacional

Um componente essencial de uma estratégia de segurança cibernética da organização é aumentar a conscientização e a educação sobre ameaças on-line e como proteger dados e serviços corporativos (BADA, 2019). O suporte e treinamento pode consistir na conscientização da política de segurança existente na organização e na realização de simulações práticas de ataques de *cybersecurity* (WEN, 2019).

Assim, suporte e treinamentos organizacionais efetivos são importantes para uma maior segurança cibernética, gerando a hipótese 5:

H5: Suporte e treinamentos organizacionais levam a uma positiva percepção da segurança.

3.3.6. Percepção de Segurança

A percepção de segurança consiste nas sensações dos usuários em relação à segurança digital, como por exemplo, o sentimento de segurança, se eles acreditam que são capazes de proteger-se ou não digitalmente e se possuem confiança na capacidade de lidar com ameaças cibernéticas.

Dessa maneira, as hipóteses utilizadas no estudo em questão são:

H1: Um gerenciamento de senhas efetivo leva a uma positiva percepção da segurança.

H2: Um gerenciamento de recursos de infraestrutura de segurança efetivo leva a uma positiva percepção da segurança.

H3: Um gerenciamento de atividades de E-mail apropriado leva a uma positiva percepção da segurança.

H4: Políticas de segurança organizacionais levam a um a uma positiva percepção da segurança.

H5: Suporte e treinamentos organizacionais levam a uma positiva percepção da segurança.

No quadro 6 podem ser observados os itens referentes à cada um dos seis construtos.

Gerenciamento de Senhas
Reutilização de uma única senha
Alteração de senha apenas quando obrigatório pela política organizacional
Nova senha semelhante à senha antiga
Armazenamento de senha em papel ou arquivo eletrônico
Armazenamento de senha em um software de gerenciamento de senhas
Compartilhamento de senha com colegas
Gerenciamento de Segurança de Infraestrutura
Presença de antivírus
Atualização de antivírus
Utilização de Firewall
Utilização de *anti-spyware*
Permissão de *scripting*
Bloqueio de computador enquanto distante do mesmo
Bloqueio de tela protegido por senha
Utilização de redes sociais
Gerenciamento de E-mail
Abertura de E-mails desconhecidos
Abertura de anexos de E-mails desconhecidos
Utilização de criptografia no E-mail
Análise das configurações de segurança de software baseado na Web
Política de Segurança Organizacional
Atenção à segurança do computador
Presença de política de segurança organizacional
Entendimento da política de segurança organizacional
Desvio da política de segurança organizacional
Percepção do desvio da política de segurança organizacional pelos colegas
Repercussões de violações na política de segurança
Suporte e Treinamento Organizacional
Disponibilidade de suporte técnico
Provisão de treinamento
Melhor compreensão da política de segurança devido ao treinamento
Percepção de Segurança
Computador pessoal é seguro
Eu consigo proteger meu computador
Segurança de computador é preocupante
Atenção especial à segurança faz diferença
Hacking é inevitável

Quadro 6 – Construtos e Subconstrutos

Fonte – SAEED (2023)

O modelo escolhido foi baseado no modelo de Saeed (2023), um estudo quantitativo empíricos pós pandemia do COVID-19, em um contexto no qual muitos dos trabalhadores migraram para o trabalho remoto, vários deles utilizando computadores pessoais para trabalhar, fator que os deixa menos protegidos para ameaças cibernéticas. O foco do trabalho foi entender as práticas de segurança dos trabalhadores da Arábia Saudita por meio dos seis construtos apresentados (SAEED, 2023).

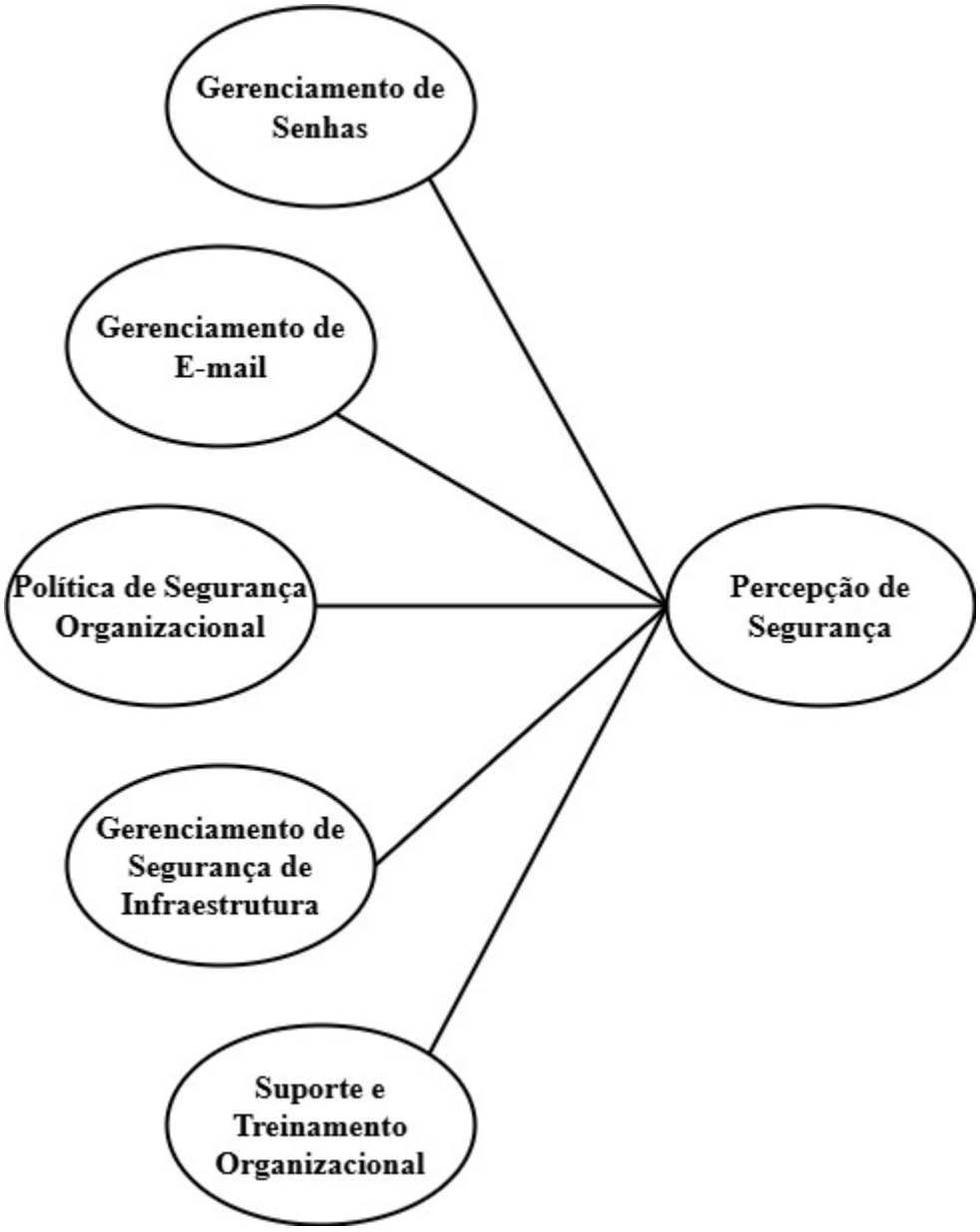


Figura 12 – Modelo teórico de SAEED
Fonte – Adaptado de SAEED, 2023.

Nesse sentido, no próximo capítulo será aprofundado a estrutura que testa a relação entre as Hipóteses e o Comportamento de Segurança da Informação utilizando o modelo de medida baseado em PLS *(Partial Least Square)*.

4. MÉTODOS

4.1. TIPO DA PESQUISA

Quanto à natureza do estudo, a pesquisa classifica-se como pesquisa aplicada, visto que tem como objetivo entender quais são os fatores que mais influenciam no Comportamento de Segurança da Informação de Trabalhadores em um contexto de Ambientes de Trabalho Digitais. Uma pesquisa aplicada, segundo Vergara (1990), é uma pesquisa que possui finalidade prática e não é motivada apenas pela curiosidade intelectual e especulação.

Quanto à forma de abordagem do problema, a pesquisa classifica-se como quantitativa, pois possui teste das hipóteses levantadas em etapas anteriores a esse trabalho. Além disso, a pesquisa quantitativa busca os fatores que influenciam um público-alvo através de uma amostra que o represente, por meio de questionário (Manzato et al. 2012).

Quanto aos objetivos gerais, a pesquisa classifica-se como explicativa, já que busca o esclarecimento de quais fatores contribuem para a Segurança da Informação dos Trabalhadores.

Quanto aos procedimentos técnicos e estratégias da pesquisa, a pesquisa é um levantamento por *Survey* porque houve a utilização de um questionário do *Google Forms* como instrumento de coleta de dados.

Inicialmente foi necessário realizar uma Revisão Sistemática da Literatura por meio do TEMAC de Mariano e Rocha (2017) com o objetivo de levantar os principais modelos e variáveis que fariam parte do trabalho. As informações relevantes obtidas nessa etapa do estudo estão presentes na parte dois desse trabalho, a Revisão da Literatura (TEMAC).

4.2. LOCAL DE PESQUISA

O local de realização da pesquisa quantitativa foi na cidade de Brasília, no Distrito Federal, Brasil. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), a estimativa da população no último censo, de 2022, foi de 2.817.381 pessoas e é a quinta concentração urbana mais populosa do Brasil (IBGE, 2022).

4.3. OBJETO DE ESTUDO

O objeto de estudo foram os profissionais de Brasília em um contexto de Ambientes de Trabalho Digitais, para entender os fatores que influenciam o Comportamento de Segurança da Informação desses trabalhadores.

4.4. INSTRUMENTO DE COLETA DE DADOS

O instrumento de coleta de dados foi realizado a partir da elaboração de um questionário com perguntas traduzidas para o português do estudo de Saeed (2023).

O questionário aplicado foi composto de 36 perguntas, sendo 33 perguntas de múltipla escolha na escala *Likert* referente aos construtos e 3 perguntas finais sobre o perfil do respondente. As perguntas da escala *Likert* possuíam cinco opções de resposta, na qual o 1 representa “discordo totalmente” e o 5 representa

"concordo totalmente". O 3, por sua vez, representa a neutralidade. As perguntas *Likert* do questionário foram baseadas nos comportamentos e práticas dos usuários em relação à seis construtos: Gerenciamento de Senhas (PM), Gerenciamento de Segurança de Infraestrutura (ISM), Gerenciamento de E-mail (EM), Política de Segurança Organizacional (OSP), Suporte e Treinamento Organizacional (OST), Percepção de Segurança (POS). Já as perguntas sobre o perfil do respondente foram referentes à identidade de gênero, faixa etária e área de atuação da organização na qual o participante trabalha.

O Quadro 7 apresenta as perguntas em escala Likert do instrumento de coleta, com as siglas referentes a cada construto e itens.

Sigla	Construto/ Item
PM	**Gerenciamento de Senhas**
PM1	Eu utilizo a mesma senha para acessar múltiplos sistemas.
PM2	Se eu altero minha senha, é principalmente por causa da política da empresa.
PM3	Quando eu altero minha senha, uso minha senha antiga como base.
PM4	Eu mantenho meus nomes de usuário/senhas em um arquivo eletrônico ou os escrevo.
PM5	Eu utilizo um software para gerenciar minhas senhas.
PM6	Eu compartilho minha senha com outros colegas.
ISM	**Gerenciamento de Segurança de Infraestrutura**
ISM1	Meu computador pessoal possui um programa de antivírus instalado.
ISM2	O programa antivírus é atualizado regularmente.
ISM3	Eu tenho um firewall instalado no meu computador.
ISM4	Eu utilizo uma ferramenta anti-spyware no meu computador.
ISM5	Eu permito scripting no meu computador.
ISM6	Eu sempre faço log off ou bloqueio o computador quando me afasto dele.
ISM7	Eu utilizo um bloqueio de tela protegido por senha.
ISM8	Eu utilizo sites de redes sociais no meu computador de trabalho.
EM	**Gerenciamento de E-mail**
EM1	Eu abro E-mails mesmo se eu não sei quem é o remetente.
EM2	Eu abro até mesmo anexos de E-mails quando eu não sei quem é o remetente.
EM3	Eu utilizo criptografia ao enviar E-mails.
EM4	Ao utilizar E-mail baseado na Web ou softwares de calendário, presto atenção às configurações de segurança do software baseado na Web.
OSP	**Política de Segurança Organizacional**
OSP1	Eu acho importante prestar atenção à segurança do computador.
OSP2	Minha organização possui uma política de segurança da informação.

Sigla	Construto/ Item
OSP3	Eu entendo a política de segurança da informação da minha organização.
OSP4	Eu desvio ou contorno a política de segurança do computador da minha organização.
OSP5	Eu acho que meus colegas desviam ou contornam a política de segurança do computador.
OSP6	Se eu ou meus colegas desviarmos ou contornarmos a política de segurança do computador e alguém descobrir, haverá repercussões.
OST	**Suporte e Treinamento Organizacional**
OST1	Se eu tiver problemas com um aplicativo de computador, é fácil para mim entrar em contato com meu administrador de rede ou sistema ou com o serviço de suporte.
OST2	Eu recebi treinamento em segurança da informação.
OST3	O treinamento em segurança da informação me ajudou a entender melhor a política de segurança da organização.
POS	**Percepção de Segurança**
POS1	Eu acredito que meu computador pessoal é seguro.
POS2	Eu acredito que posso proteger meu computador de hackers/phishers, se cuidar bem da segurança do computador.
POS3	A segurança do computador me preocupa.
POS4	Eu acho que faz diferença se eu prestar atenção especial à segurança do computador, como por exemplo, instalar um navegador menos vulnerável.
POS5	Eu acho que as informações que mantenho no meu computador não são interessantes o suficiente para as pessoas tentarem invadir meu computador.
POS6	Eu acho que não importa o que eu faça, se as pessoas tiverem más intenções, elas conseguirão invadir meu computador e nossa rede.

Quadro 7 – Instrumento de Coleta (Questionário)
Fonte – Autoria Própria (2024)

4.5. AMOSTRA

O cálculo da quantidade mínima da amostra foi realizado por meio do software G*Power. A amostra da pesquisa foi calculada via G-power a partir do tamanho de efeito. Foi considerado um efeito médio (0,15), com potência preditiva de 0,80 e alfa de 0,05, com 6 variáveis independentes. Obteve-se o número mínimo de 112 respostas necessárias para validação do modelo. A amostra final coletada foi de 119 respostas.

4.6. PROCEDIMENTO DE COLETA DE DADOS

A divulgação do questionário da pesquisa foi feita por meio da divulgação via *Instagram* e *WhatsApp*. A coleta das respostas foi realizada por meio de um formulário do *Google Forms*, disponibilizado entre os dias 08/07/2024 e 31/07/2024.

4.7. TRATAMENTO DE DADOS

Ao final do período de coleta, os dados obtidos foram convertidos em uma planilha no *Microsoft Excel*, com os construtos transformados em suas iniciais. O input foi feito no programa *SmartPLS* a partir do arquivo com as respostas em formato .csv. Esse programa analisa as informações via equações estruturais (PLS-SEM), avaliando o grau de correlação e regressão entre as variáveis.

A metodologia do PLS é dividida em três parte: 1) Validação e confiabilidade do modelo de medida, 2) Validação do modelo estrutural e 3) Implicações práticas (Ramírez et al. 2014).

Na primeira parte, de Validação e confiabilidade do modelo de medida, são avaliados: confiabilidade de item, confiabilidade interna, validade composta, validade discriminante, VIF e significância do peso. Na Segunda parte, de Validação do modelo estrutural, é realizado o cálculo do beta, do coeficiente de determinação (R-quadrado) e o *boothstrapping*. Na terceira parte são analisadas as implicações práticas referentes aos resultados da amostra.

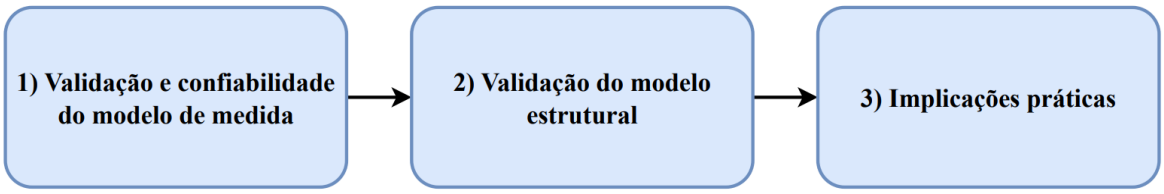


Figura 13 – Metodologia PLS
Fonte – Adaptado de Ramírez, 2014.

Um objetivo comum nas análises PLS-SEM é identificar os principais fatores que influenciam intenções comportamentais (Hair et al. 2021) e por esse motivo foi escolhido para este trabalho. Por meio da análise PLS-SEM, serão identificados os principais fatores que influenciam o comportamento de segurança da informação de trabalhadores em ambientes de trabalho digitais.

5. RESULTADOS

Após a aplicação dos questionários, os dados coletados foram consolidados e organizados, um modelo estrutural por meio da utilização do software SmartPLS. Inicialmente, será apresentada a descrição da amostra, seguida pela apresentação do modelo de acordo com a metodologia de Ramírez, Mariano e Salazar (2014). O modelo será descrito, validado e valorado por meio de testes estatísticos adequados, a análise dos resultados obtidos. Por fim, após a análise dos resultados, serão elaboradas e apresentadas as aplicações práticas do trabalho.

5.1. DESCRIÇÃO DA AMOSTRA

A amostra deste trabalho foi composta por brasileiros moradores do Distrito Federal (DF), que trabalham em Ambientes de Trabalho Digitais, ou seja, realizam em parte ou em totalidade suas atividades profissionais em dispositivos eletrônicos, como computadores. A atividade profissional pode ser realizada tanto presencialmente ou em regime de trabalho remoto.

O primeiro dado demográfico coletado na amostra é referente à identidade de gênero, sendo as opções feminino, masculino e outro. A distribuição por gênero da amostra pode ser observada na Figura 14, com leve predominância do público masculino (52,1%). É interessante observar que ambos os gêneros estão inseridos em um contexto de trabalho digital onde estão sujeitos à riscos cibernéticos em suas organizações.

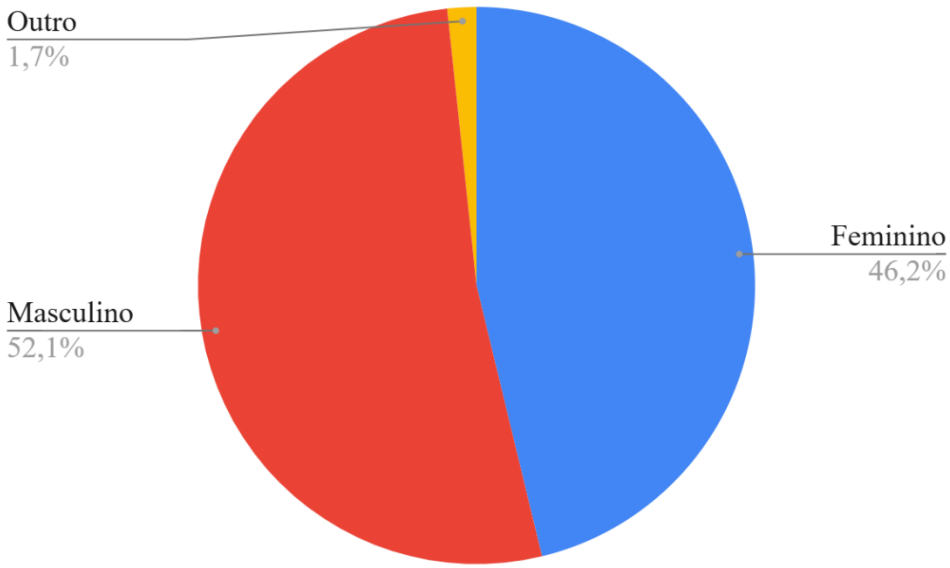


Figura 14 – Distribuição por gêneros da amostra
Fonte – Autoria própria (2025).

O segundo dado demográfico refere-se à faixa etária da amostra, como pode ser visualizada na Figura 15. A maioria dos respondentes se enquadra na faixa etária de 19 a 25 anos, representados por 81 dos 119 participantes.

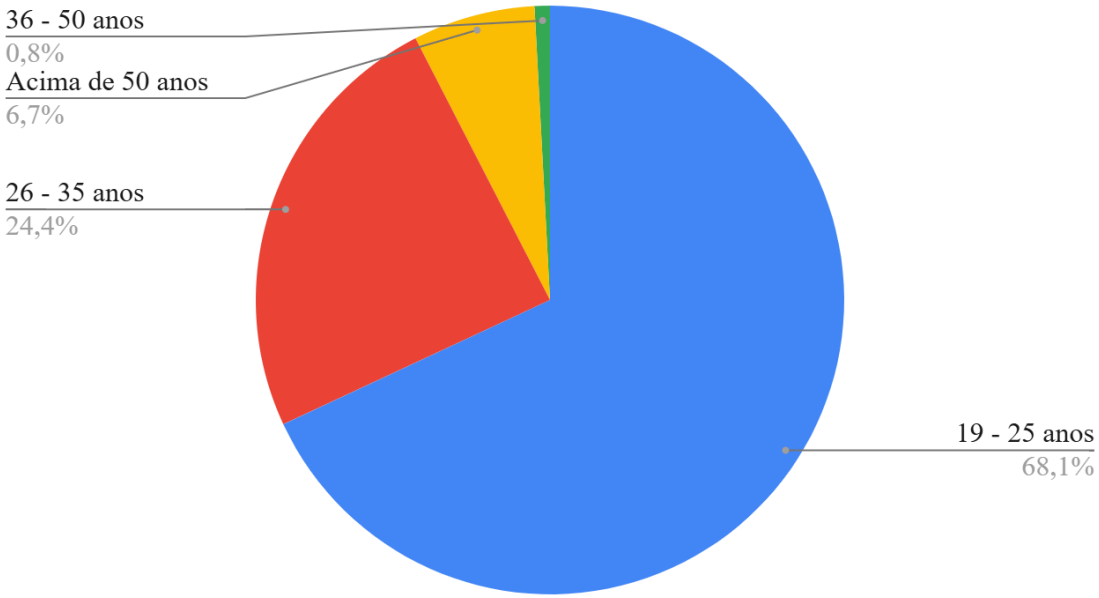


Figura 15 – Distribuição por faixa etária da amostra
Fonte – Autoria própria (2025).

O terceiro e último dado demográfico coletado é referente área de atuação da organização onde os respondentes trabalham, sendo quase metade (59 respondentes ou 49,6%) da amostra pertencente ao setor de Serviços.

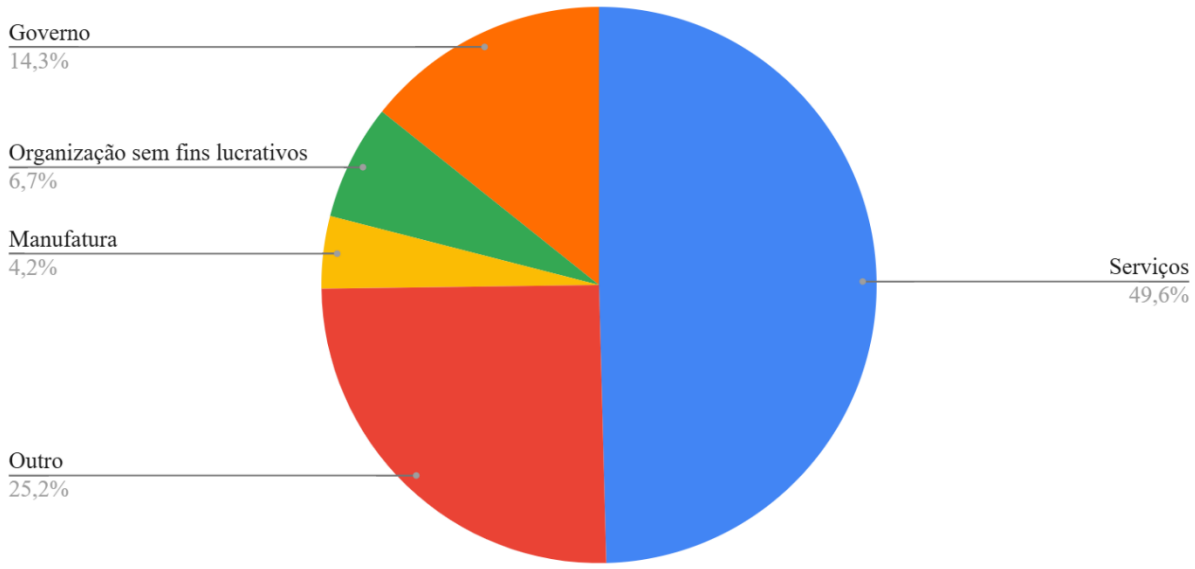


Figura 16 – Distribuição por área de atuação da amostra
Fonte – Autoria própria (2025).

As análises realizadas durante esta etapa do projeto possuem como objetivo compreender melhor a amostra e são essenciais para a anáise dos resultados das hipóteses.

5.2. CÁLCULO DO MODELO

A avaliação do modelo é dividida em três etapas: 01) Valoração do modelo de medida, 02) Valoração do modelo estrutural e 03) Implicações práticas, como pode ser observado na Figura 17, extraída de Mariano (2023).



Figura 17 – Etapas de avaliação dos modelos
Fonte – Mariano et al. (2023).

As etapas de Valoração do modelo de medida e Valoração do modelo estrutural serão descritas nesse capítulo, e a próxima etapa, de Implicações práticas, será descrita no próximo capítulo.

5.2.1. Valoração do Modelo de Medida – Reflexivo

A Valoração do Modelo de Medida será separada entre quatro partes, sendo elas: 01) Confiabilidade de Item, 02) Confiabilidade Interna, 03) Validade convergente, 04) validade discriminante. Além disso, um teste de Multicolinearidade será realizado adicionalmente. Após essas etapas, será possível realizar a validação do modelo que corresponde à pesquisa.

5.2.1.1. Descrição do Modelo

O modelo escolhido foi traduzido e adaptado do trabalho de Saeed (2023), como exposto nos capítulos anteriores. O modelo proposto é composto por 6 variáveis e 33 indicadores. As variáveis independentes (Gerenciamento de Senhas, Gerenciamento de Segurança e Infraestrutura, Gerenciamento de E-mail, Política de Segurança Organizacional e Suporte e Treinamento Organizacional) exercem influência sobre o comportamento da única variável dependente do modelo (Percepção de Segurança). Todas as variáveis do modelo são latentes, visto que não podem ser medidas diretamente como explicado no livro Hair et al. (2017), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM).*

Cada uma das variáveis latentes, sendo ela dependentes ou independentes, são representadas geometricamente, pelo formato de círculo. As perguntas do questionário são os indicadores (variáveis diretamente mensuradas), representados geometricamente pela forma retangular.

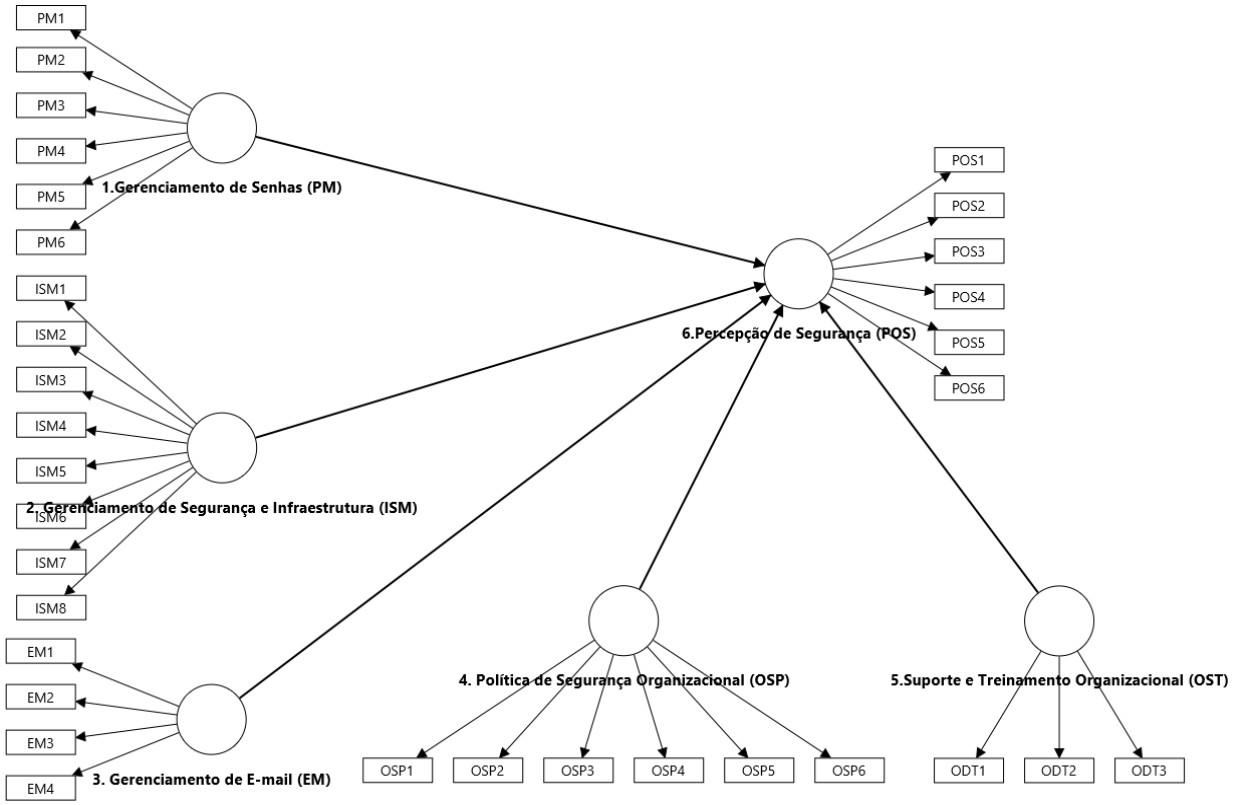


Figura 18 – Modelo estrutural
Fonte – Autoria própria, extraída do Software *SmartPLS* (2025).

Por se tratar de um modelo inicialmente construído para os trabalhadores da Arábia Saudita (SAEED, 2023), traduzido e adaptado para residentes do Distrito Federal neste trabalho, torna-se necessário realizar a validação do modelo para a realidade brasileira, para que o modelo possa ser considerado confiável (Ramírez et al. 2014).

5.2.1.2. Confiabilidade de Item

O primeiro teste para validar a confiabilidade do modelo é a confiabilidade de item, na qual é calculada a força de correlação entre variáveis e indicadores. Os valores aceitos devem ser maiores ou iguais a 0,707, de acordo com a proposta metodológica exposta no trabalho de Ramírez, Mariano e Salazar (2014). Também é possível o aceite de valores acima de 0,4, desde que não comprometa etapas posteriores (Hair, et al. 2019). Indicadores com valores abaixo de 0,4, em contrapartida, devem ser sempre eliminados do modelo de medição (Hair, Hult, Ringle, e Sarstedt, 2021).

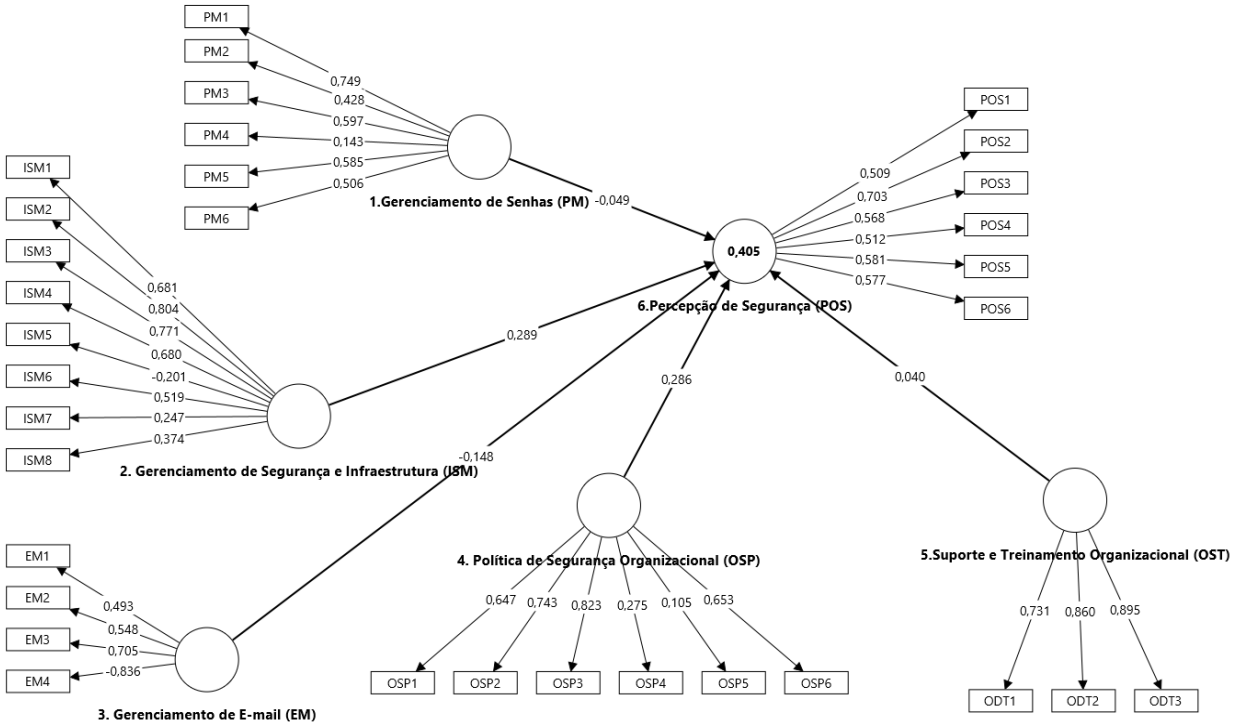


Figura 19 – Modelo Inicial de Confiabilidade de Item
Fonte – Autoria própria, extraída do Software *SmartPLS* (2025).

A Partir da Figura 19, é possível perceber que alguns dos indicadores performaram abaixo de 0,4 e devem, portanto, ser eliminados (Hair, Hult, Ringle, e Sarstedt, 2021). Desta forma, os indicadores foram sendo eliminados e as perguntas que estavam relacionadas a eles são:

- PM2 - Se eu altero minha senha, é principalmente por causa da política da empresa.
- PM4 - Eu mantenho meus nomes de usuário/senhas em um arquivo eletrônico ou os escrevo.
- PM6 - Eu compartilho minha senha com outros colegas.
- ISM5 - Eu permito *scripting* no meu computador.
- ISM7 - Eu utilizo um bloqueio de tela protegido por senha.
- ISM8 - Eu utilizo sites de redes sociais no meu computador de trabalho.
- EM1 - Eu abro E-mails mesmo se eu não sei quem é o remetente.
- EM4 - Ao utilizar E-mail baseado na Web ou softwares de calendário, presto atenção às configurações de segurança do software baseado na Web.
- OSP4 - Eu desvio ou contorno a política de segurança do computador da minha organização.
- OSP5 - Eu acho que meus colegas desviam ou contornam a política de segurança do computador.

Além do critério estatístico, é importante também levar em consideração o perfil dos respondentes da amostra ao interpretar os motivos de descarte desses indicadores e as perguntas relacionadas a eles. Alguns itens, como ISM5 (uso de scripting) e EM4 (atenção às configurações de segurança do e-mail), envolvem termos técnicos que podem ter gerado falta de identificação ou compreensão entre os participantes. O ISM7

(bloqueio de tela com senha), por sua vez, se refere a uma prática automatizada por muitas empresas, já que muitas vezes o bloqueio ocorre automaticamente após alguns minutos de inatividade, o que pode levar os usuários a não perceberem essa ação como uma prática consciente de segurança. Já os indicadores PM4 e PM6, relacionados ao armazenamento e compartilhamento de senhas, assim como OSP4 e OSP5, que tratam de práticas inadequadas como burlar regras de segurança, e ISM8 (uso de redes sociais no computador do trabalho), envolvem comportamentos sensíveis, que possivelmente geraram receio por parte dos respondentes em admitir práticas consideradas incorretas ou inseguras. Esses resultados mostram que, além dos critérios técnicos, é importante considerar se os itens fazem sentido para a realidade dos participantes e são compreendidos pelos respondentes do questionário, reforçando a necessidade de alinhar os indicadores ao contexto da amostra.

Após a primeira identificação dos indicadores que estão fora do modelo, a análise foi refeita com a retirada dos indicadores abaixo da meta 0,4, com o intuito de que as correlações do modelo sejam consideradas satisfatórias. Dessa maneira, o novo modelo assinala que os indicadores estão atrelados às variáveis corretas dentro do modelo. O novo modelo estável de confiabilidade de item da amostra pode ser observado na Figura 20.

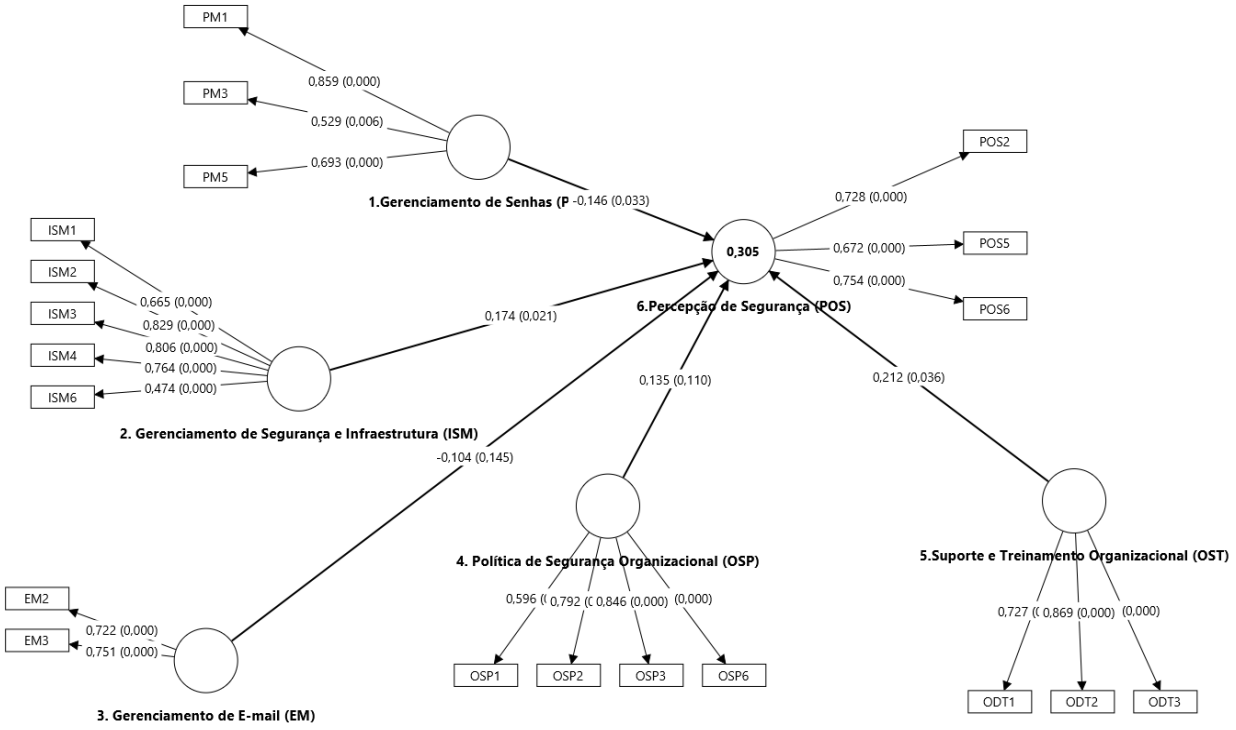


Figura 20 – Modelo Final de Confiabilidade de Item
Fonte – Autoria própria, extraída do Software *SmartPLS* (2025).

Dessa forma, a confiabilidade de item alcançou o exposto em Hair (2019), e a próxima etapa a ser analisada é a Confiabilidade interna.

5.2.1.3. Confiabilidade Interna *(rho_c)*

O segundo teste realizado para medir a confiabilidade do modelo é a confiabilidade interna, que explica e comprova se os indicadores são suficientes para explicar sua respectiva variável latente. Nessa parte, foi realizada a análise da confiabilidade do constructo por meio da confiabilidade composta *(rho_c).* Segundo Ramírez *et al.* (2014), são aceitos índices de *rho_c* acima de 0,7.

Na tabela 1, pode-se observar que todas as variáveis atingiram o valor meta 0,7, exposto por Hair *et al.* (2017). Por isso, o modelo foi considerado confiável, já que atendeu aos requisitos de confiabilidade.

Além dos testes de confiabilidade, foram realizados dois testes de validação: 01) Variância Média Extraída (AVE) e 02) Validade Discriminante, com o objetivo de garantir a validade do modelo.

5.2.1.4. Variância Média Extraída (AVE)

Foi realizado o teste de Variância Média Extraída (*Average Variance Extracted* – AVE), para o qual todas as variáveis devem apresentar valor maior ou igual a 0,5, para o modelo ser considerado válido (Fornell e Larcker, 1981).

Variável	rho_c	AVE
1.Gerenciamento de Senhas (PM)	0,743	0,500
2. Gerenciamento de Segurança e Infraestrutura (ISM)	0,838	0,517
3. Gerenciamento de E-mail (EM)	0,703	0,542
4. Política de Segurança Organizacional (OSP)	0,824	0,544
5.Suporte e Treinamento Organizacional (OST)	0,870	0,693
6.Percepção de Segurança (POS)	0,762	0,517

Tabela 1 – Indicadores da Confiabilidade Interna e Variância Média Extraída
Fonte – Autoria própria, extraída do Software *SmartPLS* (2025).

Na tabela 1, observa-se que todos os valores para AVE são maiores que 0,5, sendo Gerenciamento de E-mail (EM) com o menor valor e Suporte e Treinamento Organizacional (OST) com o maior valor. Dessa maneira, o modelo foi validado em relação à Variância Média Extraída.

5.2.1.5. Validade Discriminante – Fornell Larcker

Além da Variância Média extraída, realizou-se a medição da validade discriminante segundo o critério de Fornell-Larcker (1981), cujo intuito é validar se cada construto explica seus próprios indicadores. Para esse critério, a raiz quadrada da Variância Média Extraída (AVE) deve ser maior do que suas respectivas correlações com os outros construtos, o que significa que o construto está mais fortemente relacionado com seus próprios itens do que com os de outros.

Variável	1	2	3	4	5	6
1.Gerenciamento de Senhas (PM)	**0,707**					
2. Gerenciamento de Segurança e Infraestrutura (ISM)	-0,285	**0,719**				
3. Gerenciamento de E-mail (EM)	0,258	-0,462	**0,736**			
4. Política de Segurança Organizacional (OSP)	-0,259	0,508	-0,488	**0,737**		
5.Suporte e Treinamento Organizacional (OST)	-0,198	0,347	-0,394	0,647	**0,832**	
6.Percepção de Segurança (POS)	-0,300	0,406	-0,371	0,449	0,430	**0,719**

VIF≤3,3

Tabela 2 – Resultados Fornell-Larcker

Fonte: Autoria própria, extraída do Software *SmartPLS* (2025).

Na tabela 2, pode-se observar que a condição é confirmada para todos os construtos analisados, indicando que cada um mede um conceito distinto no modelo e seus valores estão representados pela diagonal da tabela. Dessa forma, pode-se concluir que o modelo é confiável e válido.

5.2.2. Valoração do Modelo Estrutural

Após a valoração do modelo de medida, com a realização dos cálculos de Confiabilidade de Item, Confiabilidade Interna *(rho_c),* Variância Média Extraída e Validade Discriminante (Fornell-Larcker), iniciou-se a fase de Valoração do Modelo Estrutural. Essa fase possui como objetivo identificar os fatores determinantes na percepção de segurança dos trabalhadores.

Esta fase divide-se em três etapas. Na primeira etapa, é realizado o teste de Multicolinearidade, na segunda etapa, é calculado o coeficiente de Determinação (R^2) e na terceira e última etapa é determinada a importância das variáveis do Coeficiente Beta (β).

5.2.2.1. Multicolinearidade

A primeira etapa da fase de Valoração do Modelo Estrutural, a análise de multicolinearidade, é realizada pelo cálculo do Fator de Inflação de Variância (VIF). Elevados níveis de colinearidade reduzem a precisão de estimativa dos pesos e podem elevar o erro padrão, fatores que comprometem os resultados da análise.

O VIF deve ser menor ou igual a 3,3 para garantir a confiabilidade do modelo. Caso o VIF ultrapasse o valor de 3,3, será necessário a remoção de indicadores (Hair *et al.* 2023). Valores de VIF superiores a 10, por sua vez, significam um problema significativo de multicolinearidade (Ramírez *et al.* 2014). Para o modelo em questão, após a realização do teste de VIF, todas as variáveis retornaram valores de VIF menores ou iguais a 3,3 e, portanto, o modelo não apresenta multicolinearidade, como pode ser observado na Tabela 2.

5.2.2.2. Coeficiente de Determinação (R^2)

O Coeficiente de Determinação possui como objetivo avaliar o grau de influência que cada variável independente exerce sobre a variável dependente, ou seja, o nível de predição do modelo. Segundo Hair *et al.*

(2019), valores de acima 13% já podem ser considerados satisfatórios como nível de predição do modelo.

No Modelo Estrutural representado na Figura 20, é possível observar a relação entre as variáveis e o valor do Coeficiente de Determinação (R^2) para a única variável dependente do modelo: Percepção de Segurança (POS). A variável Percepção de Segurança (POS) é explicada em 30,5% pelas demais variáveis do modelo: Gerenciamento de Senhas (PM), Gerenciamento de Segurança e Infraestrutura (ISM), Gerenciamento de E-mail (EM), Política de Segurança Organizacional (OSP) e Suporte e Treinamento Organizacional (OST). Isso significa que o as variáveis explicam suficientemente a Percepção de Segurança (POS), pois o R^2 calculado apresentou valor acima de 30,05% (Hair *et al*. 2019).

5.2.2.3. Coeficiente Beta (β)

Após a análise do Coeficiente de Determinação (R^2) e sua validade, inicia-se a análise do Coeficiente Beta (β), cujo intuito é avaliar o grau de influência de cada relação entre as variáveis e validar as hipóteses formuladas anteriormente. Os valores de β foram calculados no *Software SmartPLS* e representam os valores das setas que conectam os construtos, os caminhos. Os valores calculados para o Coeficiente Beta (β) do Modelo Estrutural podem ser visualizados na tabela 3.

Segundo Chin (1998), valores recomendados para β são $\beta \geq 0,3$ ou $\beta < -0,3$, sendo valores $\beta \geq 0,2$ ou $\beta \leq -0,2$ também considerados significativos para a análise. Após a análise do Coeficiente Beta (β), foi realizado o procedimento de *bootstrapping* para garantir a estabilidade das estimativas das amostras. O método *bootstrapping* mapeia, de forma randômica, 10.000 subamostras dos dados originais e permite calcular o *t-student* e *p-value*. Os valores utilizados como referência para garantir a confiabilidade do modelo são: *t-student* ≥ 1,64 e *p-value* ≤ 0,05 e os resultados do *bootstrapping* para o modelo em questão podem ser observados na tabela 3.

	Hipóteses	Beta	%	T-valor	Intervalo de confiança		Suportada?
					5.0%	95.0%	
H1	1.Gerenciamento de Senhas (PM) ➜ 6.Percepção de Segurança (POS)	-0,146*	4,38%	1,834	-0,290	-0,032	Sim
H2	2. Gerenciamento de Segurança e Infraestrutura (ISM) ➜ 6. Percepção de Segurança (POS)	0,174*	7,06%	2,038	0,041	0,323	Sim
H3	3. Gerenciamento de E-mail (EM) ➜ 6.Percepção de Segurança (POS)	-0,104 ns	3,86%	1,057	-0,271	0,052	Não
H4	4. Política de Segurança Organizacional (OSP) ➜ 6.Percepção de Segurança (POS)	0,135 ns	6,06%	1,225	-0,032	0,330	Não
H5	5.Suporte e Treinamento Organizacional (OST) ➜ 6.Percepção de Segurança (POS)	0,212*	9,12%	1,798	0,005	0,393	Sim

ns ; *p<0,05; ** p<0,01; ***p<0,001

Tabela 3 – Testes de Hipóteses
Fonte: Autoria própria, extraída do Software *SmartPLS* (2025).

As hipóteses suportadas do modelo foram H1, H2 e H5, visto que apresentaram valores de Coeficiente Beta (β) considerados significativos*, t-value* maiores que 1,64 e *p-value* menores que 0,05. As variáveis que exercem influência significativa positiva são Gerenciamento de Segurança e Infraestrutura (ISM) e Suporte e Treinamento Organizacional (OST), sendo Suporte e Treinamento Organizacional (OST) a de maior influência positiva. Gerenciamento de Senhas (PM), por sua vez, apresenta uma influência significativa negativa.

Os resultados da análise indicam que a Percepção de Segurança (POS) é fortemente influenciada pelo Suporte e Treinamento Organizacional (OST), o que significa que os colaboradores em um ambiente digital necessitam de apoio de sua organização para a proteção no ambiente digital. Esse resultado é consistente com a ideia de que, aumentando-se a conscientização dos trabalhadores de uma empresa, por meio de suporte e treinamento, aumenta-se a segurança da empresa como um todo.

Com a validação das hipóteses do estudo, é necessário aprofundar a análise e os resultados obtidos.

6. ANÁLISE E DISCUSSÃO DAS HIPÓTESES

6.1. DISCUSSÃO DAS HIPÓTESES

Após a realização das etapas de validação e valoração do modelo estrutural, torna-se necessário a análise e discussão das hipóteses, bem como suas implicações práticas. Além disso, será realizada a comparação entre os resultados do modelo deste estudo, com trabalhadores do Distrito Federal, em relação ao modelo proposto por SAEED (2023), com trabalhadores da Arábia Saudita e suas principais similaridades e diferenças.

- **H1: Um gerenciamento de senhas efetivo leva a uma positiva percepção da segurança.**

O resultado encontrado na primeira hipótese é da relação entre o gerenciamento de senhas efetivo e o comportamento positivo de segurança da informação. A porcentagem do quanto o gerenciamento efetivo de senhas explica o comportamento de segurança da informação é 4,38%, com valores de *t-student* e *p-value* satisfatórios. Essa hipótese foi suportada tanto no trabalho em questão quanto no estudo de SAEED (2023).

No formulário aplicado na amostra, foram realizadas perguntas referentes à utilização da mesma senha para múltiplos sistemas, alteração da senha utilizando a senha antiga como base e utilização de um software para gerenciamento de senhas. Segundo o estudo de Tam *et al.* (2010), os usuários possuem o conhecimento do que é uma senha forte ou fraca e boas práticas em relação a senhas, entretanto, podem priorizar a conveniência ao invés da segurança, por não perceberem as consequências desses comportamentos. Conclui-se que a utilização de senhas fortes, diferentes e alteradas com eficiência, além de tecnologias de apoio no armazenamento de senhas (como softwares de gerenciamento de senhas, por exemplo) tornam-se essenciais para um comportamento positivo de segurança da informação, com a facilitação e conveniência no armazenamento de senhas, por meio de softwares de gerenciamento *user-friendly*.

- **H2: Um gerenciamento de recursos de infraestrutura de segurança efetivo leva a uma positiva percepção da segurança.**

No presente estudo, a variável Gerenciamento de Segurança e Infraestrutura (ISM) explicou em 7,06% o comportamento de segurança da informação. Além disso, foi suportada com com valores de *t-student* e *p-value* considerados satisfatórios. A diferença entre os estudos foi que para a pesquisa aplicada por SAEED (2023), essa hipótese foi rejeitada, enquanto no estudo atual ela resultou na segunda hipótese que mais explica o comportamento de segurança da informação.

As perguntas referentes ao Gerenciamento de Infraestrutura de Segurança foram sobre a utilização e atualização de programas de antivírus no computador, utilização de firewall e ferramenta *anti-spyware*, além da realização do bloqueio do computador quando longe do mesmo. O suporte à H2 no presente estudo mostra a importância do suporte de tecnologias de infraestrutura no comportamento de segurança da informação. Entretanto, o trabalho de Dutta e Mccrohan (2002) sugere que o Gerenciamento de Infraestrutura de Segurança e suas tecnologias é necessário, porém torna-se insuficiente sem medidas organizacionais e sociais.

- **H3: Um gerenciamento de atividades de E-mail apropriado leva a uma positiva percepção da segurança.**

A H3, referente ao gerenciamento de atividades de E-mail, não foi suportada no estudo em questão, por apresentar valores de *t-value* e *p-value* insatisfatórios. Entretanto, no estudo de Saeed (2023), essa relação foi positiva, sendo considerado um fator relevante na explicação do comportamento positivo de segurança da informação, mas com apenas dois dos quatro subfatores sendo relevantes.

No contexto desse estudo, os resultados indicam que um gerenciamento de atividades de E-mail apropriado não desempenha um papel relevante no comportamento positivo de segurança da informação, com outros fatores sendo considerados mais relevantes. As perguntas aplicadas na amostra, referentes a esse estudo, foram sobre a abertura de anexos de E-mails de remetentes desconhecidos e a utilização de criptografia no envio de E-mail. O resultado pode ser explicado pelo fator de que maioria dos serviços de E-mail atuais já utilizam algum tipo de criptografia, como a criptografia em trânsito (TLS), por exemplo, para proteger as mensagens enquanto são transferidas entre os servidores do remetente e do destinatário. Apesar de não suportada pelo trabalho em questão, é importante salientar boas práticas em relação ao gerenciamento de atividades de E-mail, como por exemplo, ferramentas de autenticação de 2FA *(Two-Factor-Authentication)* ou MFA *(Multi-Factor-Authentication)*, como exposto por Sumecki (*et al.* 2011)

- **H4: Políticas de segurança organizacionais levam a uma positiva percepção da segurança.**

A quarta hipótese formulada no estudo, foi rejeitada tanto pelo trabalho de SAEED (2023), quanto pelo estudo em questão, aplicado com trabalhadores residentes do Distrito Federal, visto que não atingiu valores de *t-student* e *p-value* considerados satisfatórios.

As perguntas aplicadas na amostra referentes à essa hipótese foram sobre a importância de prestar atenção à segurança do computador, a presença de uma política de segurança da informação na organização, bem como o entendimento dessa política e ao desvio ou contorno da política de segurança da informação e suas repercussões, caso o desvio seja descoberto. Esses resultados podem ser explicados pelo fato de que somente a existência e entendimento da política da empresa não é suficiente para um comportamento de segurança da informação se ela não for acompanhada de medidas para implementação da política na prática. Além disso, atualmente existem muitos trabalhadores que utilizam os próprios dispositivos para o trabalho, BYOD (Bring your own device), nos quais as políticas e implementações de segurança não podem invadir a privacidade do computador de uso pessoal (HOVAV *et al.* 2016). Dessa forma, políticas de segurança organizacionais não desempenham um papel tão relevante no comportamento de segurança da informação, conforme os resultados deste trabalho e do trabalho de SAEED (2023).

- **H5: Suporte e treinamentos organizacionais levam a uma positiva percepção da segurança.**

No presente estudo, a variável Suporte e Treinamento Organizacional (OST) apresentou a maior relevância na explicação da percepção de segurança da informação, com a explicação de 9,12% da percepção

de segurança da informação. Entretanto, no estudo de SAEED (2023), essa hipótese foi rejeitada por não possuir valores satisfatórios na etapa de valoração.

No estudo em questão, para os trabalhadores do Distrito Federal, todas as perguntas iniciais referentes ao Suporte e Treinamento Organizacional foram mantidas. Para essa hipótese, foram realizadas perguntas sobre a facilidade para entrar em contato com o administrador de rede ou sistema ou com o serviço de suporte em caso de problemas com um aplicativo, o recebimento de treinamento em segurança da informação, e a ajuda do treinamento em segurança da informação no entendimento da política de segurança da organização. Os resultados do estudo refletem a importância de apoio organizacional na conscientização e implementação de segurança da informação, visto que muitos dos trabalhadores da amostra, inseridos no contexto de ambientes de trabalhos digitais, possuem diferentes áreas de atuação e necessitam de suporte da equipe de TI e da organização onde estão inseridos para colocar em prática comportamentos positivos de segurança da informação. Programas de treinamento de qualidade, respeitosos e bem-comunicados são mais bem recebidos pelos colaboradores (LOWRY *et al.* 2015).

6.2. IMPLICAÇÕES PRÁTICAS

A partir dos dados aplicados e dos estudos desenvolvidos durante todo o projeto, foi possível compreender melhor os fatores humanos na percepção e comportamento em cibersegurança.

Com o objetivo de complementar a análise PLS-SEM, foi elaborado o gráfico de importância-desempenho (IPMA), que auxilia em obter mais insights e estabelecer prioridades para a busca de melhorias, segundo Ringle e Sarstedt (2016). No gráfico IPMA, figura 21, observa-se a importância de cada fator no eixo X e seu desempenho no eixo Y. Dessa maneira, primeiramente devem ser tratados os pontos de alta importância e baixo desempenho, representados pelo quadrante inferior direito (quadrante 1), seguindo, após isso, a ordem numérica indicada na imagem figura 21.

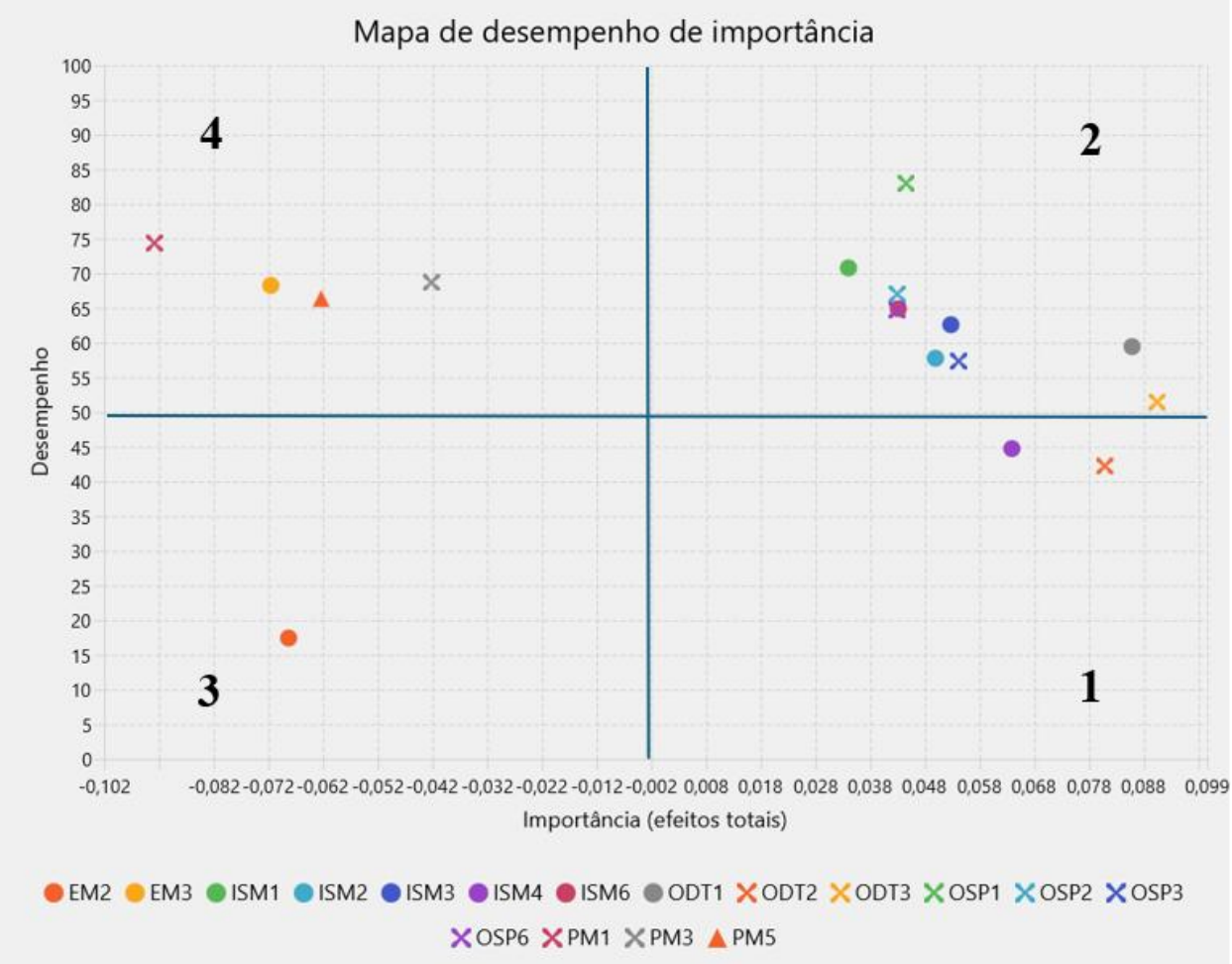


Figura 21 – Gráfico Importância VS Desempenho
Fonte – Autoria própria, extraída do Software *SmartPLS* (2025).

No primeiro quadrante, de alta importância e baixo desempenho, estão posicionados os indicadores OST2 e ISM4, que devem ser o foco inicial da pesquisa. Esses são os indicadores que mais contribuem para explicar a Percepção de Segurança, mas estão com desempenho baixo, e por isso devem ser priorizados para os planos de ação. O OST2 está relacionado à pergunta do construto OST (Suporte e Treinamento Organizacional) e o ISM4 deste quadrante está relacionado à pergunta do construto ISM (Gerenciamento de Segurança de Infraestrutura), respectivamente:

- OST2: Eu recebi treinamento em segurança da informação.
- ISM4: Eu utilizo uma ferramenta anti-spyware no meu computador.

Suporte e Treinamento Organizacional explicou em 9,12% a Percepção de Segurança na etapa de teste de hipóteses e foi o fator que mais explicou a variável dependente. Segundo WEN (2019), simulações práticas de ataques cibernéticos, em um ambiente seguro e controlado, são efetivas para um comportamento positivo em segurança cibernética, o que demonstra a importância desse indicador e a necessidade de aumento em seu desempenho para uma maior proteção em ambientes de trabalho digitais.

Para o indicador ISM4, ao analisar o gráfico como um todo, percebe-se que os usuários possuem

antivírus atualizado regularmente no computador (alto desempenho e alta importância), entretanto, não utilizam ferramentas anti-spyware no computador, o que demonstra que muitos usuários tendem a superestimar a proteção oferecida pelo antivírus e subestimar a necessidade de ferramentas específicas contra spyware. Segundo a investigação empírica da adoção de softwares anti-spyware no estudo de Lee e Kozar (2008), o spyware é responsável por cerca de 12% de todas as chamadas para suporte técnico, sendo que mais de 80% dos problemas atuais causados por spyware poderiam ser resolvidos com o uso de softwares anti-spyware, o que demonstra sua importância, em linha com o que foi identificado na análise IPMA. Portanto, torna-se necessário adotar medidas para uma proteção mais abrangente, além do antivírus tradicional, já utilizado por grande parte dos usuários respondentes.

O segundo quadrante, por sua vez, localizado no canto superior direito, representa os indicadores com alta importância e alto desempenho, que devem ser mantidos e reforçados para garantir a continuidade de alta performance.

- OST3: O treinamento em segurança da informação me ajudou a entender melhor a política de segurança da organização.
- OST1: Se eu tiver problemas com um aplicativo de computador, é fácil para mim entrar em contato com meu administrador de rede ou sistema ou com o serviço de suporte.
- OSP3: Eu entendo a política de segurança da informação da minha organização.
- ISM2: O programa antivírus é atualizado regularmente.

Os indicadores OST3 e OSP3 revelam que a percepção em relação ao suporte e à efetividade do treinamento auxilia na adesão às práticas de segurança, promove comportamentos positivos em ambientes de trabalho digitais e facilita a compreensão da política de segurança (Puhakainen e Siponen, 2010). Entretanto, houve um baixo desempenho no indicador OST2 (“Eu recebi treinamento em segurança da informação”), o que mostra que, quando os usuários recebem treinamento, ele realmente contribui para o entendimento da política, mas que essa capacitação não ocorre de forma consistente para todos. Além disso, percebe-se que a facilidade para entrar em contato com o serviço de suporte, fator de alta importância para a percepção de segurança, apresentou desempenho elevado entre os respondentes da pesquisa, o que reforça comportamentos positivos de segurança no dia a dia. Por fim, embora os respondentes tenham apresentado baixo desempenho no indicador ISM4, relacionado ao uso de anti-spyware, o indicador ISM2 mostra que os usuários mantêm a atualização regular do programa de antivírus, prática consolidada e essencial para a proteção dos dispositivos.

O terceiro e quarto quadrante representam indicadores que possuem menor relevância para a pesquisa e não serão priorizados na análise deste trabalho.

	Fatores Positivos	Fatores Negativos
	Forças	**Fraquezas**
Fatores Internos	Entendimento da política de segurança por meio de treinamento (OST3)	Falta de uso de anty-spyware (ISM4)
	Facilidade no contato com o administrador de rede ou sistema ou com o serviço de suporte (OST1)	Oferta inconsistente de treinamentos de segurança (OST2)
	Entendimento da política de Segurança da Informação (OSP3)	
	Atualização regular do programa de antivírus (ISM2)	
	Oportunidades	**Ameaças**
Fatores Externos	Crescimento da oferta de plataformas de treinamento em segurança da informação no mercado (simulações práticas de phishing e recursos gamificados, por exemplo).	Crescimento de ameaças digitais sofisticadas e ataques do tipo zero-day
	Pressões regulatórias e de compliance impulsionando a necessidade de onboarding estruturado com foco em segurança.	Controles de segurança rígidos impactam na usabilidade dos sistemas
	Tendência de mercado e de frameworks de segurança que reforçam a importância da melhoria contínua para continuar à frente de cibercriminosos	
	Demanda de stakeholders por maior transparência em saber como está a segurança da informação nas organizações.	

Quadro 8 – Matriz SWOT
Fonte: Autoria própria (2025).

Com base na análise SWOT apresentada, que resume as principais forças e fraquezas (fatores internos) e oportunidades e ameaças (fatores externos) relacionadas aos fatores humanos que influenciam a percepção de cibersegurança, propõem-se a seguir um conjunto de ferramentas da Engenharia de Produção. Essas ferramentas visam potencializar os pontos fortes, explorar as oportunidades identificadas e mitigar as fraquezas e ameaças mapeadas, contribuindo para o desenvolvimento de um ambiente organizacional mais seguro.

A partir dos resultados obtidos no presente trabalho, é possível aplicar ferramentas da Engenharia de Produção de forma prática para aprimorar a percepção de cibersegurança na organização. As ferramentas apresentadas a seguir buscam 01) potencializar os pontos fortes mapeados e manter a alta performance do segundo do gráfico de IPMA, de alta importância e desempenho, 02) mitigar as fraquezas identificadas no primeiro quadrante de alta importância e baixa performance do gráfico IPMA (como o baixo uso de antispyware e a oferta inconsistente de treinamentos), 03) explorar as oportunidades externas (como o avanço de soluções de treinamento) e 04) reduzir a exposição às ameaças do ambiente. Dessa forma, a proposta é, a partir dos resultados obtidos e análise de resultados, estruturar um conjunto de ações que contribuam para a melhroia contínua das práticas e comportamento de segurança da digital, alinhando a atuação da Engenharia de Produção às necessidades da área de cibersegurança.

A primeira ferramenta utilizada foi a ferramenta SIPOC, frequentemente utilizada no Lean Six Sigma

para mapeamento de processos foi utilizada para mapear de forma simples e visual o processo de onboarding e desenvolvimento de competências em cibersegurança, além da instalação e atualização de antivírus e anti-spyware. Essa ferramenta auxilia de maneira visual na identificação de pontos de melhoria em um processo de negócio, por meio da visualização de Suppliers (Fornecedores), Inputs (Entradas), Process (Processo), Outputs (Saídas) e Customers (Clientes).

S	I	P	O	C
Suppliers (Fornecedores)	**Inputs (Entradas)**	**Process (Processo)**	**Outputs (Saídas)**	**Customers (Clientes)**
Recursos Humanos (RH)	Conteúdos do treinamento (cursos, materiais de capacitação, questionários, simuladores de phishing, plataforma gamificada)	Planejamento do onboarding inicial de segurança digital	Execução de treinamentos iniciais obrigatórios com novos integrantes da empresa	Colaboradores
Equipe interna de TI ou empresa contratada de cibersegurança	Política organizacional de segurança da informação	Criação e implementação da política de segurança organizacional	Dispositivos configurados de acordo com a política da empresa	Área de TI e de Segurança da Informação, empresa como um todo
Liderança, gerência ou diretoria	Treinamentos periódicos	Avaliação do conhecimento por meio de questionários gamificados ou simulações práticas de phishing	Relatórios de participação e desempenho no treinamento, com possível ponto de atenção para colaboradores com baixa performance	Liderança da empresa
Equipe interna de TI ou empresa contratada de cibersegurança	Dispositivos de TI com antivírus e anti-spyware instalados	Configuração e atualização periódica dos antivírus, antispyware e demais ferramentas de segurança necessárias de acordo com a realidade da empresa	Atualização periódica das ferramentas de cibersegurança (como antivírus e antispyware)	Área de TI e de Segurança da Informação
Recursos Humanos (RH), equipe interna de TI ou empresa contratada de cibersegurança	Atualização dos conteúdos do treinamento de acordo com novas tendências de cibersegurança	Revisão periódica e atualização contínua do treinamento em segurança	Colaboradores com comportamento mais positivo e aderente às práticas de segurança cibernética	Organização como um todo (beneficiada por uma cultura de segurança)

Quadro 9 – SIPOC
Fonte: Autoria própria (2025).

Com o mapeamento do processo por meio do SIPOC, torna-se possível visualizar os principais pontos que impactam o comportamento e a percepção de segurança dos colaboradores e visualizar ações de onboarding, treinamento e instalação de softwares de cibersegurança, citados anteriormente no IPMA. A partir dessa base, outras ferramentas da Engenharia de Produção podem ser aplicadas para aprofundar o desenvolvimento de competências, promover a melhoria contínua e acompanhar os resultados obtidos.

Além da matriz SIPOC, a notação BPMN (Business Process Model and Notation) também poderia ser utilizada como complemento para detalhar visualmente os fluxos dos processos mapeados, permitindo uma análise mais aprofundada de etapas, decisões e pontos críticos. Combinadas, as duas ferramentas contribuem para um entendimento completo dos processos que impactam a percepção de segurança da informação na organização.

Nesse contexto, a partir da análise dos processos realizada com o SIPOC e detalhamento com BPMN, o Plano de Desenvolvimento Individual (PDI) se destaca como uma ferramenta essencial para estruturar o desenvolvimento das competências em segurança da informação que os colaboradores precisam adquirir e reforçar no seu dia a dia e para auxiliar no onboarding e continuidade do treinamento de cibersegurança. O PDI é uma ferramenta que permite personalizar o desenvolvimento à nível de cada colaborador e pode ser estruturado pelo RH ou liderança direta de cada usuário. O PDI deve ser estruturado seguindo metas SMART (Specific, Measurable, Achievable, Relevant, e Time-bound), o que facilita o acompanhamento da evolução dos colaboradores e ajuda a reduzir fraquezas, como a oferta inconsistente de treinamentos (OST2), identificada no IPMA.

Enquanto o PDI possui como foco no nível individual de cada colaborador, torna-se necessário também uma ferramenta para foco no nível organizacional. Nesse sentido, podem ser mensurados KPIs (Key Performance Indicators), são indicadores chaves para a empresa como um todo. Levando em consideração os resultados do IPMA, foi estruturada a tabela base de KPIs, que pode ser visualizada abaixo. Os KPIs, bem como sua frequência, responsável e meta podem ser adaptados de acordo com a realidade de cada organização.

Nome do KPI	Descrição	Frequência	Responsável	Meta desejada	Justificativa para inclusão
% de colaboradores treinados em segurança digital	Mede o percentual de colaboradores que concluíram os treinamentos obrigatórios de	Trimestral	RH	≥ 95% dos colaboradores treinados	Ligado a OST2 do IPMA (fraqueza)

Nome do KPI	Descrição	Frequência	Responsável	Meta desejada	Justificativa para inclusão
% de dispositivos com antispyware instalado e atualizado	Mede o percentual de dispositivos que possuem antispyware corretamente instalado e atualizado	Mensal	TI	100% dos dispositivos corporativos com antispyware instalado e atualizado	Ligado a ISM4 do IPMA (fraqueza)
% de colaboradores que compreendem a política de segurança da informação	Mede, por meio de avaliação simples (quis gamificado), o percentual de colaboradores que compreendem a política de segurança organizacional	Semestral	RH	≥ 90% com compreensão satisfatória	Ligado a OSP3 do IPMA (força a ser mantida)
% de novos colaboradores que receberam onboarding completo em segurança	Mede se os novos colaboradores passaram por todas as etapas de onboarding em segurança	Trimestral	RH, TI e lideranças diretas	≥ 100% dos novos colaboradores treinados no prazo	Ligado ao SIPOC (processo mapeado)
% de participação em simulações de phishing	Mede a taxa de participação e engajamento dos colaboradores nas campanhas práticas de simulação de phishing	Trimestral	RH e lideranças diretas	≥ 95% de participação nas simulações	Ligado às oportunidades externas (treinamentos práticos, simulações)
Taxa de incidentes causados por erro humano	Mede a proporção de incidentes de segurança com causa raiz erros de comportamento humano (sejam eles intencionais ou não)	Mensal	RH, TI e lideranças diretas	Tendência de redução contínua	Ligado ao problema central do estudo (fatores humanos na cibersegurança)

Quadro 10 – KPIs

Fonte: Autoria própria (2025).

A definição e o acompanhamento dos KPIs são essenciais para monitorar a evolução das práticas de segurança digital em um contexto de nível organizacional. No entanto, para garantir que essas práticas sejam continuamente aprimoradas e adaptadas às novas demandas e ameaças, é importante estruturar um ciclo de gestão baseado na melhoria contínua e revisão sistemática. Nesse sentido, o ciclo PDCA (Planejar, Executar, Verificar, Agir) oferece um framework para realização desse acompanhamento contínuo, sendo a última ferramenta proposta neste trabalho para apoiar a melhoria do comportamento de segurança em ambientes de trabalho digitais.

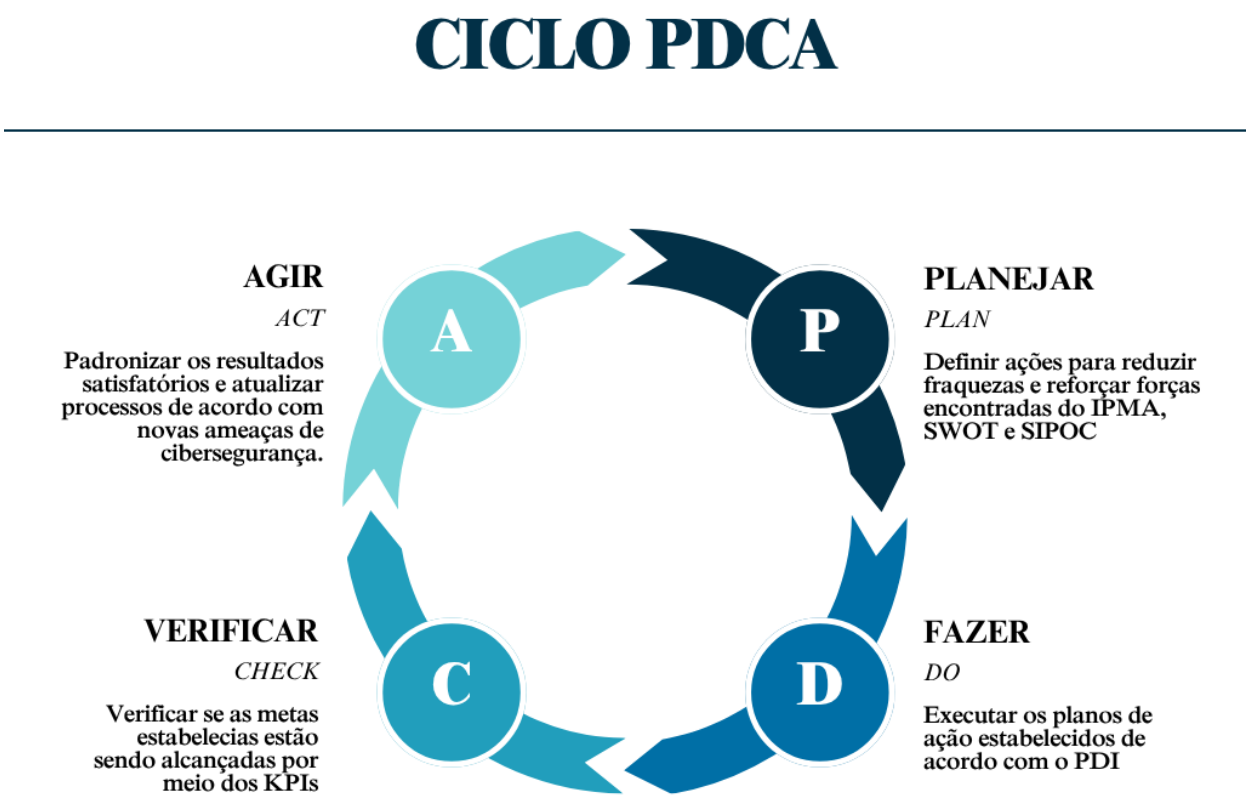


Figura 22 – Ciclo PDCA
Fonte – Autoria própria (2025).

O ciclo PDCA (Planejar, Executar, Verificar, Agir) é uma abordagem prática e amplamente utilizada na Engenharia de Produção para promover a melhoria contínua. Sua utilização é de suma importância para garantir que as práticas de segurança cibernética evoluam de forma estruturada e consistente, tendo em vista que as ameaças se alteram muito rapidamente, com novos e mais sofisticados ataques surgindo diariamente ao redor do mundo e crescentes ameaças cibernéticas do tipo zero-day. Na etapa de Planejamento (P, Plan), a organização deve definir ações específicas priorizando a mitigação das fraquezas e indicadores de baixo desempenho, mas alta importância, identificados no IPMA, como a oferta inconsistente de treinamentos (OST2) e o baixo uso de antispyware (ISM4), além de estruturar iniciativas para reforçar as forças mapeadas, de alto desempenho e alta importância, como a compreensão da política de segurança (OSP3) e o uso

consolidado de antivírus (ISM2). O planejamento deve contemplar também o aprimoramento dos processos mapeados no SIPOC e nas oportunidades da análise SWOT, como a integração de conteúdos atualizados no treinamento e a padronização e inclusão de temas de segurança digital no onboarding de novos colaboradores. Na etapa de Execução (D, Do), as ações devem ser implementadas conforme planejado, com cronogramas claros e responsáveis definidos anteriormente de acordo com a realidade de cada organização. Em Verificação (C, Check), os resultados devem ser acompanhados por meio dos KPIs, que foram definidos seguindo a metodologia SMART. Por fim, na etapa de Ação (A, Act), os planos de ação devem ser ajustados de acordo com os resultados obtidos e com as mudanças no cenário de cibersegurança, de forma a garantir a evolução contínua das práticas de segurança digital adotadas pela organização. Dessa maneira, o ciclo PDCA contribui para que as práticas de segurança digital se mantenham alinhadas e atualizadas de acordo com a realidade do negócio e cenário externo, fortalecendo a percepção de cibersegurança entre os colaboradores e reforçando comportamentos positivos de segurança digital.

Ao integrar ferramentas de Engenharia de Produção (SWOT, SIPOC, BPMN, PDI, KPIs e ciclo PDCA) nos resultados deste trabalho, espera-se que as organizações possam implementar melhorias de forma estruturada, contínua e mensurável, contribuindo não apenas para a segurança técnica, mas também para o fortalecimento da cultura de cibersegurança entre os colaboradores em um contexto de ambientes de trabalho digitais.

7. CONSIDERAÇÕES FINAIS, LIMITAÇÕES E FUTURAS LINHAS DE PESQUISA

O problema desta pesquisa foi compreender quais são os principais fatores que influenciam na percepção de segurança dos trabalhadores em um contexto de ambientes de trabalho digitais. Para isso, foi realizada uma pesquisa quantitativa, de caráter explicativo, com aplicação de equações estruturais (PLS-SEM), a partir da adaptação do modelo de Saeed (2023), utilizando uma amostra de 119 profissionais da cidade de Brasília.

Por meio da validação estatística das hipóteses H1, H2 e H5, constatou-se que Suporte e Treinamento Organizacional (OST) explica 9,12% da Percepção de Segurança (POS), sendo a hipótese que mais contribui para essa variável. Além disso, verificou-se que Gerenciamento de Senhas (PM) e Gerenciamento de Segurança de Infraestrutura (ISM) também têm influência significativa sobre a Percepção de Segurança (POS). Por sua vez, as hipóteses H3 e H4 não foram suportadas.

A análise do Mapa de Importância-Desempenho (gráfico IPMA) destacou fatores-chave que impactam diretamente a percepção de segurança dos trabalhadores em ambientes digitais. Com base nessa análise, foi desenvolvido um framework com recomendações práticas, priorizando os construtos de maior importância e menor desempenho, a fim de orientar ações estratégicas para uma melhor segurança digital nas organizações. Essas propostas foram fundamentadas em ferramentas e métodos da Engenharia de Produção, integrados a um processo de melhoria contínua da segurança organizacional. O objetivo é promover ambientes digitais mais seguros, fortalecendo a percepção de segurança dos colaboradores e reduzindo vulnerabilidades causadas por falhas humanas.

Apesar dos resultados satisfatórios, o estudo apresenta algumas limitações. A principal delas refere-se à amostra, restrita geograficamente a trabalhadores do Distrito Federal (DF), o que limita a generalização dos resultados para toda a população. Diferenças regionais, culturais e setoriais podem impactar a percepção de segurança dos trabalhadores e nem todas essas variáveis foram contempladas no presente estudo. Além disso, faixas etárias distintas podem apresentar percepções e comportamentos diferentes em relação à segurança digital, visto que o uso de tecnologias e a inserção no ambiente digital variam entre gerações,

Para futuras linhas de pesquisa, sugere-se a ampliação da amostra, tanto numericamente quanto geograficamente, para maior representatividade da realidade dos trabalhadores em contextos digitais. Além disso, incluir pesquisas qualitativas, como entrevistas mais aprofundadas, pode complementar os achados da pesquisa quantitativa, permitindo explorar nuances que podem ficar ocultas ou distorcidas nas respostas aos questionários, como a realização de comportamentos inseguros por parte dos usuários. Dessa forma, espera-se que estudos futuros e novas investigações continuem contribuindo para um ambiente digital mais seguro.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ABDRABOU, Yasmeen. **"Your Eyes Tell You Have Used This Password Before": Identifying Password Reuse from Gaze and Keystroke Dynamics.** Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, 2022. p. 1-16.

ACAR, Yasemin; FAHL, Sascha; MAZUREK, Michelle L. **You are not your developer, either: A research agenda for usable security and privacy research beyond end users.** 2016 IEEE Cybersecurity Development (SecDev), p. 3-8, 2016.

AJZEN, Icek. **Constructing a TPB questionnaire: Conceptual and methodological considerations.** 2002.

ALANAZI, Marfua; FREEMAN, Mark; TOOTELL, Holly. **Exploring the factors that influence the cybersecurity behaviors of young adults.** Computers in Human Behavior, v. 136, p. 107376, 2022.

ALBRECHT, Carmen-Maria. **Value creation for luxury brands through brand extensions.** Luxusmarkenmanagement: Grundlagen, Strategien und praktische Umsetzung, p. 261-283, 2017.

AMANKWAH-AMOAH, Joseph et al. **COVID-19 and digitalization: The great acceleration.** Journal of Business Research, v. 136, p. 602-611, 2021.

ANWAR, Mohd. **Gender difference and employees' cybersecurity behaviors.** Computers in Human Behavior, v. 69, p. 437-443, 2017.

ASLAN, Ömer et al. **A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions.** Electronics, v. 12, n. 6, p. 1333, 2023.

BADA, Maria; NURSE, Jason RC. **Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs).** Information & Computer Security, v. 27, n. 3, p. 393-410, 2019.

BEURAN, Razvan et al. **Integrated framework for hands-on cybersecurity training: CyTrONE.** Computers & Security, v. 78, p. 43-59, 2018.

BRAUN, Virginia; CLARKE, Victoria. **Using thematic analysis in psychology.** Qualitative Research in Psychology, v. 3, n. 2, p. 77-101, 2006.

CANFIELD, Casey Inez; FISCHHOFF, Baruch; DAVIS, Alex. **Quantifying phishing susceptibility for detection and behavior decisions.** Human Factors, v. 58, n. 8, p. 1158-1172, 2016.

CHANDA, Razib Chandra et al. **Assessing cybersecurity awareness among bank employees: A multi-stage analytical approach using PLS-SEM, ANN, and fsQCA in a developing country context.** Computers & Security, v. 149, p. 104208, 2025.

CHONG, Isis; XIONG, Aiping; PROCTOR, Robert W. **Human factors in the privacy and security of the internet of things.** Ergonomics in Design, v. 27, n. 3, p. 5-10, 2019.

CLAFFY, K. C. **The workshop on active internet measurements (AIMS) report.** ACM SIGCOMM Computer Communication Review, v. 39, n. 5, p. 32-36, 2009.

DUTTA, Amitava; MCCROHAN, Kevin. **Management's role in information security in a cyber economy.** California Management Review, v. 45, n. 1, p. 67-87, 2002.

EVANS, Mark. **Human behaviour as an aspect of cybersecurity assurance.** Security and Communication

Networks, v. 9, n. 17, p. 4667-4679, 2016.

FORNELL, Claes; LARCKER, David F. **Evaluating structural equation models with unobservable variables and measurement error.** Journal of Marketing Research, v. 18, n. 1, p. 39-50, 1981.

GHOBAKHLOO, Morteza**. Industry 4.0, digitization, and opportunities for sustainability.** Journal of Cleaner Production, v. 252, p. 119869, 2020.

HAIR JR, Joseph F. et al. **Partial least squares structural equation modeling (PLS-SEM) using R: A workbook.** Springer Nature, 2021.

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

HADLINGTON, Lee. **Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.** Heliyon, v. 3, n. 7, 2017.

HONG, Wilson Cheong Hin. **The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates.** Education and Information Technologies, v. 28, n. 1, p. 439-470, 2023.

HOVAV, Anat; PUTRI, Frida Ferdani. **This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy.** Pervasive and Mobile Computing, v. 32, p. 35-49, 2016.

HyveSystems. **Are Your Passwords in the Green?.** Disponível em: https://www.hivesystems.com/blog/are-your-passwords-in-the-green (acessado em 26 de maio de 2024).

ISO/IEC. **Information technology – code of practice for information security management, ISO/IEC 27002:2005.** The International Organization for Standardization/The International Electrotechnical Commission, 2005.

JAKOBSSON, Markus; MYERS, Steven. **Phishing and countermeasures: understanding the increasing problem of electronic identity theft.** John Wiley & Sons, 2006.

KHAN, Neeshe; HOUGHTON, Robert J.; SHARPLES, Sarah. **Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks.** Cognition, Technology & Work, v. 24, n. 3, p. 393-421, 2022.

KNAPP, Kenneth J. et al. **Information security policy: An organizational-level process model.** Computers & Security, v. 28, n. 7, p. 493-508, 2009.

LEE, Younghwa; KOZAR, Kenneth A. **An empirical investigation of anti-spyware software adoption: A multitheoretical perspective.** Information & Management, v. 45, n. 2, p. 109-119, 2008.

LONG, Rebecca M. **Using phishing to test social engineering awareness of financial employees.** 2013.

LOWRY, Paul Benjamin et al. **Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust.** Information Systems Journal, v. 25, n. 3, p. 193-273, 2015.

MANZATO, Antonio José; SANTOS, Adriana Barbosa. **A elaboração de questionários na pesquisa**

quantitativa. Departamento de Ciência de Computação e Estatística – IBILCE – UNESP, v. 17, 2012.

MARIANO, A. M.; GARCIA CRUZ, R.; ARENAS GAITAN, J. **Meta Análises como instrumento de pesquisa: uma revisão sistemática da bibliografia aplicada ao estudo das alianças estratégicas internacionais.** Congresso Internacional de Administração, UEPG, 2011.

MARIANO, A. M.; ROCHA, M. S. **Revisão da Literatura: Apresentação de uma Abordagem Integradora.** AEDM International Conference, 2017.

NIFAKOS, Sokratis; CHANDRAMOULI, Krishna; STATHAKAROU, Natalia. **Social Engineering: The Human Behavior Impact in Cyber Security Within Critical Information Infrastructures.** Springer Nature Switzerland, 2024. p. 173-184.

NIST. **Computer security resource center: resilience.** Disponível em: https://web.archive.org/web/20201128165137/https://csrc.nist.gov/glossary/term/resilience (acessado em 26 de maio de 2024).

NWANKPA, Joseph K.; DATTA, Pratim Milton. **Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers.** Computers & Security, v. 130, p. 103266, 2023.

ONUMO, Aristotle; CULLEN, Andrea; AWAN, Irfan. **Integrating behavioural security factors for enhanced protection of organisational information technology assets.** 2018 IEEE FiCloud Conference, p. 128-135.

PARVIAINEN, Päivi et al. **Tackling the digitalization challenge: how to benefit from digitalization in practice.** International Journal of Information Systems and Project Management, v. 5, n. 1, p. 63-77, 2017.

PIERCE, James. **Smart home security cameras and shifting lines of creepiness: A design-led inquiry.** In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019. p. 1-14.

PONEMON INSTITUTE. **2016 cost of cyber crime study & the risk of business innovation.** Ponemon Institute, 2016.

PROCTOR, Robert W.; CHEN, Jing. **The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace.** Human Factors, v. 57, n. 5, p. 721-727, 2015.

PUHAKAINEN, Petri; SIPONEN, Mikko. **Improving employees' compliance through information systems security training: an action research study.** MIS Quarterly, p. 757-778, 2010.

RAMÍREZ, Patricio E.; MARIANO, Ari Melo; SALAZAR, Evangelina A. **Propuesta Metodológica para aplicar modelos de ecuaciones estructurales con PLS: El caso del uso de las bases de datos científicas en estudiantes universitarios.** Revista ADMpg, v. 7, n. 2, 2014.

RINGLE, Christian M.; SARSTEDT, Marko. **Gain more insight from your PLS-SEM results: The importance-performance map analysis.** Industrial Management & Data Systems, v. 116, n. 9, p. 1865-1886, 2016.

SAEED, Saqib. **Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia.** Sustainability, v. 15, n. 7, p. 6019, 2023.

SARSTEDT, Marko; HAIR JR, Joseph F.; RINGLE, Christian M. **"PLS-SEM: indeed a silver bullet" – retrospective observations and recent advances.** Journal of Marketing Theory and Practice, v. 31, n. 3, p.

261-275, 2023.

SARSTEDT, Marko; RINGLE, Christian M.; HAIR, Joseph F. **Partial least squares structural equation modeling.** In: Handbook of Market Research. Cham: Springer International Publishing, 2021. p. 587-632.

SHEEHAN, Barry et al. **A quantitative bow-tie cyber risk classification and assessment framework.** Journal of Risk Research, v. 24, n. 12, p. 1619-1638, 2021.

SHEEHAN, Barry et al. **Connected and autonomous vehicles: A cyber-risk classification framework.** Transportation Research Part A: Policy and Practice, v. 124, p. 523-536, 2019.

SHENG, Steve. **Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.** Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010. p. 373-382.

SMITH, Zhanna Malekos; LOSTRI, Eugenia. **The hidden costs of cybercrime.** McAfee, 2020.

SOSTERO, Matteo et al. **Teleworkability and the COVID-19 crisis: a new digital divide?.** JRC Working Papers Series on Labour, Education and Technology, 2020.

STANTON, Jeffrey M. **Analysis of end user security behaviors.** Computers & Security, v. 24, n. 2, p. 124-133, 2005.

SUMECKI, David; CHIPULU, Maxwell; OJIAKO, Udechukwu. **Email overload: Exploring the moderating role of the perception of email as a 'business critical' tool.** International Journal of Information Management, v. 31, n. 5, p. 407-414, 2011.

TAM, Leona; GLASSMAN, Myron; VANDENWAUVER, Mark. **The psychology of password management: a tradeoff between security and convenience.** Behaviour & Information Technology, v. 29, n. 3, p. 233-244, 2010.

UEBELACKER, Sven; QUIEL, Susanne. **The social engineering personality framework.** In: 2014 Workshop on Socio-Technical Aspects in Security and Trust. IEEE, 2014. p. 24-30.

VERGARA, S. C. **Tipos de pesquisa em administração.** 1990.

VON SOLMS, Rossouw; VON SOLMS, Basie. **From policies to culture.** Computers & Security, v. 23, n. 4, p. 275-279, 2004.

WELK, Allaire K. et al. **Will the "Phisher-Men" Reel You In?: Assessing individual differences in a phishing detection task.** International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), v. 5, n. 4, p. 1-17, 2015.

WEN, Zikai Alex. **What. hack: engaging anti-phishing training through a role-playing phishing simulation game.** Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019. p. 1-12.

XIONG, Aiping. **Embedding training within warnings improves skills of identifying phishing webpages.** Human Factors, v. 61, n. 4, p. 577-595, 2019.

ZIMMERMANN, Verena et al. **Human-Centered Cybersecurity Revisited: From Enemies to Partners.** Communications of the ACM, v. 67, n. 11, p. 72-81, 2024.

APÊNDICES

APENDICE A: INSTRUMENTO DE COLETA DE DADOS



Ambientes de Trabalho Digitais e Comportamentos de Segurança da Informação de Trabalhadores

Sou uma estudante do curso de **Engenharia de Produção da UnB** e estou realizando uma pesquisa acadêmica para entender os **Comportamentos de Segurança da Informação de Trabalhadores em um contexto de Ambientes de Trabalho Digitais.**

Todas as perguntas presentes nesse questionário estão na escala Likert (1 a 5), onde a nota **"1" representa "discordo totalmente** " e a nota **"5" representa "concordo totalmente". A nota "3" representa a neutralidade.**
Participe dessa pesquisa, seus dados serão tratados com sigilo e os resultados serão para uso científico.

Caso haja qualquer dúvida, entre em contato com a aluna pelo e-mail **190039485@aluno.unb.br**. Ficarei contente em ajudar. Agradeço pela participação!

PM1. Eu utilizo a mesma senha para acessar múltiplos sistemas. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

PM2. Se eu altero minha senha, é principalmente por causa da política da empresa. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

PM3. Quando eu altero minha senha, uso minha senha antiga como base. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

PM4. Eu mantenho meus nomes de usuário/senhas em um arquivo eletrônico ou os escrevo. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

PM5. Eu utilizo um software para gerenciar minhas senhas. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

PM6. Eu compartilho minha senha com outros colegas. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM1. Meu computador pessoal possui um programa de antivírus instalado. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM2. O programa antivírus é atualizado regularmente. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM3. Eu tenho um firewall instalado no meu computador. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM4. Eu utilizo uma ferramenta anti-spyware no meu computador. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM5. Eu permito scripting no meu computador *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM6. Eu sempre faço log off ou bloqueio o computador quando me afasto dele. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM7. Eu utilizo um bloqueio de tela protegido por senha. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

ISM8. Eu utilizo sites de redes sociais no meu computador de trabalho. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

EM1. Eu abro E-mails mesmo se eu não sei quem é o remetente. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

EM2. Eu abro até mesmo anexos de E-mails quando eu não sei quem é o remetente. *

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

EM3. Eu utilizo criptografia ao enviar E-mails. *

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

EM4. Ao utilizar E-mail baseado na Web ou softwares de calendário, presto atenção às configurações de segurança do software baseado na Web. *

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

OSP1. Eu acho importante prestar atenção à segurança do computador. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OSP2. Minha organização possui uma política de segurança da informação. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OSP3. Eu entendo a política de segurança da informação da minha organização. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OSP4. Eu desvio ou contorno a política de segurança do computador da minha organização. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OSP5. Eu acho que meus colegas desviam ou contornam a política de segurança do computador. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OSP6. Se eu ou meus colegas desviarmos ou contornarmos a política de segurança do computador e alguém descobrir, haverá repercussões. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OST1. Se eu tiver problemas com um aplicativo de computador, é fácil para mim entrar em contato com meu administrador de rede ou sistema ou com o serviço de suporte. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OST2. Eu recebi treinamento em segurança da informação. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

OST3. O treinamento em segurança da informação me ajudou a entender melhor a política de segurança da organização. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

POS1. Eu acredito que meu computador pessoal é seguro. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

POS2. Eu acredito que posso proteger meu computador de hackers/phishers, se cuidar bem da segurança do computador. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

POS3. A segurança do computador me preocupa. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

POS4. Eu acho que faz diferença se eu prestar atenção especial à segurança do computador, como por exemplo, instalar um navegador menos vulnerável. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

POS5. Eu acho que as informações que mantenho no meu computador não são interessantes o suficiente para as pessoas tentarem invadir meu computador. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

POS6. Eu acho que não importa o que eu faça, se as pessoas tiverem más intenções, elas conseguirão invadir meu computador e nossa rede. *

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Qual é a sua identidade de gênero? *

- ◯ Feminino
- ◯ Masculino
- ◯ Outro

Qual é a sua faixa etária? *

- ◯ Menor que 18
- ◯ 19 - 25 anos
- ◯ 26 - 35 anos
- ◯ 36 - 50 anos
- ◯ Acima de 50 anos

Qual é a área de atuação da organização onde você trabalha? *

- ◯ Manufatura
- ◯ Serviços
- ◯ Governo
- ◯ Organização sem fins lucrativos
- ◯ Outro

Enviar Limpar formulário