



UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO



DIOGO WELLYNGTON DE SOUZA BARBOSA

**SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE NO TRABALHO REMOTO:
UMA ANÁLISE SOBRE OS RECURSOS PROVIDOS E ADOÇÃO DE BOAS
PRÁTICAS**

RECIFE

2023

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

DIOGO WELLYNGTON DE SOUZA BARBOSA

**SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE NO TRABALHO REMOTO:
UMA ANÁLISE SOBRE OS RECURSOS PROVIDOS E ADOÇÃO DE BOAS
PRÁTICAS**

Monografia apresentada ao Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE), como requisito parcial para conclusão do Curso de Ciência da Computação, orientada pelo(a) professor(a) Dra. Jessyka Flavianne Ferreira Vilela.

RECIFE

2023

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Barbosa, Diogo Wellyngton de Souza.

Segurança da informação e privacidade no trabalho remoto: uma análise sobre os recursos providos e adoção de boas práticas / Diogo Wellyngton de Souza Barbosa. - Recife, 2023.

102 : il., tab.

Orientador(a): Jéssyka Flavyanne Ferreira Vilela

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Ciências da Computação - Bacharelado, 2023.

Inclui referências, apêndices.

1. Trabalho remoto. 2. Teletrabalho. 3. Privacidade. 4. Segurança da Informação. 5. Ambiente de Trabalho. I. Vilela, Jéssyka Flavyanne Ferreira. (Orientação). II. Título.

000 CDD (22.ed.)

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

DIOGO WELLYNGTON DE SOUZA BARBOSA

SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE NO TRABALHO REMOTO:
UMA ANÁLISE SOBRE OS RECURSOS PROVIDOS E ADOÇÃO DE BOAS
PRÁTICAS

Monografia submetida ao corpo docente da Universidade Federal de Pernambuco, defendida e aprovada em 02 de outubro de 2023.

Banca Examinadora:

Jéssyka Flavianne Ferreira Vilela

Doutor(a)

Orientador(a)

Kiev Santos da Gama

Doutor(a)

Examinador(a)

Dedico este trabalho aos meus pais, que sempre me apoiaram e forneceram o suporte necessário. Além disso, gostaria de estender meus sinceros agradecimentos aos meus amigos da faculdade e à minha orientadora, pois sem o apoio deles, este trabalho não teria sido possível.

AGRADECIMENTOS

Primeiramente, quero expressar minha profunda gratidão a Deus por me conceder a capacidade, a força e a paciência necessárias para concluir este trabalho.

Gostaria de estender meus sinceros agradecimentos a pessoas que desempenharam papéis fundamentais em minha vida e na realização deste projeto.

Minha mãe, Gilvaneide de Souza Barbosa, sempre foi meu alicerce. Durante o desenvolvimento deste trabalho, ela me apoiou incondicionalmente e segurou minha mão nos momentos em que eu estava prestes a desistir e me sentia exausto.

Ao meu pai, Ugo Rufino Barbosa, agradeço por investir em minha educação e por me criar com amor e carinho, mesmo estando distante.

Quero deixar minha imensa gratidão à minha amiga e namorada, Joseane Maria, que foi a primeira pessoa a quem recorri quando estava no limite físico e mental devido a outros desafios durante a elaboração deste trabalho. Ela me acalmou, depositou sua confiança em mim e me deu forças para continuar minha jornada.

À professora Jessyka Flavyanna Ferreira Vilela, agradeço por sua orientação neste trabalho. Sua perseverança durante o longo período de desenvolvimento foi essencial, e cada correção e incentivo impulsionaram meu progresso.

Lembro-me também de todos os colegas e amigos que a universidade me proporcionou. Agradeço o apoio de alguns deles para que eu pudesse concluir minha graduação e por serem companheiros valiosos de curso. Especialmente aos meus amigos da turma de 2014.2, que continuam a ser grandes amigos mesmo após a graduação.

Estendo meus sinceros agradecimentos a todos os professores que fazem parte da minha trajetória acadêmica, desde a disciplina de introdução à computação até o trabalho de graduação.

Alguns amigos de trabalho também desempenharam um papel crucial na conclusão deste trabalho. Quero citar Neto Maciel, que me incentivou a concluir minha pesquisa, e Diogo Pinheiro, do setor de segurança da informação da minha empresa, que colaborou fornecendo feedback valioso sobre a pesquisa.

A todos vocês, minha profunda gratidão. Sem o apoio e encorajamento de cada um, esta conquista não teria sido possível.

“A privacidade é uma questão de direitos humanos e uma parte essencial da dignidade humana. A segurança da informação desempenha um papel crítico na proteção desses direitos e na preservação da liberdade individual na era digital”

(Tim Cook)

RESUMO

Nos últimos anos, houve um aumento notável na adoção do trabalho remoto por parte das empresas, impulsionado principalmente pela pandemia de COVID-19. Isso ocorreu à medida que as empresas buscavam soluções para manter suas operações em andamento, enquanto respeitavam as medidas de distanciamento social amplamente implementadas pelos governos em todo o mundo para conter a propagação da doença. Embora o conceito de teletrabalho não seja novo e tenha raízes nas décadas de 1970, quando a Crise do Petróleo levou as empresas a procurarem alternativas para reduzir os custos de transporte de seus funcionários, sua adoção em larga escala é relativamente recente. Para os funcionários, o trabalho remoto oferece vantagens significativas, como flexibilidade, economia de tempo com deslocamentos, melhoria na qualidade de vida e aumento da produtividade. Por outro lado, para as empresas, essa prática proporciona economia em relação aos custos operacionais dos escritórios, maior acesso a talentos e a possibilidade de expandir seus negócios. No entanto, a implementação bem-sucedida do trabalho remoto também traz desafios, incluindo a necessidade de fornecer recursos e ferramentas adequadas para os funcionários, pois o trabalho remoto depende fortemente da utilização de tecnologia da informação e comunicação. Além disso, a segurança da informação e a privacidade são questões críticas, especialmente com a vigência das leis de proteção de dados em todo o mundo. Esses dois últimos desafios representam as maiores preocupações, uma vez que as empresas estão cada vez mais atentas a questões relacionadas à segurança e privacidade. Avaliar o ambiente de trabalho remoto das pessoas é de suma importância para identificar possíveis lacunas na segurança dos dados das empresas e na privacidade de seus funcionários. Este trabalho tem como objetivo analisar as boas práticas e os mecanismos de segurança da informação implementados pelas empresas no contexto do teletrabalho e verificar se seus funcionários estão comprometidos em adotá-los. Para essa finalidade, uma pesquisa foi conduzida utilizando a metodologia de pesquisa "survey". Para a coleta dos dados da pesquisa, foi desenvolvido um questionário que explorou questões relacionadas ao comportamento, atitudes e conhecimento dos participantes em relação à segurança e privacidade no teletrabalho. Além disso, o questionário coletou informações sobre os recursos fornecidos pelas empresas e instituições onde os participantes trabalham. Ao final da pesquisa, foi identificado um cenário relativamente positivo, mas também foram identificadas lacunas que precisam ser preenchidas, principalmente no que diz respeito à privacidade dos funcionários e à disseminação do conhecimento por parte das empresas. Isso destaca a importância contínua de abordar questões de segurança da informação e privacidade à medida que o trabalho remoto continua a se desenvolver.

Palavras-chave: Trabalho Remoto, Teletrabalho, Privacidade, Segurança da Informação, Ambiente de Trabalho.

ABSTRACT

In recent years, there has been a notable increase in the adoption of remote work by companies, driven mainly by the COVID-19 pandemic. This occurred as companies sought solutions to keep their operations running while respecting the social distancing measures widely implemented by governments around the world to contain the spread of the disease. Although the concept of telecommuting is not new and has roots in the 1970s, when the Oil Crisis led companies to look for alternatives to reduce the costs of commuting their employees, its large-scale adoption is relatively recent. For employees, remote work offers significant advantages, such as flexibility, saving time on travel, improving quality of life and increasing productivity. On the other hand, for companies, this practice provides savings in relation to office operating costs, greater access to talent and the possibility of expanding their business. However, successfully implementing remote work also brings challenges, including the need to provide adequate resources and tools for employees, as remote work relies heavily on the use of information and communications technology. Furthermore, information security and privacy are critical issues, especially with data protection laws in force around the world. These last two challenges represent the biggest concerns, as companies are increasingly aware of issues related to security and privacy. Assessing people's remote work environment is extremely important to identify possible gaps in companies' data security and the privacy of their employees. This work aims to analyze good practices and information security mechanisms implemented by companies in the context of teleworking and verify whether their employees are committed to adopting them. For this purpose, a survey was conducted using the "survey" research methodology. To collect research data, a questionnaire was developed that explored issues related to participants' behavior, attitudes and knowledge regarding security and privacy when teleworking. Furthermore, the questionnaire collected information about the resources provided by the companies and institutions where the participants work. At the end of the research, a relatively positive scenario was identified, but gaps that need to be filled were also identified, especially with regard to employee privacy and the dissemination of knowledge by companies. This highlights the continued importance of addressing information security and privacy concerns as remote work continues to develop.

Keywords: Remote Working, teleworking, Privacy, Information Security, Remote Working Environment.

SUMÁRIO

1. INTRODUÇÃO.....	1
1.1 Contexto e motivação.....	1
1.2 Objetivos.....	3
1.3 Trabalhos Relacionados.....	3
1.3.1 Avaliação da Cultura de Segurança da Informação: A Aplicação de um Survey sobre Cultura de Segurança da Informação nas Organizações.....	4
1.3.2 Working from home during COVID-19 crisis: a cyber security culture assessment survey.....	5
1.3.3 Análise das dimensões dos trabalhos.....	6
1.4 Estrutura do documento.....	8
2. REVISÃO DA LITERATURA.....	9
2.1 Teletrabalho.....	9
2.2 Uso de dispositivos pessoais no trabalho - Byod.....	11
2.3 Segurança da Informação e Privacidade no trabalho remoto.....	13
2.4 Leis de proteção de dados.....	14
2.5 Engenharia social.....	16
3. METODOLOGIA.....	18
3.1 Definição dos objetivos da pesquisa.....	19
3.2 Identificação de características do público-alvo.....	19
3.3 Definição do plano de amostragem.....	21
3.4 Elaboração do questionário.....	22
3.5 Condução do teste piloto.....	23
3.6 Distribuição do questionário.....	24
3.7 Análise dos resultados obtidos.....	25
3.8 Ameaças à validade e considerações éticas.....	25
3.8.1 Validade de Construção.....	26
3.8.2 Validade Interna.....	26
3.8.3 Validade Externa.....	27
3.8.4 Validade de Conclusão.....	28
3.8.5 Aspecto Ético da Pesquisa.....	28
4. Resultados da pesquisa.....	30
4.1 Limpeza e tratamento dos dados.....	30
4.2 Perfil dos participantes.....	31
4.3 Comportamento dos participantes.....	45
Pergunta 14 - “Você utiliza recurso pessoal para fins de trabalho? Exemplo: Computador pessoal, celular pessoal, licença de software pessoal, etc...”.....	45
Pergunta 15 - “Quando você trabalha na sua casa, geralmente você trabalha em qual cômodo?”.....	47
Pergunta 16 - “Você costuma trabalhar em ambientes de coworking?”.....	47

Pergunta 17 - “Você compartilha suas credenciais de sistemas com outras pessoas?”	48
Pergunta 18 - “Você bloqueia seu computador ao se ausentar da mesa?”	49
Pergunta 19 - “Você costuma trabalhar com seus equipamentos conectados em redes de internet públicas (por exemplo: Wifi de shoppings, aeroportos, cafés)?”	50
Pergunta 20 - “Você troca suas senhas com qual frequência?”	51
Pergunta 21 - Você usa seu computador ou equipamentos de trabalho para fins pessoais?	52
Pergunta 22 - “Você empresta seu computador ou equipamento de trabalho para terceiros?”	53
Pergunta 23 - Você comenta assuntos sigilosos relacionados ao seu trabalho no ambiente doméstico?	54
Pergunta 24 - Você participa de reuniões sem fones de ouvido mesmo quando há outras pessoas próximas?	55
Pergunta 25 - Você costuma fechar a Webcam e o microfone dos seus equipamentos quando não está utilizando?	56
Pergunta 26 - Você costuma trafegar informações de trabalho em redes sociais como Facebook, WhatsApp, Instagram e outras?	57
Pergunta 27 - Você já participou de treinamentos sobre segurança da informação?	58
Pergunta 28 - Você foi instruído a tomar medidas de segurança específicas para trabalhar remotamente?	59
Pergunta 29 - Você foi instruído a tomar medidas de segurança específicas para trabalhar remotamente?	60
4.4 Recursos providos pelas instituições e empresas aos seus funcionários.....	62
4.5 Nível de conhecimento sobre a importância de alguns tópicos relacionados a segurança e privacidade no trabalho remoto.....	63
4.6 Discussão sobre os resultados.....	66
5. CONCLUSÕES FINAIS E TRABALHOS FUTUROS.....	76
5.1 Conclusões.....	77
5.2 Contribuições do trabalho.....	79
5.3 Trabalhos futuros.....	80
REFERÊNCIAS.....	81
APÊNDICES.....	89
APÊNDICE A - Termo de consentimento de participação.....	89
APÊNDICE B - Questionário da pesquisa.....	90

LISTA DE FIGURAS

Figura 1 - Fluxograma da metodologia da pesquisa survey.....	18
Figura 2 - Gráfico de particionamento dos dados após limpeza e filtragem.....	31
Figura 3 - Faixa etária do público-alvo.....	32
Figura 4 - Maior grau de instrução de cada participante.....	33
Figura 5 - Áreas de formação categorizadas.....	35
Figura 6 - Áreas de trabalho de cada participante categorizadas.....	37
Figura 7 - Setores das instituições onde os participantes trabalham.....	38
Figura 8 - Porte da Instituição.....	39
Figura 9 - Tempo de trabalho na instituição atual de trabalho dos participantes.....	40
Figura 10 - Setores e departamentos onde os participantes atuam nas suas instituições de trabalho.....	43
Figura 11 - Regimes de trabalho do público alvo.....	44
Figura 12 - Distribuição de participantes pelas suas regiões globais de atuação.....	45
Figura 13 - Ramos de atividades econômicas das instituições dos participantes categorizados.....	46
Figura 14 - Utilização de recursos próprios para fins de trabalho.....	47
Figura 15 - Utilização de recursos próprios para fins de trabalho, comparação entre os modelos de trabalho remoto.....	47
Figura 16 - Cômodos utilizados para trabalho em casa.....	48
Figura 17 - Participantes que trabalham em coworking.....	49
Figura 18 - Compartilhamento de credenciais.....	49
Figura 19 - Bloqueio do computador ao se ausentar da mesa.....	50
Figura 20 - Bloqueio do computador ao se ausentar da mesa restrito no ambiente de coworking.....	51
Figura 21 - Uso de redes públicas para trabalho.....	52
Figura 22 - Frequência de trocas de senhas.....	53
Figura 23 - Uso dos equipamentos de trabalho para fins pessoais.....	54
Figura 24 - Empréstimo de equipamentos de trabalho para terceiros.....	55
Figura 25 - Costume de comentar assuntos sigilosos do trabalho em ambiente doméstico.....	56
Figura 26 - Uso de fone de ouvido em reuniões.....	57
Figura 27 - Costume de fechar a webcam e o microfone enquanto estão ociosos.....	58
Figura 28 - Costume de trafegar dados do trabalho em redes sociais.....	59
Figura 29 - Dados referentes à realização de treinamentos de segurança.....	60
Figura 30 - Dados sobre instruções de segurança específicas.....	61
Figura 31 - Conhecimento sobre dados pessoais ou sensíveis.....	65
Figura 32 - Análise do nível de conhecimento sobre a importância dos itens citados na questão 31.....	66
Figura 33 - Uso de recursos pessoais para fins de trabalho por porte da empresa.....	70
Figura 34 - Uso dos equipamentos providos pelas empresas para fins pessoais.....	71
Figura 35 - Tráfego de dados do trabalho através de redes sociais por porte das empresas e instituições.....	72
Figura 36 - Bloqueios de webcam e microfone ociosos em diferentes tipos de	

cômodos.....	73
Figura 37 - Relação de conhecimento e proteção de dados sigilosos e sensíveis.....	74
Figura 38 - Distribuição dos itens pelas instituições e empresas.....	75
Figura 39 - Relação de disseminação de orientações específicas para o trabalho remoto.....	76

LISTA DE TABELAS

Tabela 1 - Comparação entre os trabalhos relacionados e o trabalho proposto.....	7
Tabela 2 - Tabela de particionamento dos dados após limpeza e filtragem.....	31
Tabela 3 - Tabela de categorização das áreas de formação dos participantes.....	34
Tabela 4 - Resultado da categorização das áreas de formação.....	34
Tabela 5 - Áreas de trabalho dos participantes.....	36
Tabela 6 - Áreas de trabalho dos participantes categorizadas.....	37
Tabela 7 - Setor de trabalho dos participantes dentro das suas respectivas instituições.....	41
Tabela 8 - Setores de trabalho dos participantes dentro das suas respectivas instituições categorizados.....	43
Tabela 9 - Recursos providos pelas instituições aos seus funcionários.....	63

TABELA DE SIGLAS

Sigla	Significado
VPN	<i>Virtual private network</i>
MDM	<i>Mobile device management</i>
GDRP	<i>General data protection regulation</i>
LGPD	Lei Geral de Proteção de Dados Pessoais
TIC	Tecnologias da informação e da comunicação
IPEA	Instituto de Pesquisa Econômica Aplicada

1. Introdução

1.1 Contexto e motivação

Nos últimos anos o trabalho remoto tem sido adotado por muitas empresas, esse modelo de trabalho vem se popularizando à medida que as tecnologias de informação e comunicação (TICs) foram se difundindo cada vez mais na vida dos cidadãos comuns. Existe muitos benefícios por trás da adoção dessa forma de trabalho, para o lado das empresas e instituições a redução de custos operacionais com os escritórios e transporte de funcionários é um dos motivos para que muitas empresas tenham aderido a esse modelo. De acordo com o ministério da economia durante março de 2020 e junho de 2021, durante a crise sanitária de Covid-19 foi economizado R\$1,419 bilhão aos cofres público, dentre esses custos, a economia com transporte de pessoas foi em torno de R\$ 512,6 milhões, com diárias cerca de R\$ 450,2 milhões e com serviço de energia elétrica foi em torno de R\$ 392,9 milhões [1].

Do lado dos funcionários o trabalho remoto permite a eles economizarem tempo com deslocamento e transporte público, aumentando a produtividade e permitindo uma flexibilidade maior de horários.

De acordo com uma pesquisa realizada pela Alelo, em dezembro, com cerca de 2,7 mil colaboradores, 56% dos profissionais afirmaram adequar melhor suas rotinas no *home office* que no presencial e desses, 75% afirmaram estarem extremamente satisfeitos [2].

O trabalho remoto também possibilita ampliar o leque de talentos que as organizações podem contratar, já que não existe a limitação geográfica, dessa forma os departamentos de pessoas e recursos humanos podem ter uma base de candidatos bem maior aumentando as chances de contratação de mão de obra mais qualificada e especializada.

Vale ressaltar que a adoção do trabalho remoto traz consigo alguns desafios, a distância entre os colaboradores trás uma certa dificuldade para a gestão das pessoas, para isso é imprescindível a implantação de mecanismos e ferramentas que auxiliam a comunicação das pessoas. Para que os colaboradores possam trabalhar distante dos escritórios é importante que haja uma boa infraestrutura de rede e que equipamentos e recursos essenciais como computadores, telefones corporativos, softwares para vídeo conferências, VPN, entre outros sejam providos pelas empresas e instituições onde essas pessoas trabalham.

Segundo uma pesquisa da empresa de consultoria PwC Brasil em parceria com o instituto Locomotiva, foi apontado que cerca de 81% da população com 10 anos ou mais

usam a internet, mas somente 20% têm acesso a uma conexão de qualidade, esse dado corrobora com a questão da dificuldade de acesso a uma infraestrutura de qualidade para se desempenhar o trabalho remoto, já que a internet é um dos recursos mais importante para isso [3].

Com a distância o uso de tecnologias é imprescindível para a execução do trabalho remoto, o uso de computadores, acesso à internet, uso de softwares para comunicação e para o compartilhamento de dados são essenciais para um pleno desenvolvimento do trabalho. O uso dessas tecnologias fora dos escritórios das empresas traz consigo grandes desafios em relação à segurança da informação e privacidade devido a dificuldade de controlar o comportamento das pessoas nos seus ambientes de trabalhos heterogêneos e na gerência mais descentralizada dos recursos providos pelas organizações.

O controle dos ativos e mitigação de eventuais vulnerabilidades para proteção dos dados das empresas são algumas das dimensões básicas para gestão de segurança de informação, hoje em dia o zelo pela integridade, confidencialidade e disponibilidade dos dados têm sido pontos importantes para empresas, principalmente devido às leis de proteção aos dados vigentes pelo mundo, como por exemplo a GDPR (Regulamento Geral Sobre a Proteção de Dados) e a LGPD (Lei Geral de Proteção de Dados Pessoais).

Segundo relatório da Alliance Virtual Offices entre 2020 a 2022 durante o período pandêmico o número de ataques cibernéticos aumentou em 238%, foi durante esse período onde nos últimos anos houve uma alavancada na adoção desse modelo de trabalho [4].

Foi observado pela empresa de cibersegurança ESET que no primeiro semestre de 2022 se observou um crescimento de 226% nos ataques de *phishing*, esse tipo de técnica de ataque explora a vulnerabilidade humana através de engenharia social [5].

Outro dado relevante em relação a engenharia social foi apresentado em um relatório de 2021 da empresa Verizon chamado de “Relatório de Investigação de Violação de Dados 2021”, onde foi identificado que 40% dos crimes cibernéticos praticados em 2020 se utilizavam de técnicas de manipulação psicológica sobre as vítimas.

Nesse contexto se observa a necessidade das empresas investirem em políticas voltadas para a prevenção de incidentes e mitigação de potenciais vulnerabilidades no ambiente de trabalho remoto de seus funcionários, para isso a adoção do uso de ferramentas e tecnologias de proteção como uso de VPNs, antivírus, ferramentas de MDM, criptografia de dispositivos de armazenamento, sistemas de gerenciamento de credenciais, entre outros. são armas de combate contra as ameaças de segurança e proteção da privacidade dos usuários.

Porém antes da adoção de medidas e criação de políticas para assegurar a segurança dos dados e privacidade das pessoas é muito importante entender qual o cenário do ambiente de trabalho dos colaboradores, só a partir daí será possível identificar quais pontos devem ser trabalhados para a promoção de um ambiente de trabalho seguro e respeitando a privacidade dos indivíduos.

1.2 Objetivos

O objetivo deste trabalho é entender qual o cenário atual de segurança da informação e privacidade no trabalho remoto. Para isso será realizado as seguintes etapas:

- Investigar o comportamento, atitudes e conhecimento das pessoas relacionados a segurança e privacidade no trabalho remoto;
- Analisar quais recursos são providos pelas empresas para oferecer um ambiente de trabalho remoto mais seguro;
- Conduzir uma pesquisa *survey* voltada para pessoas que trabalham nos regimes de 100% remoto ou híbrido;
- Analisar os dados coletados para caracterizar o cenário de segurança e privacidade representado pelas informações obtidas na pesquisa.

1.3 Trabalhos Relacionados

Devido às mudanças no contexto atual do trabalho, onde há um avanço constante em direção à maior digitalização e informatização das tarefas e processos nas organizações, os colaboradores tiveram que se adaptar a novas ferramentas e a um modelo de trabalho diferente do tradicional. Essas mudanças trouxeram à tona questões relevantes sobre como ter um controle maior sobre as informações e dados das instituições, bem como sobre como manter a privacidade das pessoas envolvidas nesse contexto.

A cada dia, novos estudos surgem para abordar essas preocupações em constante evolução. Nesta seção, serão apresentados alguns trabalhos que serviram de base para esta análise.

1.3.1 Avaliação da Cultura de Segurança da Informação: A Aplicação de um Survey sobre Cultura de Segurança da Informação nas Organizações

Neste trabalho, foi abordada a relevância de avaliar e aprimorar a cultura de segurança da informação nas organizações, com o objetivo de reduzir os riscos de vazamentos e incidentes relacionados a informações sensíveis e privadas [6].

Através da pesquisa realizada, ficou evidente que o fator humano desempenha um papel central nos incidentes de segurança da informação. A técnica da Engenharia Social, na qual pessoas maliciosas utilizam estratégias para obter informações vitais por meio da conquista da confiança, foi identificada como uma das principais ameaças nesse contexto. É fundamental, portanto, que as organizações desenvolvam uma cultura de segurança forte e disseminada para enfrentar esse desafio.

A cultura de segurança da informação nas organizações é moldada pelos valores, crenças e atitudes dos funcionários e partes interessadas em relação à segurança. Essa cultura é essencial para garantir que as práticas de segurança sejam amplamente adotadas e seguidas dentro da empresa. Além disso, uma cultura de segurança robusta cria uma consciência coletiva sobre a importância da proteção de informações confidenciais, contribuindo para minimizar os riscos associados a comportamentos inseguros.

O trabalho propôs a condução de um survey como ferramenta de avaliação da cultura de segurança da informação nas organizações. O questionário elaborado abrangeu dimensões relevantes propostas na literatura, permitindo coleta dados de funcionários de diversas empresas e setores. Os resultados obtidos revelaram algumas conclusões importantes:

- **Necessidade de Treinamentos em Segurança da Informação:** A maioria dos participantes nunca recebeu treinamentos em segurança da informação e expressou a necessidade de capacitações. Essa lacuna na educação dos funcionários pode comprometer a segurança das organizações, tornando-as mais vulneráveis a incidentes de segurança.
- **Compreensão da Política de Segurança da Informação:** Observou-se que existe uma incongruência entre o conhecimento e a aplicação dos procedimentos descritos na política de segurança da informação. Muitos funcionários conhecem a política, mas têm dificuldades em aplicá-la corretamente em suas atividades diárias.

- **Importância da Sensibilização:** A pesquisa evidenciou a necessidade de campanhas de conscientização e sensibilização em segurança da informação, pois mesmo que os funcionários possuam algum conhecimento sobre o tema, ainda há espaço para melhorias no entendimento e adoção de práticas seguras.
- **Aceitação de Mudanças:** De forma encorajadora, a maioria dos participantes mostrou-se aberta a mudanças de comportamento no ambiente de trabalho para contribuir com a segurança dos ativos de informação da organização. Essa atitude positiva pode ser explorada para implementar melhorias efetivas.

As contribuições deste trabalho incluem uma investigação de métodos de avaliação da cultura de segurança da informação, a elaboração de um questionário abrangente e a aplicação desse instrumento para obter uma visão abrangente da cultura de segurança nas organizações. Para trabalhos futuros, sugere-se ampliar a pesquisa para obter mais respostas e uma avaliação mais abrangente. Além disso, entrevistas com funcionários e estudos de caso podem enriquecer a compreensão dos aspectos culturais de segurança da informação em diferentes contextos organizacionais.

No geral, este trabalho destacou a importância crucial de uma cultura de segurança da informação sólida nas organizações para mitigar os riscos de vazamentos e incidentes. Os resultados obtidos podem ser utilizados como base para implementar ações que aprimorem as práticas de segurança da informação e contribuam para a proteção eficaz dos dados e informações sensíveis, resguardando a integridade e a reputação das organizações [6].

1.3.2 Working from home during COVID-19 crisis: a cyber security culture assessment survey

O artigo aborda a importância da cultura de cibersegurança durante a pandemia da COVID-19, com foco no trabalho remoto. Foi desenvolvido um framework para avaliar a cultura de segurança em organizações, considerando a influência de fatores variados em diferentes níveis organizacionais e individuais. A cultura de segurança é moldada pela conscientização e prontidão em segurança, adaptando-se ao longo do tempo e das mudanças [7].

Os resultados da pesquisa mostram que as organizações e indivíduos apresentam variações significativas na segurança da informação, indicando que ainda há um longo caminho para que a cibersegurança se torne uma parte inquebrável das operações comerciais e da realidade da força de trabalho. À medida que as organizações se descentralizam e adotam o trabalho remoto, é fundamental que a cultura de segurança evolua e se ajuste, fornecendo políticas, procedimentos e medidas adequadas à nova realidade.

A conscientização, familiaridade e expertise dos funcionários em questões de segurança são essenciais e devem ser incentivadas por meio de treinamentos contínuos e participação ativa em simulações de segurança. O cibercrime está em constante evolução, explorando oportunidades ao longo do tempo e espaço, exigindo que a cultura de cibersegurança acompanhe esse ritmo.

A pesquisa destaca algumas surpresas, como a quantidade significativa de funcionários incapazes de trabalhar remotamente, a falta de mecanismos de colaboração em teletrabalho, e a existência de ativos de hardware desprotegidos. Também é preocupante que muitos participantes não tenham recebido orientações de segurança adequadas de seus empregadores durante a crise.

A conclusão destaca a importância de focar em ajustes de segurança para diferentes setores e empresas, à medida que o trabalho remoto se torna uma necessidade atual. Além disso, é essencial enfatizar as características individuais de segurança, como comportamento, atitude, conscientização e conformidade, e pesquisar para quantificar esses indicadores de forma a obter uma abordagem cultural confiável em relação à cibersegurança. O fator humano é fundamental para o progresso da segurança da informação e ainda permanece pouco explorado [7].

1.3.3 Análise das dimensões dos trabalhos

Nesta seção será apresentado uma comparação entre os trabalhos relacionados e este trabalho, a tabela 1 apresenta algumas das principais diferenças.

Tabela 1 - Comparação entre os trabalhos relacionados e o trabalho proposto.			
Critérios	SANTOS (2020)	GEORGIADOU, MOUZAKITIS e ASKOUNIS (2021)	Trabalho Proposto
Metodologia utilizada	Pesquisa survey.	Pesquisa survey.	Pesquisa survey.
Instrumento de coleta dos dados	Questionário.	Questionário.	Questionário.
Público-alvo	Funcionários de instituições públicas e privadas no geral.	Funcionários que trabalhavam em empresas europeias de diferentes setores críticos afetadas pela pandemia.	Funcionários que trabalhavam remotamente no regime 100% remoto ou híbrido.
Tipos de dados coletados	Opiniões sobre engajamento, confiança e conhecimento relativos a engenharia social e cultura de segurança da informação.	Dados sobre incidentes de segurança, medidas adotadas, uso de recursos providos pelas empresas e opiniões de satisfação referentes ao trabalho remoto.	Dados sobre os recursos providos pelas empresas, análise sobre conhecimento e importância sobre o uso de determinados recursos e boas práticas e dados sobre o comportamento dos funcionários em seu ambiente doméstico durante o trabalho remoto.
Conclusões	Incongruências entre conhecer, saber e aplicar algumas medidas de segurança. E a existência de uma necessidade de promover medidas para engajar as pessoas numa cultura de segurança da informação.	Falhas na gestão de políticas de segurança da informação. Foram verificados muitos ativos desprotegidos. Há uma necessidade de capacitação contínua dos funcionários. Muitos trabalhadores não tinham uma estrutura mínima para	Um cenário relativamente positivo na adoção de medidas de segurança e na provisão de recursos pelas organizações aos seus funcionários. Foi verificada uma lacuna na privacidade dos funcionários,

		trabalhar remotamente.	principalmente no ambiente doméstico. Verificou-se também uma necessidade das empresas investirem em treinamentos específicos para um trabalho remoto mais seguro assegurando a privacidade dos seus funcionários.
Tema focal	Avaliação da cultura de segurança da informação.	Avaliação da cultura de segurança da informação.	Avaliação da cultura de segurança da informação.
Contexto	Começo da pandemia de Covid-19.	Começo da pandemia de Covid-19.	Final do período da pandemia de Covid-19.
Ano de publicação da pesquisa	2020	2021	2023
Período da coleta dos dados	Junho de 2020 até setembro de 2020.	Abril de 2020 até maio de 2020.	Setembro de 2022 até Setembro de 2023.
Tamanho da amostra coletada	110	264	240

Fonte: Elaborada pelo autor (2023).

1.4 Estrutura do documento

Este trabalho foi elaborado utilizando a metodologia de pesquisa de survey, e sua estrutura está dividida em quatro partes, cada uma composta por uma seção, são elas: Seção 2 contém a revisão da literatura onde temas relacionados à pesquisa são abordados e trabalhos que serviram de inspiração para ela; a Seção 3 aborda o método utilizado para elaboração da pesquisa, elencando cada passo e seus respectivos objetivos; a Seção 4 apresenta os resultados obtidos nas pesquisas e as análises gerais; na Seção 5 são discutidas as conclusões sobre a pesquisa, contribuições do trabalho e sugestões para trabalho futuros.

2. Revisão da Literatura

Este capítulo é dividido em cinco seções, nelas são abordados alguns conceitos diretamente relacionados ao tema deste trabalho. A seção 2.1 conceitua e contextualiza o modelo de teletrabalho; a seção 2.2 aborda o tema do uso de dispositivos pessoais para trabalho; a seção 2.3 aborda os desafios da segurança da informação e privacidade no contexto de teletrabalho; a seção 2.4 discorre sobre leis de proteção de dados e como elas impactam empresas e pessoas; finalmente a seção 2.5 aborda sobre o tema de engenharia social conceituando e contextualizando para o ambiente de teletrabalho.

2.1 Teletrabalho

O teletrabalho, também conhecido como trabalho remoto, é uma prática que permite aos funcionários trabalhar fora do escritório de suas empresas, usando a tecnologia para se comunicar e colaborar com a equipe [8]. A consolidação do conceito de teletrabalho remonta à década de 1970 [9], quando empresas começaram a experimentar essa modalidade como uma forma de reduzir custos com escritórios e aumentar a produtividade dos funcionários.

Inicialmente, o teletrabalho era utilizado principalmente por profissionais autônomos e freelancers, que trabalhavam em casa ou em espaços de *coworking* [10]. No entanto, com o tempo, muitas empresas passaram a adotar essa prática como uma forma de oferecer mais flexibilidade aos seus funcionários e reduzir custos operacionais.

Uma das primeiras empresas a adotar o teletrabalho foi a IBM, a partir dos anos de 1980 [11]. A empresa iniciou um programa piloto em que alguns funcionários trabalhavam de casa ao invés de ir ao escritório. O programa foi um sucesso e, em pouco tempo, a IBM expandiu o teletrabalho para outros funcionários ao redor mundo. Outra empresa que se destacou na adoção do teletrabalho foi a Xerox. Na década de 80, a empresa implementou um programa chamado *Telecommuting*, que permitia que os funcionários trabalhassem em casa um ou dois dias por semana [12]. A medida reduziu os custos da empresa com escritórios e também aumentou a satisfação e produtividade dos funcionários.

Ao longo dos anos, o teletrabalho se tornou cada vez mais comum em empresas de todo o mundo. Com o surgimento da internet e da tecnologia móvel, tornou-se ainda mais fácil para os funcionários trabalharem fora do escritório. Atualmente, o teletrabalho é amplamente adotado em diversos setores, como o de tecnologia, finanças, marketing, entre

outros. No entanto, apesar dos benefícios do teletrabalho, há também desafios e preocupações relacionadas à saúde mental dos funcionários, à privacidade e segurança dos dados, provisão de infraestrutura, gestão de pessoas, entre outros [13]. É importante que as empresas adotem políticas claras e eficazes para garantir o sucesso do teletrabalho e o bem-estar dos seus funcionários também.

Outro modelo de trabalho é o regime híbrido, ele é uma forma de trabalho que combina características do modelo remoto com o presencial [14]. Com a popularidade crescente do trabalho remoto, muitas empresas estão adotando esse modelo como uma forma de permitir que seus funcionários trabalhem de casa parte do tempo, enquanto ainda colaboram presencialmente com colegas de trabalho em outros momentos.

A origem do teletrabalho está ligada a diversos fatores, incluindo a tecnologia, a globalização e a evolução das relações de trabalho. No entanto, foi a pandemia do Covid-19 que impulsionou sua adoção em larga escala nos últimos anos, tornando-o uma forma de trabalho essencial para muitas empresas [15]. Antes da pandemia, o trabalho remoto era uma opção limitada para muitos trabalhadores, restrito a trabalhadores autônomos, profissionais de tecnologia e algumas profissões específicas. Com a chegada da pandemia, o trabalho remoto se tornou uma necessidade para muitas empresas, a fim de manter seus negócios em funcionamento e garantir a segurança de seus funcionários. A pandemia forçou empresas de todos os setores a repensar suas estratégias de trabalho e adotar novas formas de colaboração, comunicação e trabalho em equipe.

Segue abaixo alguns dados relevantes sobre o teletrabalho na pandemia de covid-19:

- De acordo com uma pesquisa realizada pela Fundação Instituto de Administração (FIA), em parceria com a Fundação Oswaldo Cruz (Fiocruz), 46% dos trabalhadores brasileiros passaram a atuar em regime de home office durante a pandemia de covid-19 [16].
- Segundo dados da NordVPN de 2020, os trabalhadores estenderam em média mais duas horas na sua carga horária diária de trabalho durante a pandemia trabalhando de *home office* [17].
- De acordo com um 6ª edição da pesquisa “Covid-19: como será o seu retorno ao escritório” realizada pela empresa de consultoria KPMG no Brasil, entre julho e

agosto de 2021 com participação de 287 empresas, 85% das empresas devem retomar suas atividades pós-pandemia em modelo híbrido [18].

- Uma pesquisa feita pelo LinkedIn entre 21 de janeiro de a 8 de fevereiro de 2022 revelou que 78% dos trabalhadores perceberam durante o período de pandemia que precisam e querem trabalhar de uma forma mais flexível mesmo após a pandemia influenciados pela experiência do teletrabalho durante o período de isolamento social [19].

Para que tanto o trabalho totalmente remoto seja viável, as empresas precisam atender alguns requisitos minimamente, como por exemplo: fornecer equipamentos adequados para o trabalho remoto ou promover meios para que seus funcionários utilizem seus próprios dispositivos para trabalho [8], implementar mecanismos de segurança dos dados e assegurar a privacidade dos funcionários, promover meios para uma comunicação efetiva entre os líderes e liderados para que as tarefas sejam bem gerenciadas entre empresa e seu clientes.

A pandemia de Covid-19 foi um marco importante para a consolidação do teletrabalho como uma realidade do mundo contemporâneo, impulsionando a adoção de novas tecnologias e novas formas de organização do trabalho. Apesar de ter sido uma alternativa importante para manter as atividades em meio à crise sanitária, o teletrabalho também trouxe desafios para empresas e trabalhadores, principalmente no que diz respeito à segurança e proteção de dados.

2.2 Uso de dispositivos pessoais no trabalho - Byod

Nos últimos anos, a tendência de permitir que os funcionários usem seus próprios dispositivos eletrônicos para realizar seu trabalho, esse conceito é conhecido como BYOD (*Bring Your Own Device*), termo em inglês que significa “Traga seu próprio dispositivo” [20]. Essa tendência se tornou ainda mais relevante com o aumento do teletrabalho.

A adoção do BYOD em empresas que adotam o teletrabalho pode oferecer muitos benefícios para os funcionários [21]. Com o BYOD, os funcionários podem usar seus próprios dispositivos, o que significa que têm mais controle sobre o tipo de tecnologia que usam e como a usam para realizar seu trabalho. Isso pode resultar em maior produtividade e satisfação no trabalho, pois os funcionários podem usar as ferramentas com as quais estão mais familiarizados.

O BYOD também pode permitir que os funcionários trabalhem em qualquer lugar, a qualquer hora. Isso é particularmente útil para funcionários que trabalham remotamente e precisam acessar sistemas e informações da empresa fora do escritório.

No entanto, esse conceito também apresenta riscos de segurança [22]. Se um dispositivo pessoal for comprometido por um hacker, por um vírus ou até mesmo sendo roubado, informações confidenciais da empresa podem ser expostas. Além disso, se um funcionário sair da empresa e ainda tiver acesso a informações confidenciais da empresa em seu dispositivo pessoal, isso pode representar um risco de segurança significativo. Um outro grande desafio relacionado a BYOD é a gestão de dispositivos. Com o uso de dispositivos pessoais, pode ser difícil para as empresas manter o controle sobre os dispositivos e aplicar políticas de segurança consistentes em todos os dispositivos usados pelos funcionários.

Por esses motivos, é importante que as empresas implementem políticas rigorosas de segurança quando adotar o BYOD [23]. Isso pode incluir a instalação de software de segurança, a exigência de senhas complexas e atualizações frequentes de software. As empresas também podem monitorar os dispositivos usados pelos funcionários para garantir que apenas dispositivos seguros e atualizados sejam usados para acessar os sistemas corporativos.

Outro aspecto importante a ser considerado é a compatibilidade de dispositivos e sistemas [24]. Nem todos os dispositivos pessoais podem ser compatíveis com os sistemas da empresa, o que pode levar a problemas de acesso e produtividade. Portanto, as empresas devem estabelecer uma lista de dispositivos aprovados e garantir que os funcionários estejam cientes das restrições e limitações do uso de dispositivos pessoais.

Por esse motivo, muitas empresas optam por utilizar soluções de MDM (*Mobile Device Management*), que permitem que as empresas gerenciem e monitorem remotamente os dispositivos móveis usados pelos funcionários. Com uma solução MDM, as empresas podem garantir que seus funcionários estejam usando dispositivos seguros e atualizados e podem aplicar políticas de segurança consistentes em todos os dispositivos [23].

Além disso, essa solução pode permitir que as empresas rastreiem os dispositivos e apaguem remotamente dados confidenciais em caso de perda ou roubo de dispositivo. Isso pode ajudar a minimizar o risco de perda ou vazamento de informações confidenciais da empresa.

No geral, o BYOD pode oferecer muitos benefícios para as empresas que adotam o teletrabalho, mas também apresenta desafios em relação à segurança, gestão de dispositivos e

o aspecto da privacidade do funcionário, já que ele utiliza um dispositivo pessoal para trabalho.

2.3 Segurança da Informação e Privacidade no trabalho remoto

Segurança da Informação e privacidade são conceitos próximos porém não são iguais, a segurança da informação é responsável por proteger os dados se utilizando de artifícios técnicos, utilizando ferramentas e aplicando regras preestabelecidas com a finalidade de manter todos os dados seguros em posse do seu tutor. A segurança da informação é baseada em cinco pilares, são eles: confiabilidade, disponibilidade, integridade, autenticidade e irretrabilidade. Já a privacidade dos dados está diretamente relacionada às diretrizes de como esses dados em posse de seus tutores possam ser manipulados e ou compartilhados para que eles não caiam na mão de terceiros não autorizados [25].

Esses temas são questões críticas que afetam as empresas que adotam o teletrabalho. Com a crescente adoção desse regime de trabalho, muitas empresas estão enfrentando novos desafios de segurança e privacidade que precisam ser abordados para garantir a proteção adequada dos dados da empresa e dos funcionários.

Uma das principais preocupações relacionadas à segurança da informação no teletrabalho é a possibilidade de ataques cibernéticos. Os funcionários que trabalham remotamente, muitas vezes, estão usando dispositivos pessoais conectados eventualmente conectados a redes públicas, o que pode aumentar o risco de ataques de hackers. Nesse contexto, as empresas precisam determinar que seus funcionários utilizem antivírus, VPNs (*Virtual Private Network*), e sigam as políticas e boas práticas para o uso seguro dos seus equipamentos de trabalho [23].

Outro problema de segurança é a possibilidade de acesso não autorizado aos dados da empresa. Com o teletrabalho, os funcionários podem acessar os dados da empresa em seus próprios dispositivos pessoais ou em computadores compartilhados, o que pode aumentar o risco de violações de segurança. Para minimizar esse risco, as empresas devem adotar políticas de controle de acesso e utilizar soluções de segurança de dados, como criptografia de dados e soluções de gerenciamento de acesso.

De acordo com uma pesquisa realizada pela empresa de segurança cibernética Kaspersky em 2020, 67% dos funcionários brasileiros entrevistados pela empresa não

receberam treinamento e instruções de boas práticas de cibersegurança para trabalharem remotamente protegidos [26].

Uma análise feita pela empresa de segurança Check Point Software Technologies apontou que no primeiro ano da pandemia durante a migração das empresas para o regime de teletrabalho houve um aumento de 50% nos ataques cibernéticos sofisticados, isso devido a grande quantidade de dispositivos e redes diferentes geradas pela demanda dos funcionários para trabalharem de casa. Com esse cenário o gerenciamento segmentado de cada dispositivo em lugares diferentes com pessoas diferentes trouxe um grande desafio para as empresas em relação a gerenciamento e rastreabilidade deles, na mesma pesquisa é citado que ao menos 46% das empresas conseguiram monitorar aplicativos e programas maliciosos baixados pelos seus funcionários nos seus respectivos dispositivos de trabalho [27].

Esses dados destacam a necessidade urgente de as empresas garantirem a segurança e privacidade dos dados de seus funcionários durante o teletrabalho. As empresas precisam estar vigilantes em relação a ameaças cibernéticas e garantir que seus funcionários tenham acesso a treinamento de segurança de dados e soluções de segurança confiáveis sempre respeitando as normas e leis que regem a segurança e privacidade dos dados tanto dos funcionários quanto das próprias empresas e instituições afins.

2.4 Leis de proteção de dados

Com a convergência de muitos serviços para internet, sejam sites de vendas, aplicativos de transportes, redes sociais e aplicativos de pagamentos, entre outros, as pessoas cada vez mais vem expondo e oferecendo seus dados para muitas empresas, que por muitas vezes utilizam dessas informações como uma mercadoria [28]. É importante que as pessoas analisem bem essas instituições as quais elas irão fornecer seus dados, além disso ler os termos e condições referente a essa ação é de extrema importância para resguardar a privacidade dos usuários. A privacidade e proteção desses dados são direitos fundamentais dos indivíduos [29]. Por esse motivo, muitos países têm leis específicas que regem a proteção de dados pessoais.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em setembro de 2020, é a principal legislação que regula a proteção de dados pessoais [30]. Ela estabelece regras para o tratamento de dados pessoais, como a necessidade de consentimento explícito do titular dos dados para o seu uso, a obrigação de informar ao titular

sobre o uso dos seus dados e a garantia de segurança dessas informações. A LGPD também define as penalidades em caso de descumprimento da lei, que podem variar de advertências a multas de até 2% do faturamento da empresa, limitadas a R\$50 milhões por infração.

Além da LGPD, outras leis e regulamentações também podem afetar a proteção de dados dos brasileiros, como o Marco Civil da Internet [31] e o Código de Defesa do Consumidor [32].

No âmbito internacional, a *General Data Protection Regulation* (GDPR) da União Europeia é uma das leis mais abrangentes sobre a proteção de dados pessoais. Ela estabelece diretrizes para a coleta, armazenamento e uso de informações pessoais por empresas e organizações que operam na União Europeia. A GDPR também estabelece multas significativas em caso de violação da lei, que podem chegar a 4% do faturamento global da empresa [33].

A proteção de dados pessoais também é uma preocupação importante no contexto do trabalho remoto [22]. Com mais pessoas trabalhando em casa e usando dispositivos pessoais para acessar informações corporativas, há um aumento no risco de violação de dados e invasões de privacidade.

Nesse contexto, as empresas que adotam o trabalho remoto devem garantir que seus colaboradores sigam as políticas de proteção de dados e de segurança da informação, incluindo [23] o uso de senhas seguras, a criptografia de dados, a proteção de dispositivos móveis e a utilização de redes virtuais privadas (VPNs) para acessar informações corporativas de forma segura. As empresas também devem orientar seus colaboradores sobre as políticas de privacidade e proteção de dados pessoais, garantindo que todas as informações coletadas dos funcionários sejam utilizadas de acordo com as leis e regulamentações aplicáveis.

Portanto, é fundamental que as empresas que adotam o trabalho remoto estejam cientes das leis de proteção de dados e das suas responsabilidades em relação à proteção da privacidade e segurança das informações pessoais de seus colaboradores. O tema da proteção de dados pessoais é uma preocupação cada vez mais presente nas empresas, não só no contexto do trabalho remoto, mas em qualquer atividade que envolva o tratamento de informações pessoais [29].

2.5 Engenharia social

A engenharia social é uma prática que busca manipular pessoas a fim de obter informações ou realizar ações que possam comprometer a segurança das informações [34]. Esse tipo de prática foi amplamente adotada por cibercriminosos para coletar dados e informações sigilosas, como senhas, credenciais e dados pessoais dos usuários, durante a pandemia [35].

Um exemplo de técnica de ataque engenharia social é o *phishing* [36], que consiste em enviar mensagens falsas por e-mail ou outras formas de comunicação eletrônica para induzir o usuário a clicar em algum link malicioso ou fornecer informações sensíveis, como senhas ou dados bancários além da possibilidade de instalações de vírus como *malwares* e *spywares* nos dispositivos dos usuários. Com a adoção do teletrabalho, muitas empresas têm recorrido a ferramentas de comunicação eletrônica, como e-mails e aplicativos de mensagens, o que pode aumentar a exposição dos colaboradores a esse tipo de prática.

Para evitar esse tipo de ataque, as empresas devem adotar medidas de segurança, como a utilização de filtros de email *anti-spam*, uso de antivírus e *firewalls* em computadores e dispositivos móveis, a realização de treinamentos para conscientização dos colaboradores e a adoção de políticas de segurança da informação, que orientem sobre a conduta a ser adotada no tratamento das informações [37].

A engenharia social é uma das principais ameaças de segurança da informação atualmente e tem sido bastante explorada pelos cibercriminosos em diferentes contextos. Segundo um relatório da empresa de segurança digital Kaspersky [38], o phishing (que é uma forma de engenharia social) foi responsável por mais da metade dos ataques de *malware* em 2020. Além disso, a pandemia do COVID-19 foi um tema muito explorado pelos criminosos em suas campanhas de phishing, aproveitando-se do contexto de incertezas e medo das pessoas para obter informações sensíveis.

Outro dado relevante da empresa de segurança cibernética Proofpoint apontou que os ataques de phishing aumentaram em 350% durante a pandemia do COVID-19, sendo que os setores de educação, saúde e varejo foram os mais afetados [39].

Por isso, é fundamental que as empresas adotem medidas de segurança para prevenir esses tipos de ataques usando ferramentas adequadas e disseminando o conhecimento para seus funcionários já que um dos elos mais fracos da segurança da informação são as pessoas. No lado dos colaboradores eles devem estar atentos a possíveis tentativas de engenharia social

e adotar medidas de precaução, como verificar a veracidade das informações antes de clicar em links ou fornecer informações sensíveis [34].

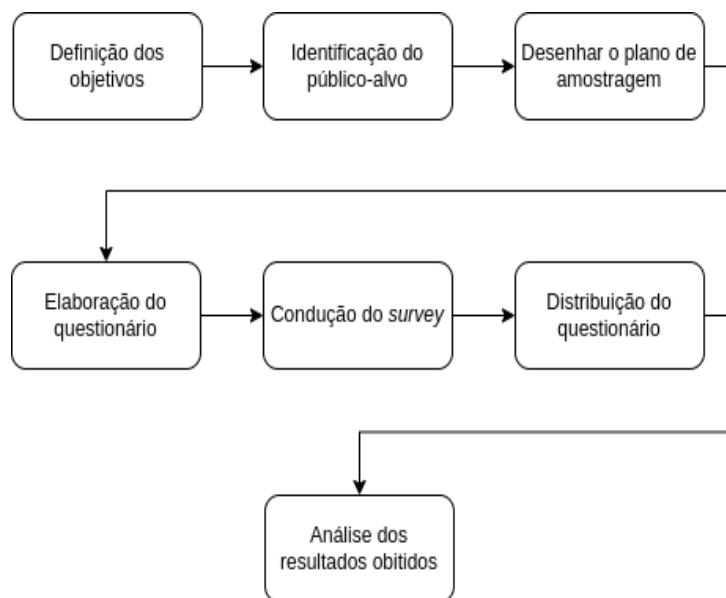
A engenharia social é uma ameaça real e presente no contexto do teletrabalho e as organizações devem ter um cuidado maior sobre os seus funcionários, pois não basta serem implementadas só as ferramentas adequadas para mitigar eventuais problemas, a prevenção nesse caso começa pela conscientização das pessoas.

3. Metodologia

Este capítulo aborda a metodologia utilizada no desenvolvimento da pesquisa *survey* que é a base para a coleta dos dados analisados neste trabalho. Como característica geral este tipo de pesquisa tem como objetivo coletar informações sobre um determinado grupo ou público alvo captando as suas opiniões, atitudes, dados demográficos e também comportamentais, permitindo que o pesquisador extraia *insights* e desenvolva suas próprias conclusões sobre o tópico da pesquisa.

Como referência para o desenvolvimento do *survey* foi utilizado os métodos descritos no trabalho de Kasunic em 2005 [40]. De acordo com o autor, uma pesquisa *survey* é composta por sete etapas bem definidas são elas: Definição dos objetivos da pesquisa, identificação e características do público-alvo, desenhar o plano de amostragem, elaboração do questionário, condução do teste piloto, distribuição do questionário e análise do resultados.

Figura 1 - Fluxograma da metodologia da pesquisa *survey*.



Fonte: Adaptado do trabalho *Designing an Effective Survey* de autoria do Mark Kasunic (2005).

São características destes tipo de metodologia ser sistemático, imparcial, ser representativo, ter uma base teórica para fundamentação, ser quantitativo para uma análise

uniforme dos dados e replicável para certificar que pelo mesmo método e mesmo meio será obtido os mesmos resultados.

É importante salientar que uma pesquisa *survey* não é simplesmente um questionário, o questionário só é o meio pelo qual se coletam as informações pois a pesquisa é caracterizada por todo processo de desenvolvimento através das etapas elencadas anteriormente. As etapas do desenvolvimento da pesquisa *survey* serão abordadas nas próximas seções.

3.1 Definição dos objetivos da pesquisa

Com o propósito de cumprir os objetivos desta fase da pesquisa, uma revisão de literatura foi conduzida, abrangendo trabalhos que tratam da segurança da informação e da privacidade no contexto do teletrabalho. Para essa revisão, foram consultadas fontes de estudo como artigos acadêmicos, revistas especializadas, trabalhos de graduação, livros e periódicos.

A revisão de literatura auxiliou na contextualização dos objetivos da pesquisa, proporcionando um embasamento sólido ao explorar estudos relacionados ao tema. Isso permitiu delinear com maior clareza a abordagem da pesquisa e as questões que serão abordadas ao longo do estudo.

O objetivo deste trabalho é entender qual o cenário atual de segurança da informação e privacidade no trabalho remoto a partir da análise do comportamento e conhecimento dos participantes referentes ao tema da pesquisa além da verificação dos recursos providos pelas organizações para seus colaboradores com o objetivo de prover um ambiente de teletrabalho seguro para os dados das partes.

3.2 Identificação de características do público-alvo

A pesquisa *survey* realizada neste trabalho foi voltada para trabalhadores engajados em modelos de teletrabalho, sejam eles em regime 100% remoto ou híbrido, é crucial compreender de maneira abrangente as características específicas desse público-alvo. Essa compreensão detalhada desempenha um papel fundamental na formulação de perguntas pertinentes, na orquestração eficaz da coleta de dados e na interpretação significativa dos resultados [40].

- **Características Demográficas e Profissionais:** A identificação do público-alvo deve considerar tanto as características demográficas, como idade, grau de instrução, área de formação, área de atuação no trabalho, tempo de trabalho na empresa, entre outros. Aspectos esses que podem ser levados em consideração na análise sobre distintos resultados para perfis diferentes de participantes.
- **Comportamentos dos trabalhadores relacionados à Segurança da Informação:** A compreensão dos comportamentos dos trabalhadores em relação à segurança da informação é de extrema importância. Perguntas que explorem a adoção de medidas de segurança cibernética, o manuseio de informações confidenciais e a conscientização sobre ameaças cibernéticas podem fornecer insights valiosos sobre a postura dos trabalhadores em relação à proteção de dados.
- **Atitudes em Relação à Privacidade e Segurança:** Investigar as atitudes e a conscientização dos trabalhadores em relação à privacidade e segurança online é fundamental. Questões que abordem o conhecimento sobre políticas de privacidade, percepções sobre riscos cibernéticos e níveis de confiança nas práticas de segurança da organização podem oferecer insights sobre os pontos fortes e fracos da cultura de segurança.
- **Desafios de Segurança e Necessidades Específicas:** Entender os desafios específicos que os trabalhadores enfrentam em relação à segurança da informação é crucial para a eficácia da pesquisa. Questões que explorem preocupações com o vazamento de dados, a vulnerabilidade de dispositivos pessoais e as barreiras para a implementação de boas práticas de segurança podem oferecer insights valiosos sobre as necessidades desse público.
- **Impacto nos Modelos de Teletrabalho e Segurança:** Direcionar a pesquisa para questões de segurança da informação no contexto de modelos de teletrabalho permite entender como esses modelos afetam a postura dos trabalhadores em relação à proteção de dados. Questões que investigam a influência do teletrabalho na aderência a políticas de segurança e na conscientização sobre ameaças cibernéticas podem fornecer *insights* sobre a eficácia das medidas de segurança implementadas.

A identificação e a análise das características do público-alvo em pesquisas survey voltadas para trabalhadores em modelos de teletrabalho, considerando a segurança da informação e a privacidade, são cruciais para obter *insights* pertinentes e direcionados. Esses *insights* não apenas enriquecem a pesquisa, mas também podem guiar estratégias de segurança e políticas que atendam às necessidades específicas desse grupo, assegurando um ambiente de trabalho remoto mais seguro tanto para o funcionário quanto para a empresa.

3.3 Definição do plano de amostragem

Um plano de amostragem em uma pesquisa é uma etapa onde se estabelece de forma detalhada como uma amostra de dados será coletada a partir de uma população maior. Ele descreve quem será incluído na amostra, qual o tamanho da amostra, como os elementos da amostra serão selecionados, como os dados serão coletados, e como os resultados da amostra serão interpretados e aplicados à população maior.

Este plano é fundamental para garantir que os resultados da pesquisa sejam confiáveis e representativos da população-alvo. A escolha adequada do tamanho da amostra e do método de seleção ajuda a minimizar o viés e a aleatoriedade nos dados coletados. Além disso, o plano de amostragem define os procedimentos que garantem a precisão na coleta de dados e a validação das conclusões tiradas a partir da amostra.

O plano de amostragem é uma parte essencial de qualquer pesquisa, pois assegura que os resultados sejam significativos e úteis para fazer inferências sobre a população sem a necessidade de estudar todos os seus elementos.

Para este trabalho foi utilizado uma amostra não probabilística de dados, isso significa que os elementos ou participantes da população de interesse não têm uma chance conhecida e igual de serem escolhidos para fazer parte da amostra [42]. Nesse tipo de amostragem, a seleção dos elementos da amostra não é aleatória e, portanto, não pode ser quantificada de forma precisa em termos de probabilidade. A escolha desse tipo de amostragem se deu ao fato de não haver um controle estatístico na coleta dos dados para uma representação universal devido ao modelo de pesquisa onde o questionário foi auto preenchido pelos seus participantes e de forma voluntária e espontânea.

3.4 Elaboração do questionário

A etapa de elaboração do questionário em uma pesquisa de levantamento é uma fase crítica do processo. Nesse estágio, os pesquisadores projetam as perguntas e a estrutura que guiarão a coleta de dados com os participantes. Esta etapa é vital para garantir que os resultados sejam confiáveis, precisos e úteis para alcançar os objetivos da pesquisa. Para uma boa elaboração do questionário deve-se ter atenção a alguns pontos essenciais, são eles:

- Definir bem os objetivos da pesquisa, para isso é importante estudar e ter uma análise prévia sobre o tema abordado na pesquisa.
- Planejar a estrutura do questionário para que o fluxo das perguntas siga de uma maneira lógica.
- Escolher quais serão os tipos de pergunta, se serão abertas, fechadas, perguntas demográficas, escalas de avaliação, entre outras.
- Elaborar perguntas claras e mais simples possível para evitar interpretações dúbias.
- Ter uma atenção ao tempo estimado necessário para responder o questionário, pois questionários muito extensos sobrecarregam os participantes e desestimulam a participação deles.

O questionário da pesquisa sobre segurança da informação e privacidade de dados no teletrabalho foi elaborado com base em estudos da literatura, incorporando pesquisas já existentes relacionadas ao tema. As perguntas foram cuidadosamente organizadas no questionário, dando prioridade aos tópicos mais relevantes e importantes. Isso assegura que a pesquisa aborda de forma abrangente os desafios críticos relacionados à segurança da informação e à privacidade dos dados no ambiente de teletrabalho. A abordagem metodológica sólida visa fornecer resultados precisos e valiosos para esse contexto em constante evolução.

O questionário da pesquisa foi inspirado nos questionários dos seguintes trabalhos: “Avaliação da Cultura de Segurança da Informação: A Aplicação de um Survey sobre Cultura de Segurança da Informação nas Organizações” (2020) [6] e o “*Working from home during COVID-19*” (2022) [7]. A estrutura do questionário foi dividida em três seções, onde a primeira foi um termo de consentimento para a participação na pesquisa de forma anônima e

nele continha todas as informações sobre as condições para a participação na pesquisa; a segunda seção continha as perguntas relacionadas ao perfil do participante e a terceira seção era composta por perguntas sobre o conhecimento, opiniões e atitudes dos participantes relacionados ao tema da pesquisa.

A composição das perguntas do questionário foi a seguinte:

- 12 perguntas sobre o perfil do participante, fechadas de múltipla escolha, onde tinham perguntas relacionadas a faixa etária, área de atuação no trabalho, grau de formação, entre outras;
- 20 perguntas sobre conhecimento, atitudes e opiniões dos participantes relacionados a tópicos referentes ao tema da pesquisa, onde dessas perguntas 16 foram de múltiplas escolhas fechadas, 2 perguntas do tipo matriz e outras 2 abertas complementares.
- Por último uma pergunta aberta sobre a opinião dos participantes referente ao questionário e ao tema da pesquisa.

3.5 Condução do teste piloto

A condução de um teste piloto em uma pesquisa survey é uma etapa essencial que envolve a coleta de respostas de uma pequena amostra da população-alvo antes da pesquisa em larga escala. No caso deste estudo, foi realizado um teste piloto com 6 participantes voluntários, dos quais um deles era um especialista na área de segurança da informação, atuando como gerente de equipe de segurança da informação em uma empresa de tecnologia. Os outros participantes eram de áreas distintas, mas também trabalhavam em empresas de tecnologia.

Esse grupo diversificado de participantes foi cuidadosamente selecionado para refletir diferentes perspectivas e conhecimentos relevantes. Mais do que isso, para assegurar a qualidade do questionário, foram conduzidas várias rodadas de testes, resultando em um total de 4 versões diferentes do questionário. A última versão refinada por meio dessas iterações foi a que acabou sendo aplicada em massa (Visualizar no apêndice B).

Esse processo de teste piloto minucioso foi fundamental para identificar problemas, avaliar a clareza das perguntas e a eficácia da metodologia de coleta de dados. A expertise do especialista em segurança da informação também ajudou a garantir que as questões relacionadas a esse campo fossem precisas e relevantes. Ao investir tempo e recursos nesse

teste piloto, a pesquisa de levantamento foi capaz de aperfeiçoar seu questionário e fornecer resultados mais confiáveis e valiosos no final.

3.6 Distribuição do questionário

A etapa de distribuição do questionário requer uma atenção especial em relação à estratégia utilizada para captar o máximo de dados representativos para a pesquisa. É o ponto em que os pesquisadores fazem contato direto ou indiretamente com os participantes com o intuito de coletar as respostas necessárias para a pesquisa. Esta fase pode assumir diversas formas, dependendo da metodologia escolhida, incluindo questionários impressos, pesquisas online, entrevistas por telefone ou pessoalmente, para esse trabalho a pesquisa foi realizada através de um formulário online.

O questionário foi distribuído de maneira abrangente, utilizando múltiplos canais de comunicação. Isso incluiu o envio através de listas de e-mail, como a lista de e-mail dos alunos de graduação e pós-graduação do Centro de Informática da UFPE. Além disso, o questionário foi compartilhado em grupos de WhatsApp e Telegram, bem como enviado diretamente para algumas pessoas através do Telegram e foi publicado em grupos do Facebook e LinkedIn. Foi incentivado aos participantes voluntários que compartilhassem o questionário com outras pessoas, ampliando ainda mais seu alcance.

Vale salientar que a ferramenta utilizada para criar e distribuir o questionário foi o Google Forms. Essa plataforma online permitiu uma coleta eficaz e organizada das respostas dos participantes. O formulário ficou disponível entre 16 de setembro de 2022 e 11 de setembro de 2023, durante esse intervalo de tempo houveram duas campanhas de divulgação para coleta de mais dados, uma durante 16 de setembro de 2022 a 20 de novembro de 2022 e outra entre 20 de julho de 2023 até 11 de setembro de 2023.

Essa estratégia de distribuição foi cuidadosamente planejada para evitar que o questionário atendesse apenas a um nicho específico de pessoas e para garantir um alcance mais amplo. O objetivo era coletar dados não apenas de profissionais de tecnologia, mas também de pessoas de outras áreas, tornando os resultados da pesquisa mais representativos e abrangentes.

A etapa de distribuição do questionário é o ponto de contato direto entre os pesquisadores e os participantes, e sua eficácia influencia diretamente na qualidade dos dados

coletados. Portanto, planejar e executar essa fase com precisão é fundamental para o sucesso de qualquer pesquisa de levantamento.

3.7 Análise dos resultados obtidos

A etapa de análise dos resultados numa pesquisa de *survey* é um processo crítico que requer atenção para evitar conclusões precipitadas que podem comprometer toda a pesquisa. Para uma análise ser bem feita dos dados, deve-se evitar vieses e o pesquisador sem imparcial diante das informações obtidas com o tratamento dos dados e as conclusões devem ser o reflexo da realidade trazida pelas informações obtidas e não pela vontade do pesquisador.

Para esta pesquisa foram coletadas 350 respostas durante o período que o questionário ficou disponível, essa informação está presente na subseção 3.6, para a apresentação dos dados obtidos foram elaborados gráficos e relatórios que estão presentes nas seções 4 e 5.

Com a realização desta pesquisa foi possível entender melhor o contexto atual de segurança dos dados e privacidade no ambiente de teletrabalho, com os dados coletados através das respostas do participantes voluntários foi possível fazer uma análise qualitativa sobre o comportamento dos participantes e engajamentos dos funcionários da adoção de medidas de segurança básicas para um trabalho seguro e preservando a sua privacidade no teletrabalho e quais recursos que as empresas fornecem para prover um ambiente seguro nesse contexto.

3.8 Ameaças à validade e considerações éticas

A pesquisa científica é uma jornada em busca de respostas, uma exploração sistemática do desconhecido. No entanto, essa busca não está isenta de desafios cruciais que podem comprometer a confiabilidade e a validade dos resultados obtidos. É muito importante o processo de mapeamento de possíveis ameaças para pesquisa, pois isso garante uma maior credibilidade dos resultados, ajuda na tomada de decisões corretas, economiza tempo do pesquisador evitando o desperdício de tempo em pesquisas que podem não produzir resultados válidos, além de ter um caráter ético pois torna transparente as limitações e possíveis vieses em um estudo. Nesta seção serão abordados alguns tipos de ameaças à validade da pesquisa que foram abordadas nos trabalhos de Jacques Wainer (2007) [41] e de Guilherme Travasso (2002) [43]. Essa seção é dividida em quatro subseções são elas: 3.8.1

Validade de Construção; 3.8.2; Validade Interna; 3.8.3 Validade Externa; 3.8.4 Validade de Conclusão; Ética da Pesquisa.

3.8.1 Validade de Construção

A validade de construção, de acordo com Travassos et al. (2002) [43], refere-se à análise dos vínculos entre a teoria e a observação. Em outras palavras, visa determinar se o tratamento retrata adequadamente a causa e se o resultado representa de forma precisa o efeito. No processo de avaliação da validade da construção um aspecto muito importante a ser observado é o humano, tanto do lado do pesquisador quanto do participante, pois os dois lados são potencialmente suscetíveis a falhas e sujeitos a serem influenciados por vieses e induzidos ao erro por interpretações incorretas baseados em suas suposições ou até mesmo por uma falha na elaboração da pesquisa abrindo espaço para interpretações dúbias.

Nesta pesquisa um ponto de ameaça de validade de construção é a forma pelo qual os participantes poderiam interpretar o questionário, além disso devido ao tema ser relacionado a algo sensível como é as questão de segurança dos dados e privacidade os participantes poderiam passar uma imagem diferente da realidade para evitar expor possíveis vulnerabilidades geradas por eles e existentes no seu ambiente de trabalho.

Para mitigar possíveis interpretações dúbias e errôneas relacionadas ao questionário, foram conduzidos testes pilotos e através dos feedbacks e estudos realizados sobre outras pesquisas *survey* o questionário passou por melhorias até chegar ao modelo final. Vale ressaltar que um dos motivos pelo qual o questionário foi elaborado de forma anônima foi para que os participantes se sentissem mais à vontade para respondê-lo sem medo de expor a sua identidade e possíveis vulnerabilidades no ambiente de trabalho.

3.8.2 Validade Interna

A validade interna é responsável por determinar se a relação observada entre o tratamento e o resultado é realmente causal, assegurando que essa relação não seja influenciada por outros fatores não controlados ou não medidos. Ao avaliarmos a validade interna, é crucial direcionar uma atenção especial para diversos elementos, incluindo a seleção dos participantes, a forma como eles foram agrupados em diferentes categorias, a

implementação dos tratamentos e considerações relativas aos aspectos sociais envolvidos no estudo [43].

Uma potencial ameaça à validade interna desta pesquisa está relacionada à seleção dos participantes. O questionário foi divulgado através de diversos canais de comunicação, como grupos de e-mail e redes sociais, como Telegram, LinkedIn, WhatsApp e Facebook. No entanto, os participantes não foram selecionados de forma estritamente aleatória, por meio de sorteio, por exemplo. É importante notar que a divulgação ocorreu principalmente em grupos em que o pesquisador tinha participação ativa.

Essa abordagem pode limitar a representatividade dos dados coletados, uma vez que, dos 350 respondentes, aproximadamente 78% tinham formação na área de Tecnologia da Informação (TI) e cerca de 28,3% dos participantes não eram público-alvo da pesquisa. Portanto, os resultados obtidos podem não ser tão generalizáveis para outras áreas, o que ressalta a importância de considerar essa possível limitação ao interpretar os resultados deste estudo.

3.8.3 Validade Externa

A validade externa está relacionada com as condições que podem restringir a capacidade de aplicar os resultados de um experimento em um contexto real. Durante a avaliação da validade externa, é fundamental considerar como o tratamento interage com as pessoas, o local e o período de tempo em que o estudo foi realizado [41][43].

Uma possível ameaça à generalização dos resultados está relacionada ao tamanho da amostragem da pesquisa. Foram coletadas 350 respostas, no entanto, a composição majoritária dos participantes era de pessoas com formação em Tecnologia da Informação (TI), correspondendo a 78% do tamanho da amostra. Além disso, cerca de 28,3% dos participantes não faziam parte do público-alvo original da pesquisa, pois declararam trabalhar no modelo presencial. No entanto, esses participantes foram incluídos na pesquisa a título de comparação com os que trabalhavam nos modelos híbrido e totalmente remoto.

Essas variações na composição da amostra podem representar um desafio para a generalização dos resultados, uma vez que a representatividade da população de interesse pode estar comprometida. Portanto, ao interpretar os resultados, é essencial levar em consideração essas nuances e limitações relacionadas à amostragem da pesquisa, isso é uma

característica inerente a esse método de pesquisa devido ao tipo de amostragem e forma como os dados foram coletados.

3.8.4 Validade de Conclusão

A validade de conclusão está intrinsecamente ligada à capacidade de se chegar a uma conclusão precisa sobre as relações entre o tratamento e os resultados de um experimento. Ao avaliar a validade da conclusão, é imperativo considerar vários conceitos, como a seleção adequada do teste estatístico, a determinação do tamanho da amostra, a confiabilidade das medidas e a consistência na implementação dos tratamentos [43].

No entanto, existem desafios que podem surgir quando se lida com a validade de conclusão. Um deles é a baixa potência do teste estatístico, o que aumenta o risco de conclusões incorretas. Alguns testes estatísticos têm requisitos específicos, como a suposição de uma distribuição normal na população de participantes.

Além disso, é importante reconhecer que os pesquisadores podem influenciar os resultados ao buscar resultados específicos. As medidas podem incluir elementos de julgamento humano, o que pode levar a resultados diferentes se o mesmo objeto for medido várias vezes.

Uma potencial ameaça à validade na pesquisa é a forma como os participantes se auto avaliam em relação ao seu conhecimento sobre os temas abordados no questionário. Além disso, não podemos garantir que as atitudes captadas no questionário correspondam à realidade dos participantes. Essa discrepância entre a autopercepção e a realidade pode influenciar as conclusões deste trabalho, embora seja uma característica inerente a esse tipo de pesquisa.

Portanto, ao avaliar a validade da conclusão, é fundamental abordar esses desafios com rigor e atenção aos detalhes, garantindo que as conclusões sejam baseadas em evidências sólidas e representativas.

3.8.5 Aspecto Ético da Pesquisa

No que diz respeito à dimensão ética desta pesquisa, o questionário foi meticulosamente elaborado para garantir a coleta de dados de forma anônima, protegendo assim a identidade dos participantes voluntários e das empresas nas quais eles estão

empregados. Adicionalmente, um termo de consentimento (Visualizar no apêndice A) foi desenvolvido e apresentado aos participantes, detalhando todos os aspectos da pesquisa. Isso não apenas proporcionou aos participantes uma visão clara sobre os dados fornecidos por eles e o propósito da pesquisa, mas também enfatizou a importância primordial da ética na pesquisa, promovendo transparência em todo o processo.

4. Resultados da pesquisa

Nesta seção do trabalho, serão apresentados os resultados obtidos por meio do questionário elaborado para esta pesquisa. Os dados que serão discutidos nesta seção foram coletados com a colaboração de voluntários e passaram por tratamento visando uma análise mais precisa. A Seção 4 está subdividida em seis subseções, a saber: 4.1 - Limpeza e tratamento dos dados; 4.2 - Perfil dos Participantes; 4.3 - Comportamento dos Participantes; 4.4 - Recursos providos pelas instituições e empresas aos seus funcionários; 4.5 - Nível de conhecimento e importância sobre alguns tópicos relacionados a segurança no trabalho remoto; E, por fim, a Seção 4.6 - Análise Final sobre os Resultados.

4.1 Limpeza e tratamento dos dados

O tratamento dos dados em uma pesquisa é um processo delicado que ocorre após a coleta inicial de informações. Nessa fase, os pesquisadores revisaram minuciosamente os dados brutos coletados para identificar e corrigir quaisquer problemas, erros ou inconsistências. O objetivo principal é garantir que os dados estejam completos, precisos e confiáveis, de modo que os resultados finais da pesquisa sejam representativos da realidade e não sejam distorcidos por informações incorretas ou ausentes.

Para este trabalho foram coletadas 350 respostas por meio do questionário distribuído durante a pesquisa. Após uma análise preliminar, foram identificadas algumas respostas incompletas e outras que não estavam alinhadas com o público-alvo da pesquisa. Com o objetivo de realizar uma análise mais precisa, foi optado por filtrar esses dados. Primeiramente, foi decidido como lidar com as respostas incompletas, que representavam 6,3% do conjunto de dados brutos, totalizando 22 respostas. Dado que as perguntas relacionadas a esses dados tinham uma natureza qualitativa, concluiu-se que utilizar estratégias estatísticas para imputar essas respostas não se mostraria viável. Portanto, optou-se por removê-las.

Após a exclusão das respostas incompletas, restaram 328 respostas. Dessas, 88 respostas não estavam alinhadas com o público-alvo da pesquisa, pois correspondiam a participantes que declararam trabalhar no regime de trabalho presencial. Esse conjunto representou 25,1% do total de respostas coletadas. Como resultado, sobraram 240 respostas, correspondendo a cerca de 68,6% do total, que verdadeiramente representavam o público-alvo.

da pesquisa e estavam completas. Essas respostas foram utilizadas como base para a análise da pesquisa. A tabela 2 e Figura 2 representam esses conjuntos de dados.

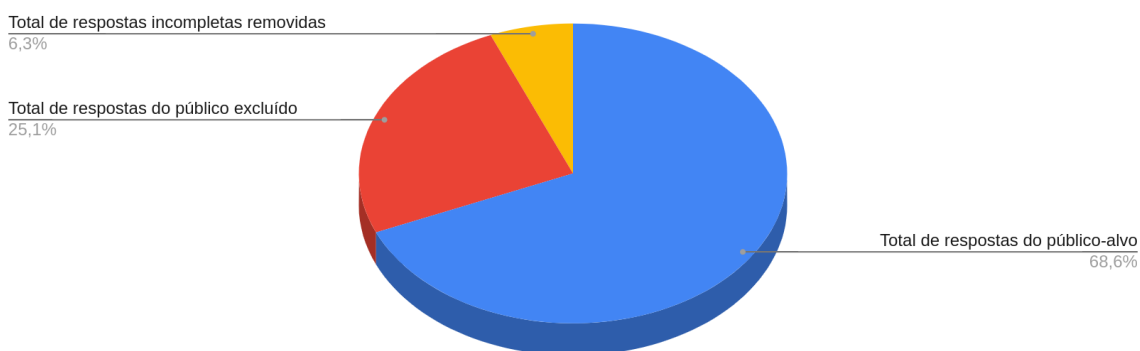
Tabela 2 - Tabela de particionamento dos dados após limpeza e filtragem.

Particionamento dos dados após limpeza e filtragem	
Total de respostas do público-alvo	240
Total de respostas do público excluído	88
Total de respostas incompletas removidas	22
Total de respostas	350

Fonte: Elaborada pelo autor (2023).

Figura 2 - Gráfico de particionamento dos dados após limpeza e filtragem.

Particionamento dos dados após limpeza e filtragem



Fonte: Elaborada pelo autor (2023).

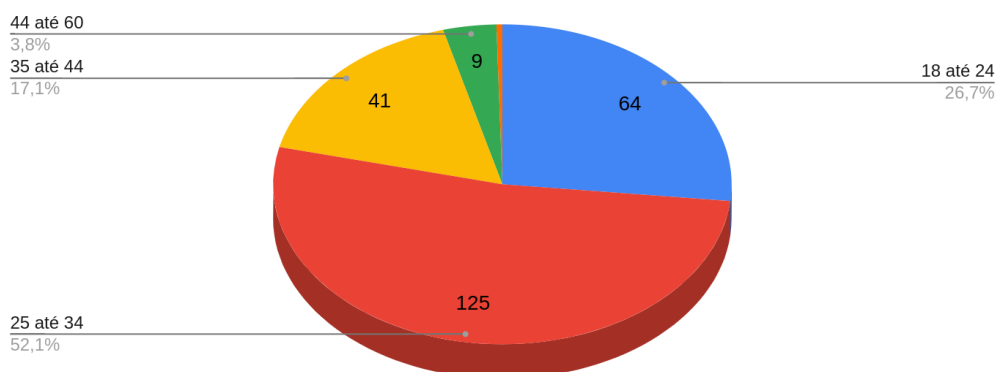
4.2 Perfil dos participantes

Esta subseção apresentará os resultados obtidos em cada questão na seção 2 do questionário, referente a dados relacionados aos perfis dos participantes.

As faixas etárias dos participantes podem ser observadas na figura 3, nota-se que a predominante na pesquisa foi a entre 24 até 34 anos correspondendo a (52,1%) do total de respostas, em segundo lugar a faixa entre 18 até 24 e em terceiro a faixa etária entre 35 até 44 anos com 17,7%, vale salientar que a faixa etária entre 44 até 60 invade o conjunto da 35 até 44 anos por um erro na elaboração do questionário que só foi observada quando o mesmo já tinha sido amplamente divulgado, porém foi analisado que a faixa entre 44 até 60 só correspondia a 3,8% das respostas logo se juntar essas última faixas etárias elas correspondem a cerca de 20,9% das resposta sendo a faixa acima de 60 anos equivalente a só 0,3% do montante total com 1 resposta.

Figura 3 - Faixa etária do público-alvo.

Faixas etárias do público-alvo

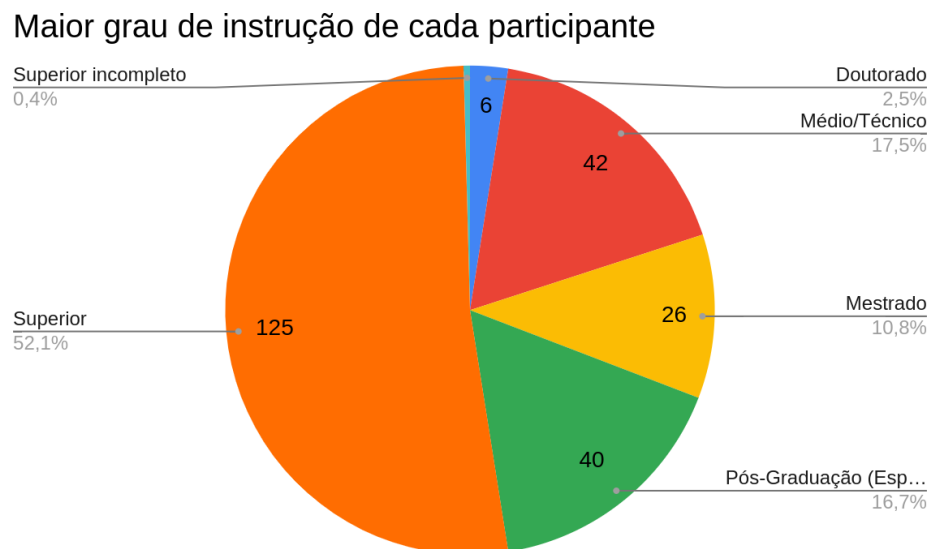


Fonte: Elaborada pelo autor (2023).

Em relação ao maior grau de instrução dos participantes notou-se que a maior parcela dos participantes tinham nível superior de escolaridade correspondente a 52,1% das respostas, em seguida nível médio/técnico (17,5%) , pós-graduação (16,7%), mestrado (10,8%) e Doutorado (2,5%). Só um participante declarou ter o nível superior incompleto (0,4%), e esse também pode ser encaixado no conjunto de pessoas só com nível médio/técnico completo, ou seja, se esses conjuntos forem somados eles dois correspondem a 17,9% das respostas, sendo

o segundo maior subconjunto presente na pesquisa. Os dados sobre o maior grau de instrução dos participantes estão representados na figura 4.

Figura 4 - Maior grau de instrução de cada participante.



Fonte: Elaborada pelo autor (2023).

Sobre a área de formação dos participantes foram coletadas muitas respostas de diferentes áreas, logo foi decidido categorizar e agrupar algumas áreas que tinham características em comum para facilitar a análise dos dados, a categorização das respostas pode ser observada na tabela 3 e o resultado final desse processo na tabela 4.

Tabela 3 - Tabela de categorização das áreas de formação dos participantes.

3- Qual sua área de formação?	Subtotais	Áreas de formação categori
Administração/Gestão/Financeira	14	Administração/Gestão/Financ
Agropecuária e Redes	1	Biológicas/Saúde
Biologia	1	Biológicas/Saúde
Comunicação	1	Ciências Humanas
Comunicação	1	Ciências Humanas
Design industrial	1	Ciências Humanas
Educação	2	Educação
Engenharia (todos os cursos de engenharia exceto engenharia	15	Engenharia (todos os cursos de engenharia exceto engenharia computação)
Estatística	1	Exatas
Estudante	1	Outros
História e Arquitetura	1	Ciências Humanas
Humanas	1	Ciências Humanas
Jurídico	2	Jurídica
Saúde	3	Biológicas/Saúde
Tecnologia/Computação	195	Tecnologia/Computação
Total geral	240	

Fonte: Elaborada pelo autor (2023).

Tabela 4 - Resultado da categorização das áreas de formação.

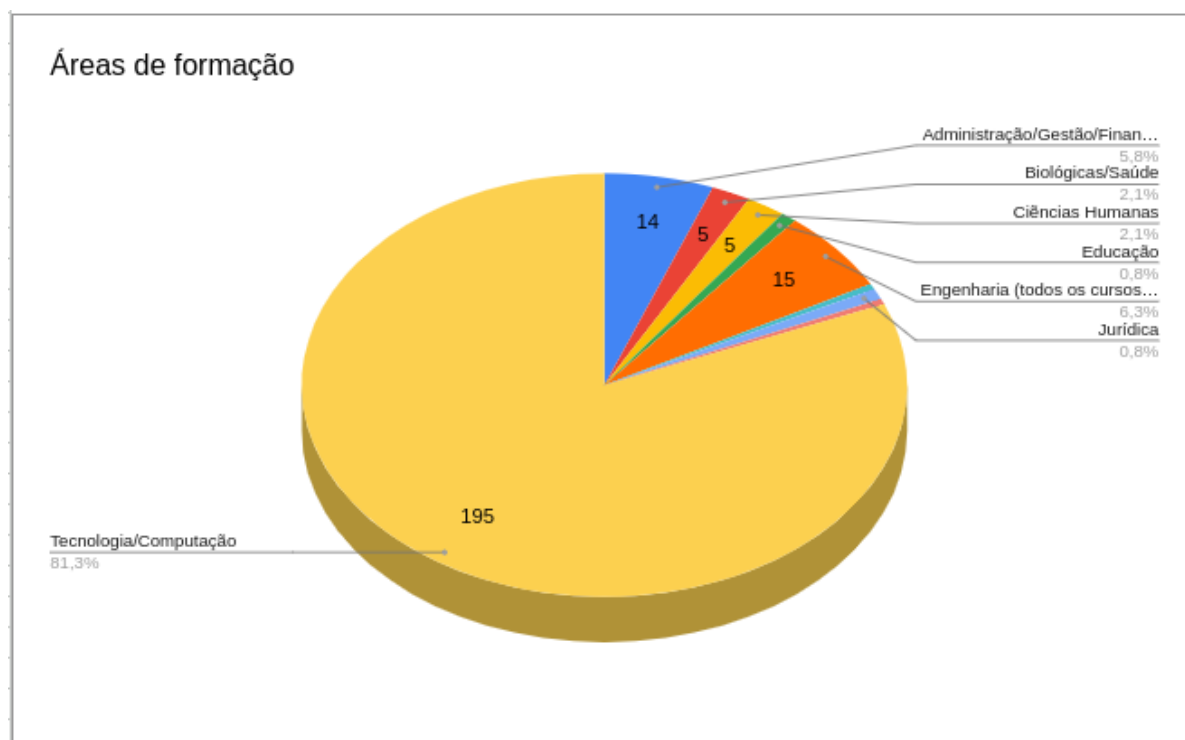
Áreas de formação categorizadas	Subtotais
Administração/Gestão/Financeira	14
Biológicas/Saúde	5
Ciências Humanas	5
Educação	2
Engenharia (todos os cursos de engenharia exceto engenharia	15
Exatas	1
Jurídica	2
Outros	1
Tecnologia/Computação	195
Total geral	240

Fonte: Elaborada pelo autor (2023).

Com a categorização dos dados observou-se que cerca de 81,3% dos participantes tinham como área de formação de tecnologia e computação, a segunda maior área foi a de engenharia (6,3%) com 15 respostas e logo em seguida as áreas de administração, gestão e financeira que somadas correspondem a (5,8%) do público-alvo com 14 respostas. As outras categorias de áreas somadas somam juntas 6,6% do público-alvo, são elas biológicas e saúde,

ciências humanas, educação, exatas, jurídica e outros. A distribuição das áreas de formação pode ser observada na figura 5.

Figura 5 - Áreas de formação categorizadas.



Fonte: Elaborada pelo autor (2023).

Um outro dado coletado no questionário foi a área de trabalho do participante, foram obtidas muitas respostas referentes a diferentes áreas, houve a necessidade de categorizar esses dados para uma melhor visualização e compreensão deles, a categorização e agrupamento desses dados pode ser observada na tabela 5 e o resultado após a categorização está presente na tabela 6.

Tabela 5 - Áreas de trabalho dos participantes.

5 - Qual a sua área de trabalho atualmente?	Subtotais	Categorização das áreas de trabalho
HR	1	Administrativo/Gestão/Financeiro
Administrativo	6	Administrativo/Gestão/Financeiro
Ambiental	1	Outras
Biologia	1	Outras
Computação	201	Computação
Consultoria	1	Outras
Dados	1	Computação
Design	1	Design/Inovação
Design de produtos digitais	1	Design/Inovação
Design digital	1	Design/Inovação
Docência	1	Educação
Educação	1	Educação
Educação	1	Educação
Educação e Laboratório de pesquisa	1	Educação
Engenharia	1	Engenharia
Fabricação	1	Engenharia
Financeiro	4	Administrativo/Gestão/Financeiro
Games	1	Outras
Inovação	1	Design/Inovação
Jurídico	3	Jurídico
Líder de Equipe Técnica em TI	1	Computação
Manutenção de subestações de energia elétrica.	1	Engenharia
Marketing	3	Marketing
Pesquisador	1	Educação
Saúde	1	Saúde
Terceiro Setor	1	Outras
Vendas	2	Vendas
Total geral	240	

Fonte: Elaborada pelo autor (2023).

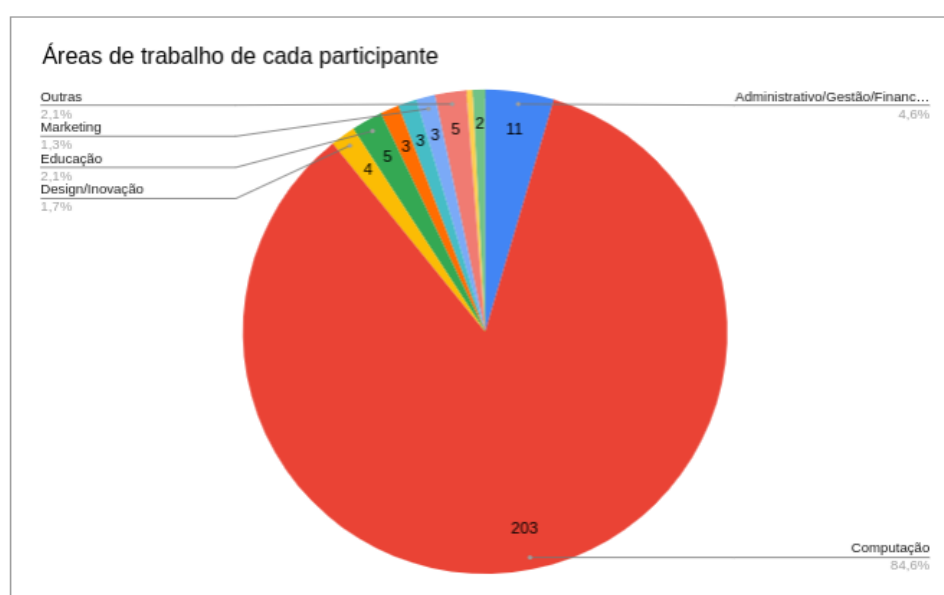
Tabela 6 - Áreas de trabalho dos participantes categorizadas.

<i>Categorização das áreas de trabalho</i>	<i>Subtotais</i>
Administrativo/Gestão/Financeiro	11
Computação	203
Design/Inovação	4
Educação	5
Engenharia	3
Jurídico	3
Marketing	3
Outras	5
Saúde	1
Vendas	2
Total geral	240

Fonte: Elaborada pelo autor (2023).

É possível observar na figura 6 que a maior parcela de participantes responderam que trabalhavam na área de computação onde essa correspondeu a 84,6% do público-alvo, logo após às áreas administrativas, gestão e financeira somam 4,6% do público-alvo e as outras áreas juntas correspondem a 10,8% das respostas, são elas design e inovação (1,7%), educação(2,1%), engenharia (1,3%), jurídica (1,3%), marketing (1,3%), saúde (0,4%), vendas (0,8%) e outras (2,1%).

Figura 6 - Áreas de trabalho de cada participante categorizadas.

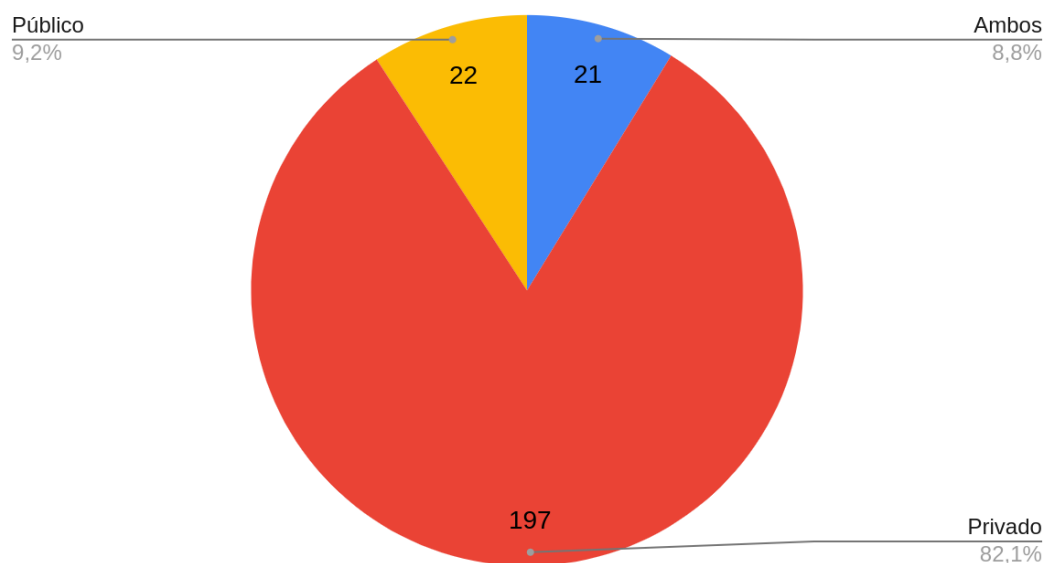


Fonte: Elaborada pelo autor (2023).

Em relação às instituições de trabalho e empresas que os participantes atuam cerca de 82,1% fazem parte do setor privado, do setor público são 9,2% e alguns declararam que trabalham em ambos os setores essa parcela corresponde a 8,8% do público-alvo. A figura 7 ilustra a distribuição desses setores.

Figura 7 - Setores das instituições onde os participantes trabalham.

Setores das instituições de trabalho dos participantes

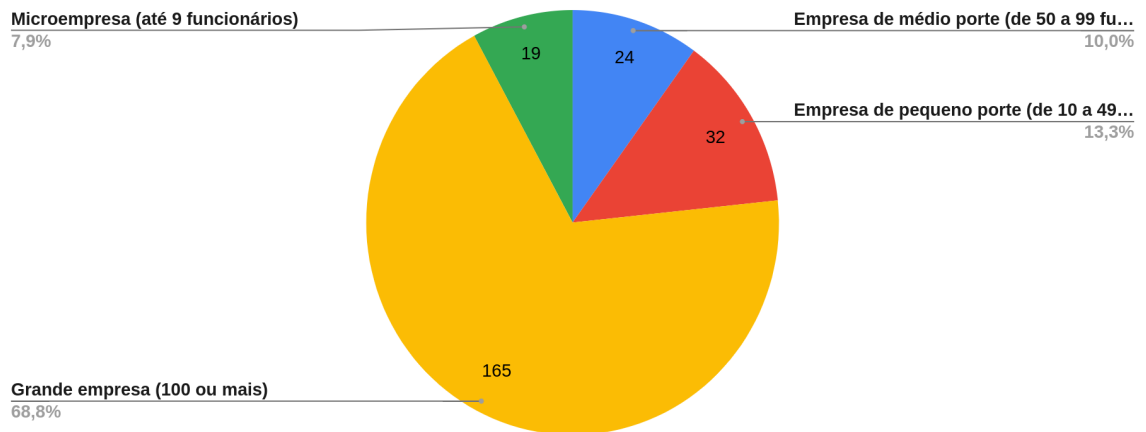


Fonte: Elaborada pelo autor (2023).

Como pode ser observado na figura 8, a maior parcela dos participantes atuam em empresas ou instituições de grande porte (68,8%), logo em seguida com 13,3% vem as de pequeno porte, com 10,0% as de médio porte e 7,9% as de pequeno porte.

Figura 8 - Porte da Instituição.

Porte das instituições de trabalho

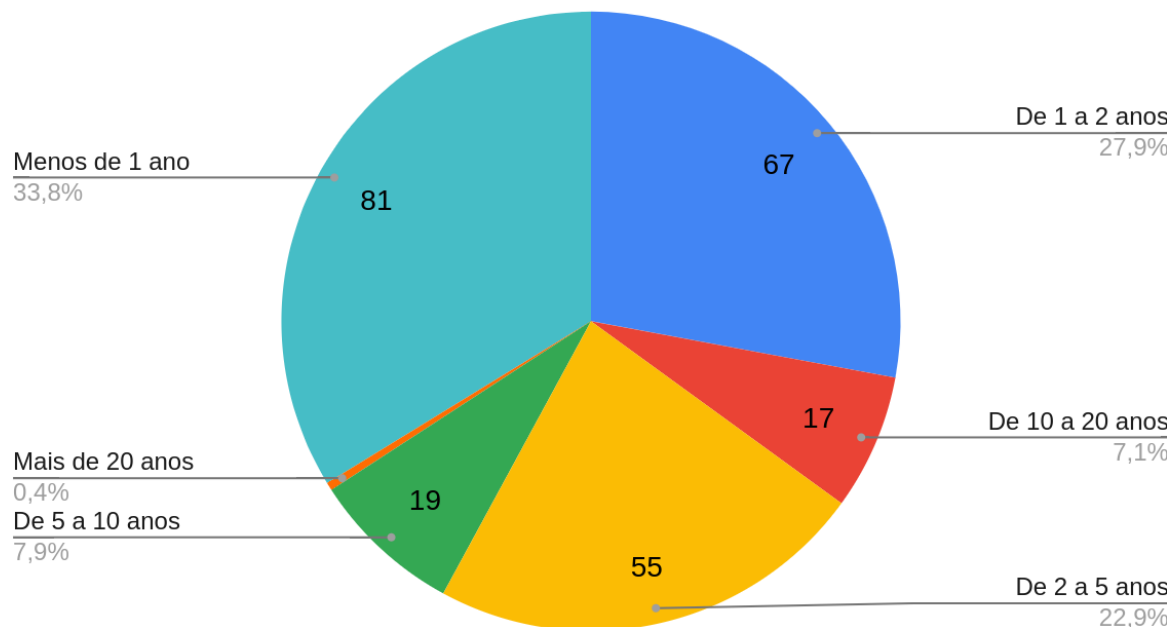


Fonte: Elaborada pelo autor (2023).

A respeito do tempo de trabalho que os participantes declaram ter nas suas atuais instituições cerca de 33,8% informaram que estavam a menos de um ano trabalhando nelas, a parcela correspondente ao tempo de casa entre 1 a 2 anos apareceu com 27,9%, logo em seguida os que tinham entre 2 a 5 anos de trabalho com 22,9%, quem tinha de 5 a 10 anos representou 7,9%, logo em seguida veio o grupo que tinha entre 10 a 20 anos e por último o grupo do que tinham mais de 20 anos de casa correspondendo a só 0,4% do público-alvo. Esses dados estão ilustrados na figura 9.

Figura 9 - Tempo de trabalho na instituição atual de trabalho dos participantes.

Tempo de trabalho na instituição



Fonte: Elaborada pelo autor (2023).

No questionário também foram coletados os dados referentes em que setor o participante trabalha dentro da sua instituição ou empresa, foram obtidos um número relevante de setores diferentes e para uma melhor análise foi preciso categorizá-los, esse processo pode ser observado na tabela 7 e o resultado da final na tabela 8.

Tabela 7 - Setor de trabalho dos participantes dentro das suas respectivas instituições.

9 - Você trabalha em qual setor da instituição?	Subtotais	Categorização dos setores nas instituições
Administrativo	4	Administrativo
Advogada	1	Jurídico
Analista de cybersecurity	1	Tecnologia da Informação
Consultoria	2	Operacional
dados	1	Tecnologia da Informação
Desenvolvedor	1	Tecnologia da Informação
Desenvolvimento	3	Tecnologia da Informação
Desenvolvimento de Produtos	1	Pesquisa/Inovação
Desenvolvimento de produtos digitais	1	Tecnologia da Informação
Desenvolvimento de software	1	Tecnologia da Informação
Desenvolvimento de software	1	Tecnologia da Informação
Engenharia	1	Operacional
Engenharia / Desenvolvimento	1	Tecnologia da Informação
Engenharia de software	2	Tecnologia da Informação
Ensino privado autônomo	1	Outros
Financeiro	3	Financeiro
Gestão	2	Administrativo
Governança de Plataformas	1	Administrativo
Homologação	1	Outros
Inovação	1	Pesquisa/Inovação
Inteligência Artificial	1	Tecnologia da Informação
Marketing	2	Outros
Modelagem e simulavão	1	Outros
Operacional (Setor responsável diretamente pelo ramo de	57	Operacional
Pesquisa & Desenvolvimento	1	Tecnologia da Informação
Pesquisa e desenvolvimento de software para veículos au	1	Pesquisa/Inovação
Projetos	1	Outros
Recursos Humanos	2	Recursos Humanos
RH e Operacional	1	Recursos Humanos
Segurança da Informação	1	Tecnologia da Informação
Segurança da informação	1	Tecnologia da Informação
TI (desenvolvimento de sistemas)	1	Tecnologia da Informação
TI (Desenvolvimento Web)	1	Tecnologia da Informação
TI (Suporte ao usuário e Infraestrutura)	134	Tecnologia da Informação
TI, desenvolvedor de SW	1	Tecnologia da Informação
Todos	1	Outros
Vendas	3	Vendas
Total geral	240	

[OBJ]

Fonte: Elaborada pelo autor (2023).

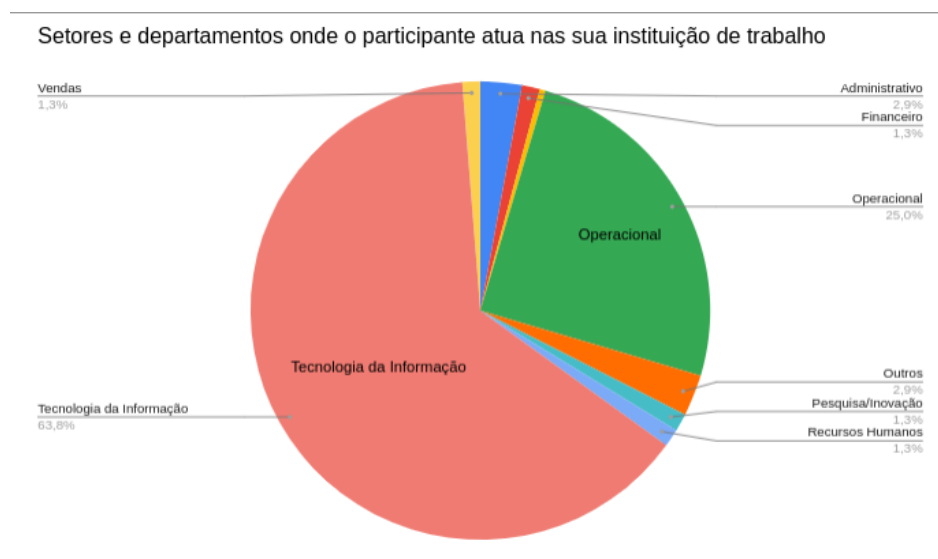
Tabela 8 - Setores de trabalho dos participantes dentro das suas respectivas instituições categorizados.

<i>Categorização dos setores nas instituições</i>	<i>Subtotais</i>
Administrativo	7
Financeiro	3
Jurídico	1
Operacional	60
Outros	7
Pesquisa/Inovação	3
Recursos Humanos	3
Tecnologia da Informação	153
Vendas	3
Total geral	240

Fonte: Elaborada pelo autor (2023).

A maior parte dos participantes informaram que trabalhavam no setor de tecnologia da informação em suas instituições de trabalho, pode-se observar na figura 10 que essa parcela equivalia a 63,8% do total de respostas, o segundo maior grupo informou que trabalhava no setor operacional da empresa, ou seja, no setor responsável pela atividade fim da empresa, esses correspondem a 25% e os outros setores somados correspondem 11,2% de total, são eles: administrativo (2,9%), vendas (1,3%), recursos humanos (1,3%), Pesquisa/Inovação (1,3%), financeiro (1,3%), jurídico (0,4%) e outros (2,91%).

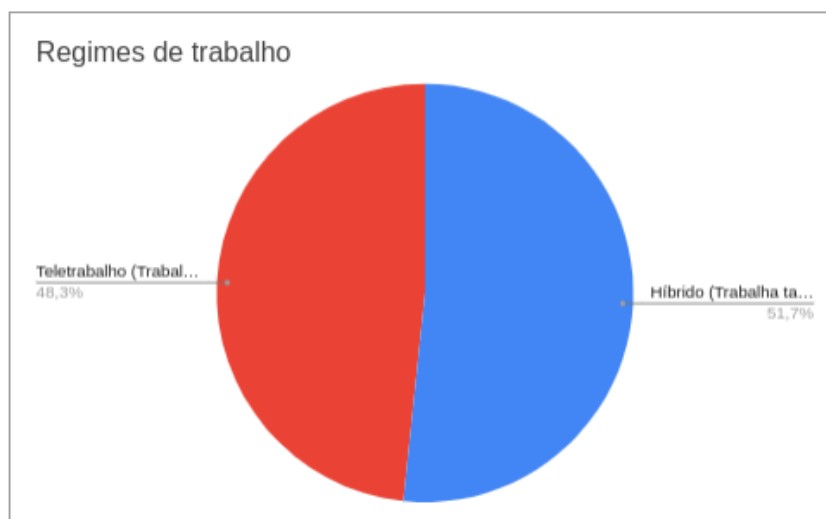
Figura 10 - Setores e departamentos onde os participantes atuam nas suas instituições de trabalho.



Fonte: Elaborada pelo autor (2023).

O público-alvo dessa pesquisa são pessoas que trabalham em regime de teletrabalho totalmente remoto ou no modelo híbrido onde o funcionário pode trabalhar parte do tempo remoto e parte do tempo no escritório da sua instituição. Após o filtro mencionado na subseção 4.1 a distribuição desses grupos ficou da seguinte forma, cerca de 48,3% informaram que trabalhavam totalmente remoto e cerca de 51,7% trabalhavam no modelo híbrido, isso pode ser observado na figura 11.

Figura 11 - Regimes de trabalho do público alvo.



Fonte: Elaborada pelo autor (2023).

A figura 12 está ilustrada a distribuição dos participantes pelas suas regiões globais de atuação, ou seja, regiões para onde eles trabalham ou prestam serviço. Vale salientar que um participante pode trabalhar para mais de uma região. Com uma parcela considerável da população o Brasil está em primeiro lugar com 89,58% dos participantes declarando trabalhar ou prestar serviço nele, em segundo lugar a América do norte com 11,27% e em seguida a América do Sul com 6,67% as outras regiões tiveram um percentual menor de 5% cada individualmente.

Figura 12 - Distribuição de participantes pelas suas regiões globais de atuação.

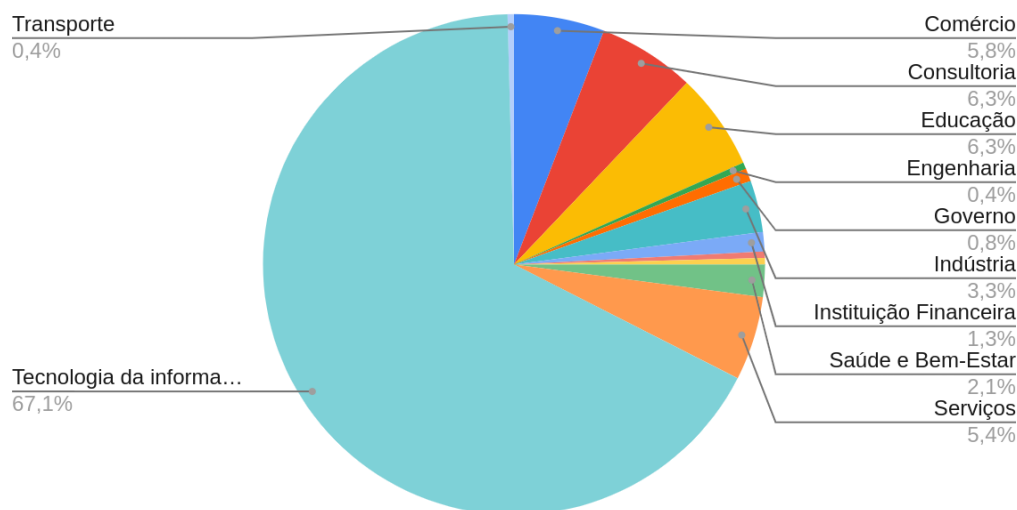


Fonte: Elaborada pelo autor (2023).

Outro ponto abordado no questionário foi sobre o ramo de atividade econômica da instituição que o participante trabalha e atua, para esse dados foram coletados muitos ramos diferentes e para uma melhor análise foi necessário categorizá-los e agrupá-los de acordo com características em comum, os dados finais estão representados na figura 13. É possível notar que o setor econômico mais presente na pesquisa é o de tecnologia correspondendo a 67,1% do número total de respostas, em segundo lugar está o setor de consultoria (6,3%), logo em seguida educação com 6,3%, comércio (5,8%), serviços (5,4%) e os outros setores somados correspondem a 2,8% do total.

Figura 13 - Ramos de atividades econômicas das instituições dos participantes categorizados.

Principais ramos de atividade econômica das instituições categorizados



Fonte: Elaborada pelo autor (2023).

4.3 Comportamento dos participantes

Esta subseção tem por finalidade apresentar os resultados referente ao comportamento dos participantes no ambiente de teletrabalho, serão apresentados os resultados referentes às perguntas do questionário relacionadas a esse aspecto.

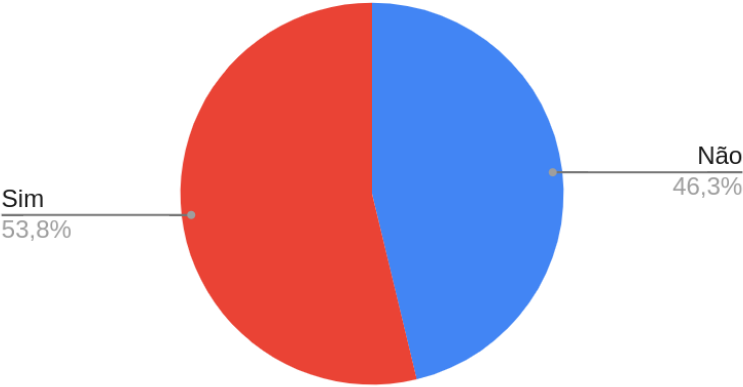
Pergunta 14 - “Você utiliza recurso pessoal para fins de trabalho? Exemplo: Computador pessoal, celular pessoal, licença de software pessoal, etc...”.

Cerca de 53,8% dos participantes declararam que utilizam recursos próprios para fins de trabalho, sendo 46,3% a parcela que declarou que não faz esse tipo de uso, como pode ser observado na figura 14. Foi realizada uma análise comparando os dois grupos que são público-alvo da pesquisa, em relação ao uso de recursos próprios para trabalho do grupo de participantes que disseram que utilizavam de recursos próprios 46,5% trabalham em regime 100% remoto e os outros 53,5% trabalham em regime híbrido. Dos que responderam que não

utilizavam recursos próprios para fins de trabalho, cerca de 50,5% eram trabalhadores no regime 100% remoto e os outros 45,5% faziam parte do grupo que trabalhava em modelo híbrido. Não se observou uma diferença significativa entre os dois grupos.

Figura 14 - Utilização de recursos próprios para fins de trabalho.

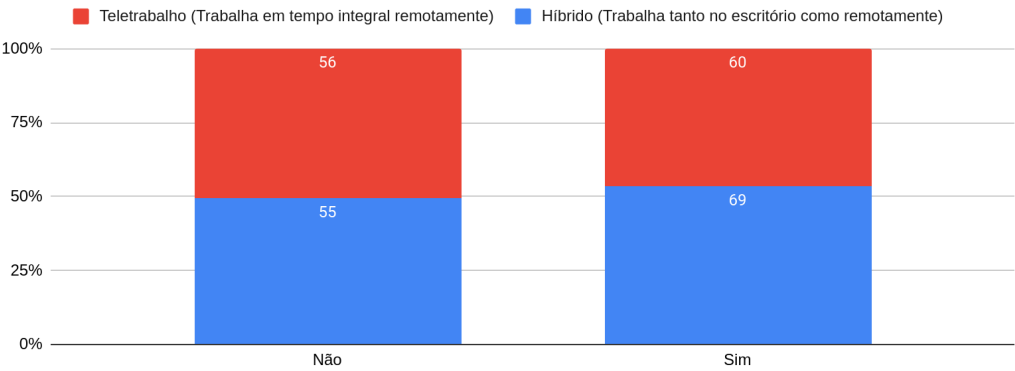
Uso de recursos pessoais



Fonte: Elaborada pelo autor (2023).

Figura 15 - Utilização de recursos próprios para fins de trabalho, comparação entre os modelos de trabalho remoto.

Uso de recursos pessoais para fins de trabalho



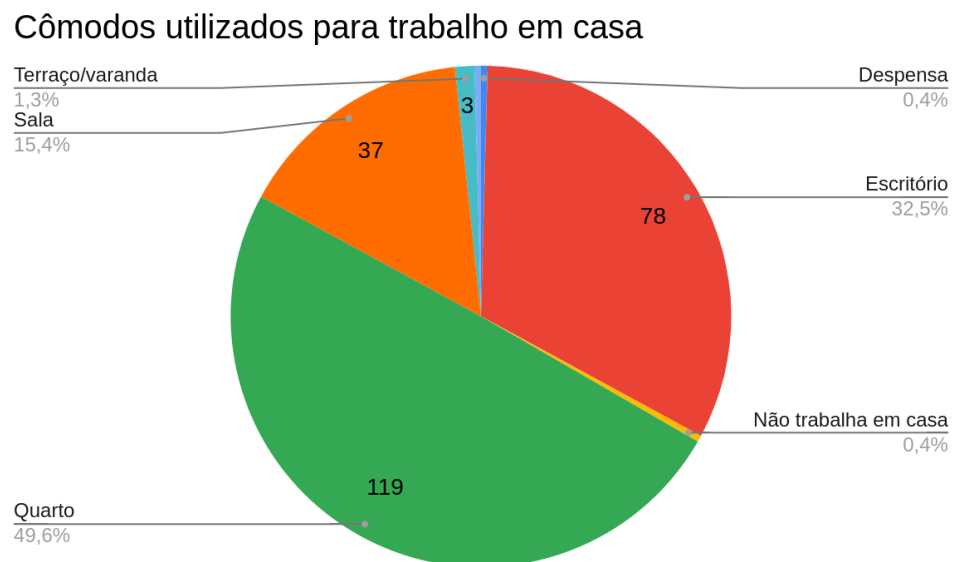
14 - Você utiliza recurso pessoal para fins de trabalho? Exemplo: Computador pessoal, celular pessoal, licença de software pessoal, e...

Fonte: Elaborada pelo autor (2023).

Pergunta 15 - “Quando você trabalha na sua casa, geralmente você trabalha em qual cômodo?”.

Em relação à pergunta 15, cerca de 49,6% dos funcionários disseram que seu cômodo de casa usual para trabalho é o quarto, 32,5% disseram que trabalham do escritório de casa e 15,4% responderam que trabalham na sala, os outros cômodos somados representam 1,7% do total e os 0,4% restantes disseram que não trabalham em casa. A figura 16 representa essa distribuição das respostas.

Figura 16 - Cômodos utilizados para trabalho em casa.

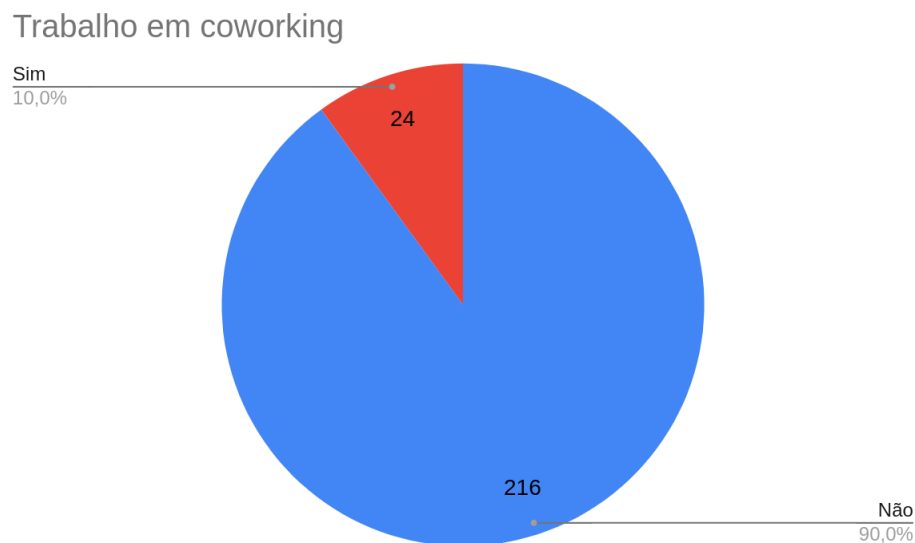


Fonte: Elaborada pelo autor (2023).

Pergunta 16 - “Você costuma trabalhar em ambientes de coworking?”

Cerca de 90,0% dos participantes declararam que não costumam trabalhar em ambiente de coworking, em contrapartida 10,0% deles disseram que trabalham nesse tipo de ambiente, vide a figura 17.

Figura 17 - Participantes que trabalham em *coworking*.

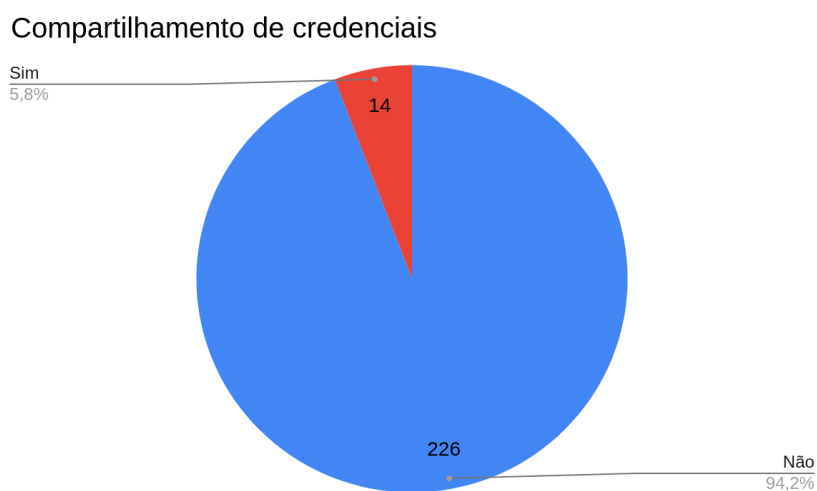


Fonte: Elaborada pelo autor (2023).

Pergunta 17 - “Você compartilha suas credenciais de sistemas com outras pessoas?”

Em relação ao compartilhamento de credenciais, cerca de 94,2% dos participantes informaram que não têm esse costume e os outros 5,8% informaram que têm esse hábito, observe na figura 18 essa representação.

Figura 18 - Compartilhamento de credenciais.



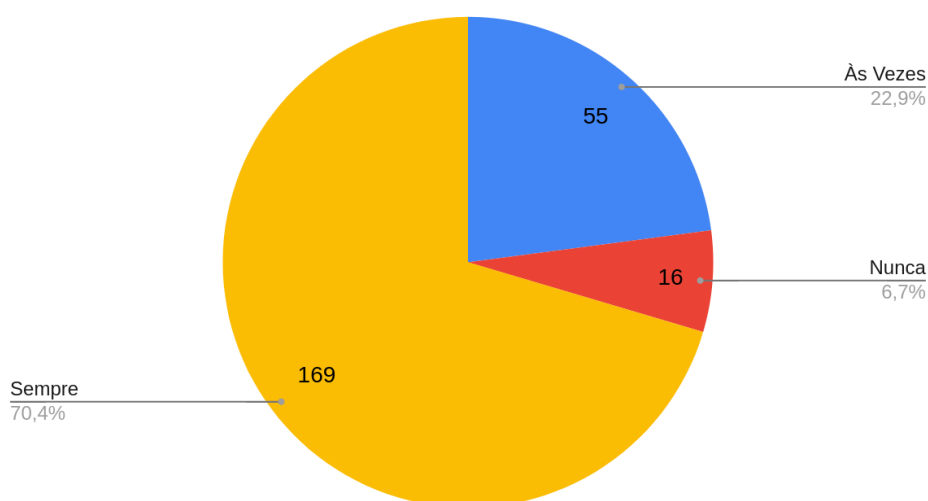
Fonte: Elaborada pelo autor (2023).

Pergunta 18 - “Você bloqueia seu computador ao se ausentar da mesa?”

Ao todo, como pode ser visto na figura 19, 70,4% dos participantes afirmaram sempre bloquear a tela do computador ao se ausentar da mesa de trabalho, 22,9% corresponderam aos que bloqueiam às vezes seus computadores e 6,7% disseram que nunca bloqueiam. Um ponto importante a se observar é que bloquear às vezes pode ser encarado como uma brecha de segurança assim como os quem nunca bloqueia o computador.

Figura 19 - Bloqueio do computador ao se ausentar da mesa.

Bloqueio do computador ao se ausentar da mesa

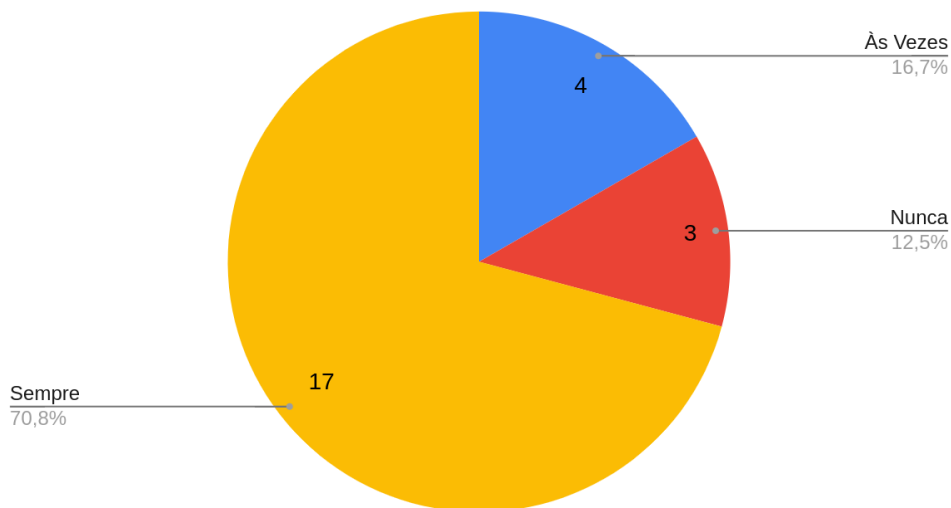


Fonte: Elaborada pelo autor (2023).

Uma outra análise foi feita restringindo os participantes que afirmaram ter costume de trabalhar em ambiente de *coworking*, a figura 20 contém a distribuição das respostas desse grupo. Desses 70,8% afirmaram bloquear a tela dos seus computadores ao se ausentar, 16,7% responderam que só bloqueiam os seus computadores às vezes e 12,5% afirmaram que nunca bloqueiam. Essa análise é muito salutar devido ao ambiente de *coworking* ser mais suscetível a riscos de segurança pois é um ambiente compartilhado entre trabalhadores de várias empresas [44].

Figura 20 - Bloqueio do computador ao se ausentar da mesa restrito no ambiente de coworking.

Bloqueio de computar ao se ausentar da mesa em coworking

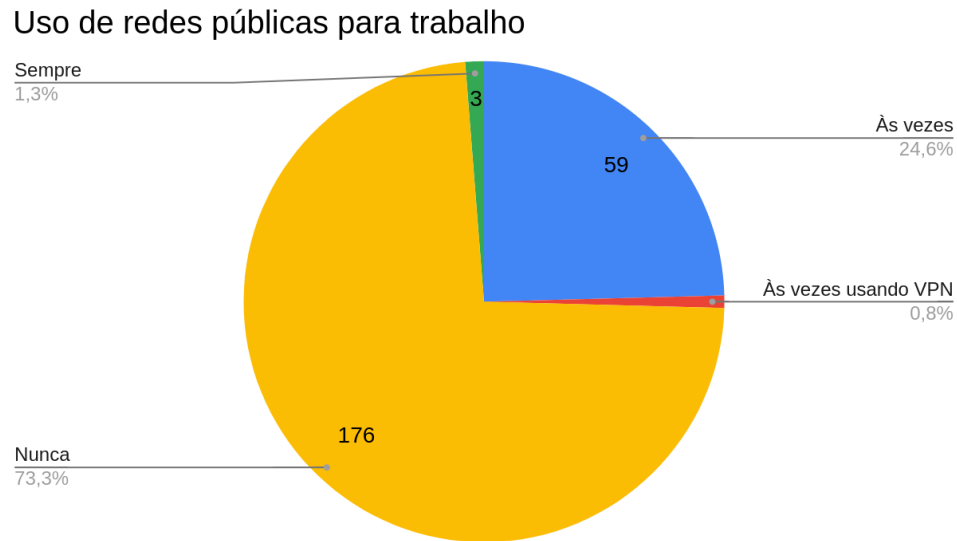


Fonte: Elaborada pelo autor (2023).

Pergunta 19 - “Você costuma trabalhar com seus equipamentos conectados em redes de internet públicas (por exemplo: Wifi de shoppings, aeroportos, cafés)?”

Cerca de 73,3% dos participantes informaram que nunca se utilizam de redes públicas para trabalhar, 24,6% informaram que utilizam às vezes desse recurso, 1,3% deles sempre utilizam e 0,8% declarou que utiliza redes públicas para trabalho às vezes, porém usam VPN para proteção das suas conexões como se observa na figura 21. O uso de redes públicas para trabalho representa um grande risco para os dados da empresa quanto do funcionário, existem mecanismos para proteger as conexões, o mais conhecido é o uso de VPN (*Virtual Private Network*), mas se deve evitar o constante uso delas para esse fim.

Figura 21 - Uso de redes públicas para trabalho.



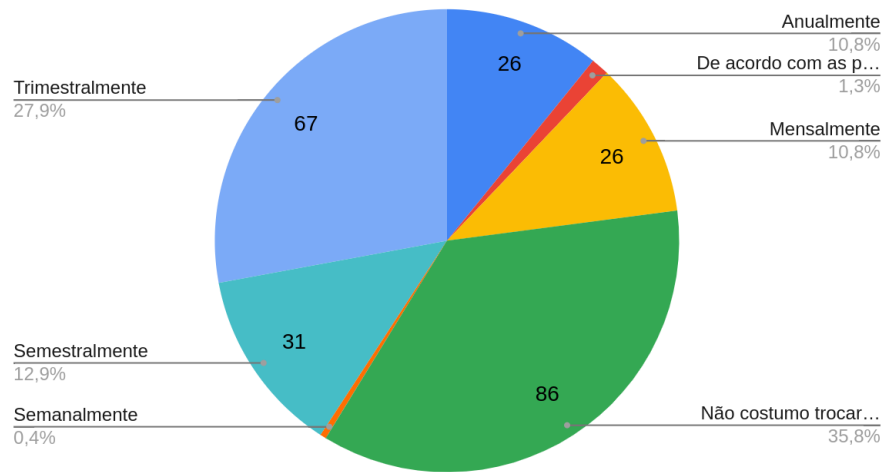
Fonte: Elaborada pelo autor (2023).

Pergunta 20 - “Você troca suas senhas com qual frequência?”

A periodicidade de trocas de senhas e credenciais é um ponto importante para proteção da identidade e dados dos usuários e sistemas de informação, na figura 22 é possível visualizar a periodicidade de troca de senhas dos participantes, cerca de 35,8% deles informaram que não costumam trocar suas senhas, 27,9% trocam suas credenciais trimestralmente, 12,9% trocam semestralmente, quem troca anualmente e mensalmente representam 10,8% das respostas cada, alguns responderam que trocam de acordo com as políticas dos sistemas esses representaram só 1,3% e os que declararam que trocavam semanalmente só representaram 0,4% .

Figura 22 - Frequência de trocas de senhas.

Frequência de trocas de senhas



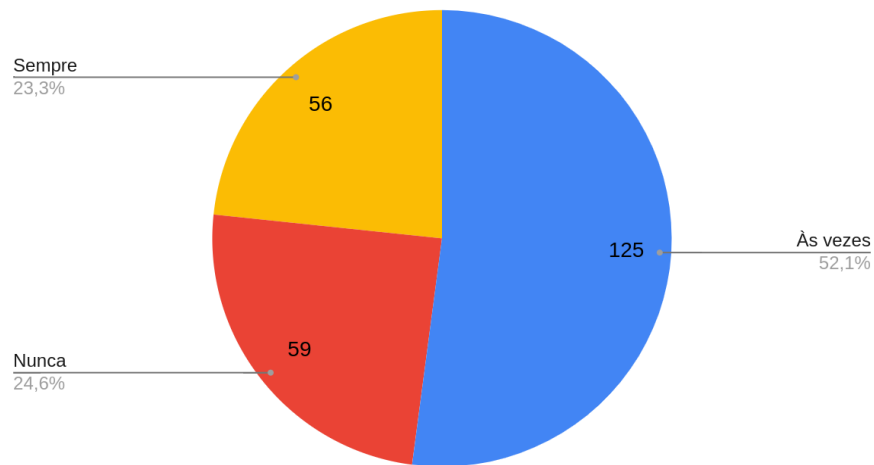
Fonte: Elaborada pelo autor (2023).

Pergunta 21 - Você usa seu computador ou equipamentos de trabalho para fins pessoais?

Em relação ao uso de equipamentos de trabalho para fins pessoais, 52,1% dos participantes utilizam às vezes, 23,3% utilizam sempre e 24,6% informaram que nunca fazem esse tipo de uso, como mostra a figura 23. Neste contexto, pessoas que sempre utilizam e as que utilizam às vezes podem ser categorizadas como pessoas que usam, somando essas duas parcelas pode ser considerado que 75,4% dos participantes utilizam equipamentos para uso pessoal independente da frequência.

Figura 23 - Uso dos equipamentos de trabalho para fins pessoais.

Uso dos equipamentos de trabalho para fins pessoais



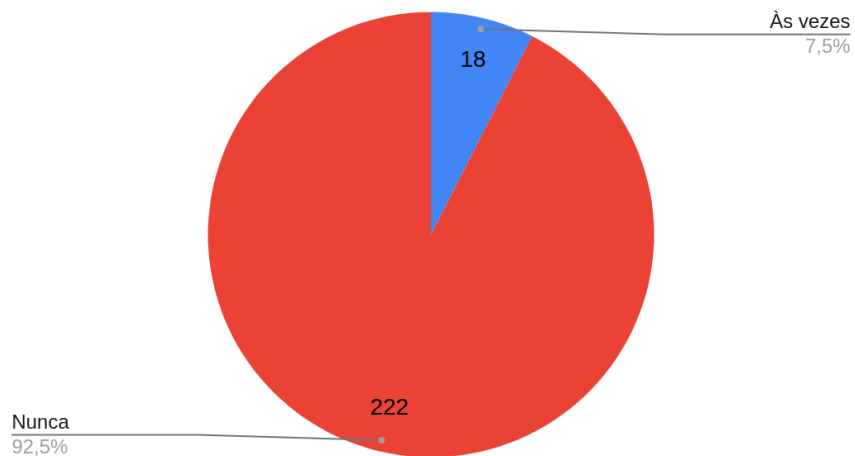
Fonte: Elaborada pelo autor (2023).

Pergunta 22 - “Você empresta seu computador ou equipamento de trabalho para terceiros?”

Como mostra a figura 24 cerca de 92,5% dos participantes informaram que não têm esse hábito de emprestar seus equipamentos de trabalhos para terceiros, um número relativamente alto e esperado de respostas, representa uma boa prática de segurança, já 7,55% do total declararam emprestar às vezes, atitude essa que deve ser evitada. O empréstimo de equipamentos de trabalho indevidamente pode abrir brechas de segurança para as empresas e instituições tanto como prejudicar a privacidade dos funcionários.

Figura 24 - Empréstimo de equipamentos de trabalho para terceiros.

Emprestimo de equipamentos de trabalho para terceiros

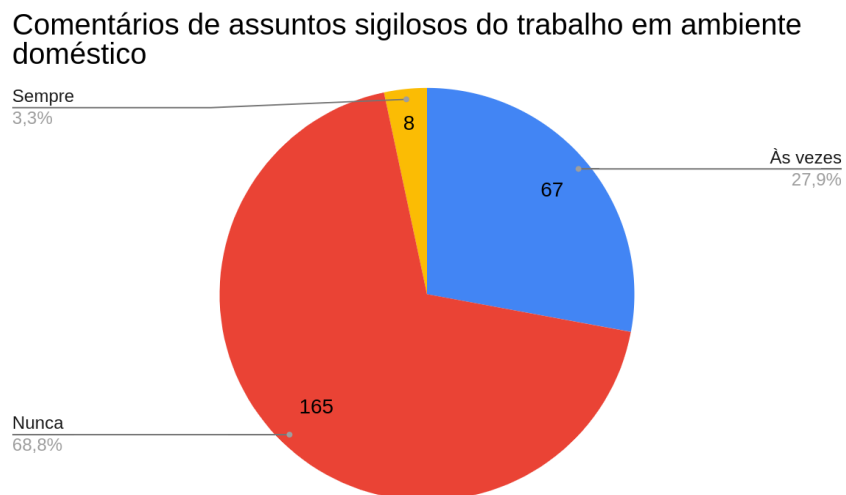


Fonte: Elaborada pelo autor (2023).

Pergunta 23 - Você comenta assuntos sigilosos relacionados ao seu trabalho no ambiente doméstico?

No contexto de teletrabalho as relações pessoais com as de trabalho podem se misturar em algum ponto, 68,8% dos participantes informaram que nunca comentam sobre assuntos sigilosos do trabalho no ambiente doméstico, 27,9% informaram que comentam às vezes e 3,3% declararam que sempre comentam, como mostra a figura 25. Se forem somadas as duas últimas parcelas, as duas equivalem a 31,2% do total de participantes, levando em conta o aspecto crítico dessa atitude, esses são números consideráveis.

Figura 25 - Costume de comentar assuntos sigilosos do trabalho em ambiente doméstico.



Fonte: Elaborada pelo autor (2023).

Pergunta 24 - Você participa de reuniões sem fones de ouvido mesmo quando há outras pessoas próximas?

No trabalho remoto é muito comum a realização de reuniões por videoconferência, e a depender do contexto, assuntos abordados nelas devem ser guardados em sigilo, por outro lado em um ambiente doméstico assuntos privados e pessoais muitas vezes não podem ser externados para terceiros fora do contexto domiciliar. Para isso, uma medida simples mas eficaz é o uso de fones de ouvido durante videoconferências e chamadas. Como pode ser visto na figura 26, 82,1% dos participantes responderam que nunca participam de reuniões remotas sem utilizar fones de ouvido, 14,2% declararam que às vezes não utilizam e 3,8% são os que sempre participam sem o uso de fones.

Figura 26 - Uso de fone de ouvido em reuniões.



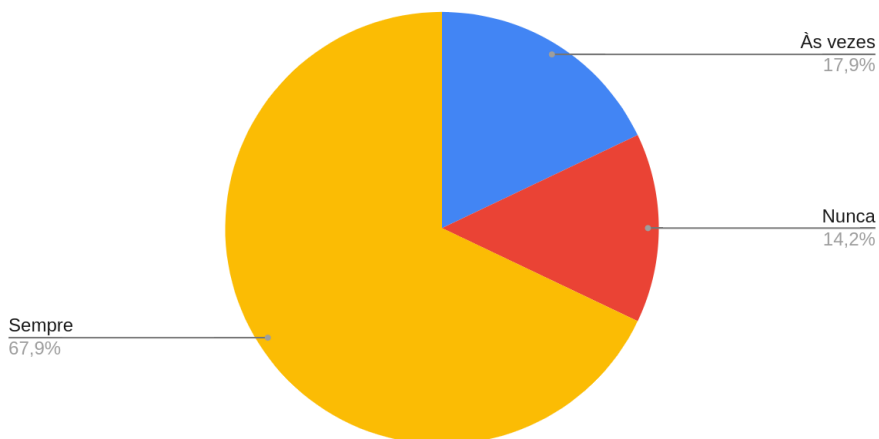
Fonte: Elaborada pelo autor (2023).

Pergunta 25 - Você costuma fechar a *Webcam* e o microfone dos seus equipamentos quando não está utilizando?

O uso de webcam e microfones para realização de reuniões remotas é muito comum, porém algumas medidas devem ser tomadas para evitar a exposição da privacidade dos usuários em seu ambiente privado. Para isso, uma medida simples é fechar a webcam e microfones quando eles não estiverem sendo utilizados. Cerca de 67,9% dos participantes responderam que sempre fecham os dispositivos quando não estão utilizando, 14,2% declararam que nunca fecham e 17,9% informaram que só fecham os dispositivos às vezes como pode ser conferido na figura 27.

Figura 27 - Costume de fechar a webcam e o microfone enquanto estão ociosos.

Costume de fechar a webcam e microfone quando estão ociosos



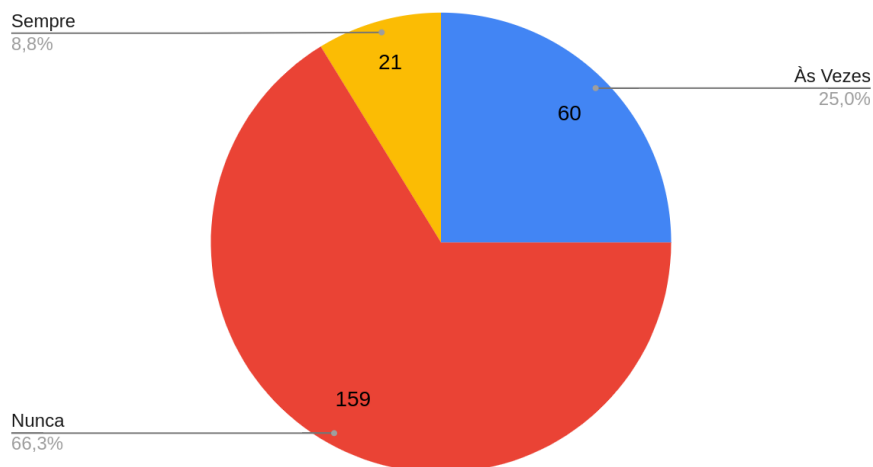
Fonte: Elaborada pelo autor (2023).

Pergunta 26 - Você costuma trafegar informações de trabalho em redes sociais como Facebook, WhatsApp, Instagram e outras?

Algumas empresas se utilizam das redes sociais como meio de comunicação oficial com clientes e também para comunicação interna entre colaboradores, nesses dois casos deve-se ter uma política bem definida para o uso consciente e seguro delas, pois trafegar as informações de forma indevida pelas redes sociais pode gerar insegurança para os dados das empresas e a privacidade dos seus colaboradores. Na figura 28 cerca de 66,3% dos participantes disseram que nunca trafegam dados do trabalho em redes sociais, 25,0% informaram que trafegam às vezes e 8,8% informaram que sempre trafegam.

Figura 28 - Costume de trafegar dados do trabalho em redes sociais.

Costume de trafegar dados em redes sociais



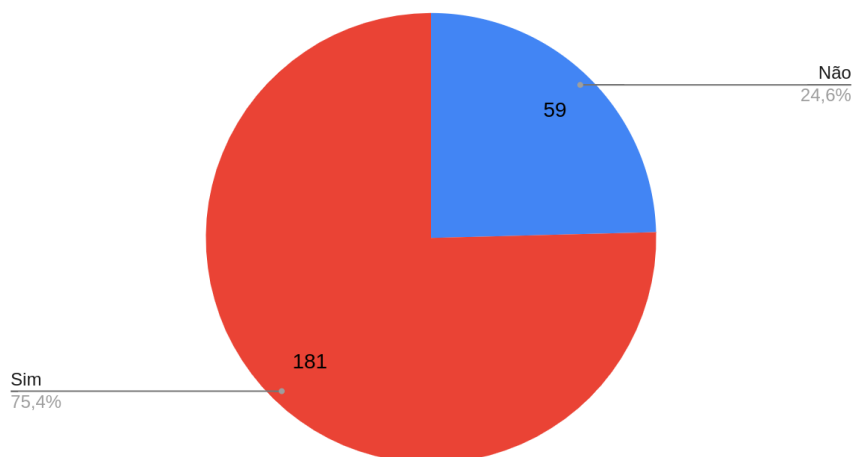
Fonte: Elaborada pelo autor (2023).

Pergunta 27 - Você já participou de treinamentos sobre segurança da informação?

Para que os colaboradores no seu ambiente de trabalho possam adotar medidas de segurança é muito importante que suas instituições onde eles atuam disseminem o conhecimento sobre os temas relacionados a segurança da informação, para isso é preciso investir em treinamentos e capacitação dos seus membros, como pode ser visto na figura 29 cerca de 75,4% dos participante responderam que já realizou treinamentos relacionados a segurança da informação, em contrapartida 24,6% dos participantes informaram que nunca realizaram treinamentos relacionados a esse tema, isso equivale a quase $\frac{1}{4}$ do público-alvo.

Figura 29 - Dados referentes à realização de treinamentos de segurança.

Realizou treinamento de segurança



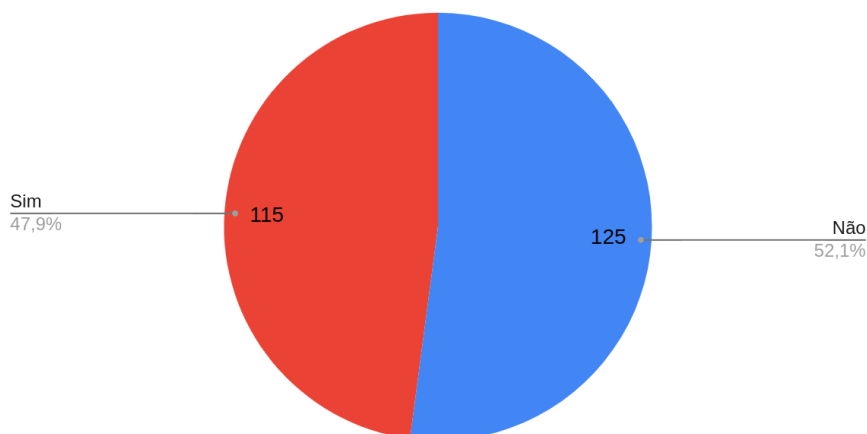
Fonte: Elaborada pelo autor (2023).

Pergunta 28 - Você foi instruído a tomar medidas de segurança específicas para trabalhar remotamente?

Levando em consideração o contexto de trabalho remoto, cerca de 52,1% dos participantes informaram que não receberam instruções sobre quais medidas e cuidados deveriam ser tomar relacionados à segurança da informação e outros 47,9% disseram que já receberam, mais detalhes sobre essa informação podem ser observados na figura 30.

Figura 30 - Dados sobre instruções de segurança específicas.

28 - Você foi instruído a tomar medidas de segurança específicas para trabalhar remotamente?



Fonte: Elaborada pelo autor (2023).

Pergunta 29 - Você foi instruído a tomar medidas de segurança específicas para trabalhar remotamente?

A pergunta 29 foi aberta, nela os participantes puderam compartilhar as instruções que eles receberam relacionadas a segurança da informação para serem adotadas no trabalho remoto. A seguir seguem algumas respostas coletas:

1. “Seguir orientações do manual da empresa que trata do assunto.”;
2. “Evitar conectar em redes públicas, acessar sites desconhecidos e não conectar equipamentos ao computador.”;
3. “Utilizar proteção de tela para pessoas próximas não poderem ver sua tela, usar um gerenciador de senhas, em caso de call usar fones.”;
4. “Não utilizar redes públicas e nem dispositivos compartilhados, utilizar senhas fortes e gerenciador de senhas, tomar cuidado com golpes de phishing.”;
5. “Evitar wifi's públicos, negar acesso ao computador corporativo a terceiros, sempre que suspeitar de um e-mail comunicar ao time responsável e sempre buscar fontes seguras para softwares.”;
6. “Bloqueio de equipamento de trabalho em casos de ausência, cuidados com acesso às redes, acessar portais sigilosos da empresa por VPN, apenas se

comunicar sobre os assuntos de trabalho pelos meios de comunicações oficiais da instituição.”

7. “Quando realizar algum processo interno, estar com a vpn ligada, acessar o site da empresa onde tem descrito quais softwares podem ser utilizados no computador do trabalho, e quando houver qualquer situação que pode ou gerou algum tipo de instabilidade ou vulnerabilidade da rede/recursos , entrar em contato com o suporte imediatamente.”
8. “Sempre encerrar minha sessão após término do trabalho, não compartilhar minha senha, limpar o cache, entre outras...”
9. “Criptografia disco, utilização 2fa e yubikey.”
10. “Instruções declaradas na PSI da empresa”
11. “Cuidados com redes públicas, credenciais, bloqueio de máquina, compartilhamento de informações através de Clouds(google drive, one drive e etc...).”
12. “Não deixar credenciais expostas, em post its por exemplo. Ter cuidado com fotos, para não expor informações da tela ou outros dados da empresa que estejam no ambiente.”

Nota-se que algumas instruções foram citadas na questão 29 foram abordadas em questões anteriores do questionário, como por exemplo: evitar o uso de redes públicas, bloquear equipamentos quando não estiverem sendo utilizados, se comunicar só pelos meios de comunicação oficiais da empresa e ler manuais de instruções da empresa referentes a medidas que devem ser adotadas.

4.4 Recursos providos pelas instituições e empresas aos seus funcionários

Esta subseção tem como objetivo mostrar os resultados sobre os dados relacionados aos recursos que as instituições e empresas fornecem aos seus funcionários para um trabalho remoto mais seguro.

30 - Esses recursos são providos pela a instituição onde você trabalha?

Como pode ser observado na tabela 9, grande parte de recursos essenciais para um trabalho seguro remotamente são providos pelas empresas, como por exemplo computador e notebook, onde cerca de 87,08% dos participantes informaram que suas instituições e empresas fornecem. Outro recurso importante para proteção dos dados, principalmente durante o trabalho remoto, é o uso de VPNs, 77,50% dos participantes informaram que eles têm disponível esse recurso. Já se for levado em consideração os itens que foram declarados que não são disponibilizados ou que os participantes não sabem se são foram: Telefone corporativo (77,08%), Sistemas de gerenciamento de senhas (42,08%) e antivírus (32,92%).

Tabela 9 - Recursos providos pelas instituições aos seus funcionários.

	Sim	Não	Não Sei
Computador ou notebook	87,08%	12,50%	0,42%
VPN	77,50%	20,83%	1,67%
Email Corporativo	92,50%	7,50%	0,00%
Telefone Corporativo	19,17%	77,08%	3,75%
Antivírus	62,08%	32,92%	5,00%
Sistema de gerenciamento de senhas	52,50%	42,08%	5,42%
Softwares Licenciados	83,75%	12,08%	4,17%
Suporte de TI remoto	73,75%	22,92%	3,33%
Treinamentos relacionados a segurança da informação	69,58%	27,50%	2,92%
Canal para tirar dúvidas e reportar incidentes relacionados a segurança	69,17%	25,83%	5,00%

dos dados			
SSO - Sistema de login único para todos os sistemas	53,33%	38,75%	7,92%

Fonte: Elaborada pelo autor (2023).

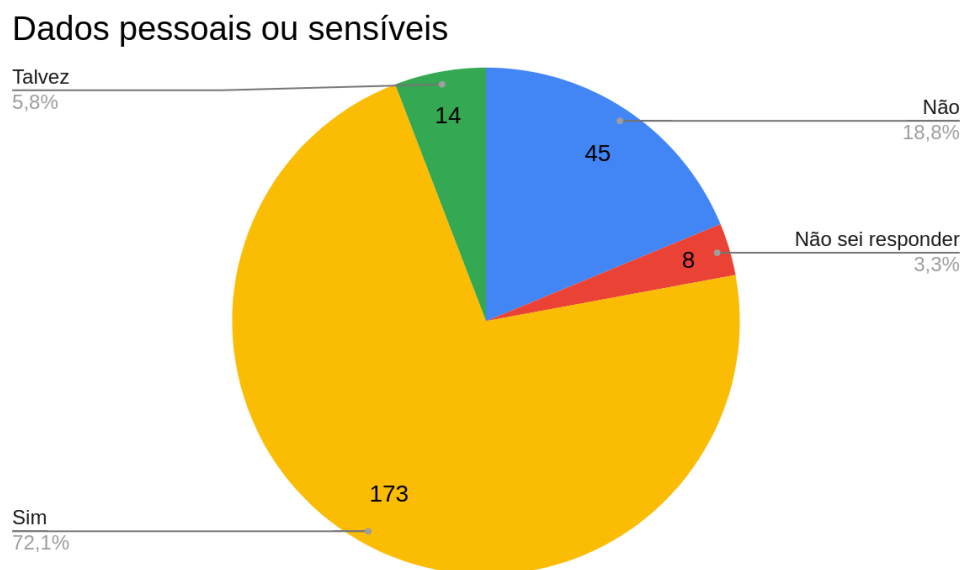
4.5 Nível de conhecimento sobre a importância de alguns tópicos relacionados a segurança e privacidade no trabalho remoto

Essa subseção busca apresentar dados relacionados ao nível de conhecimento dos participantes sobre determinados tópicos referentes à segurança da informação e ou também saber qual o nível de importância que os mesmos dão a cada um desses itens sejam boas práticas, conceitos ou adoção de algum recurso para proteção dos seus dados.

Pergunta 13 - “Você trabalha com dados pessoais ou sensíveis?”

O tratamento para alguns tipos de dados requer uma atenção maior, a forma como tratar dados pessoais e sensíveis inclusive é regido por leis como por exemplo a LGPD e GDPR. Na figura 31 é possível notar que cerca de 72,1% dos participantes trabalham com dados pessoais ou sensíveis, 18,8% disseram que não trabalham com esses tipos de dados, 5,8% estavam na dúvida se possivelmente eles trabalhavam e 3,3% não souberam responder.

Figura 31 - Conhecimento sobre dados pessoais ou sensíveis.



Fonte: Elaborada pelo autor (2023).

Pergunta 31 - "Em um grau de 1 a 5, qual o seu nível de conhecimento sobre a importância de cada um desses itens abaixo listados para a segurança e privacidade dos dados no seu ambiente de trabalho?"

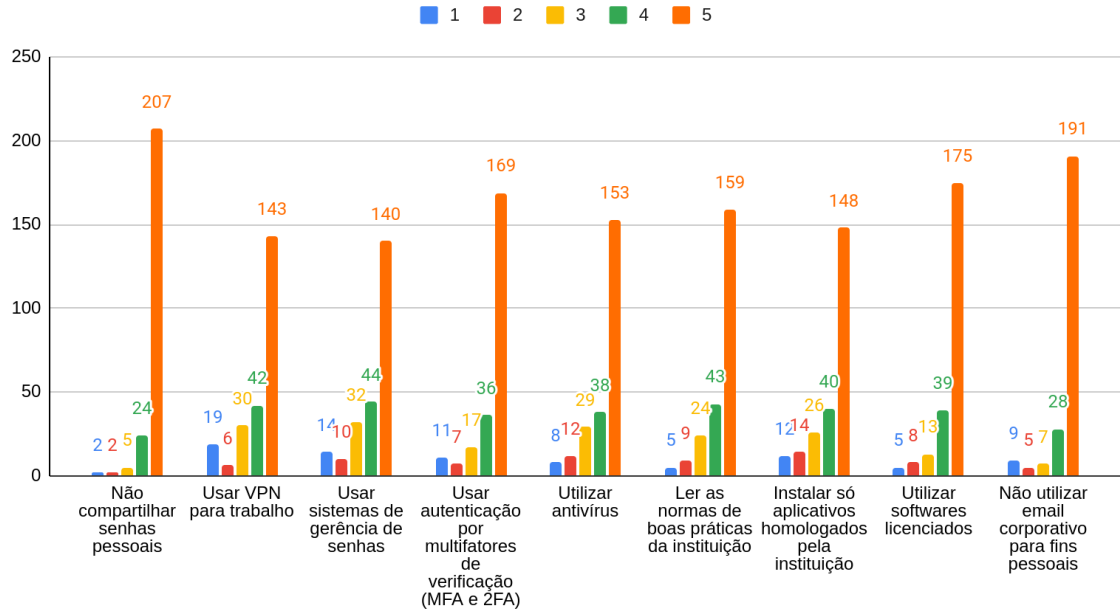
OBS:

- 1 significa que você não tem conhecimento algum;
- 5 significa que você tem total conhecimento sobre a importância daquele recurso."

Os dados representados na figura 32 ilustram bem o nível de importância dos participantes para os itens listados, no geral todos os itens receberam mais de 50% das respostas referente ao maior grau de importância que no caso foi definido como 5, desses se destacam como os três primeiros: Não compartilhar senhas pessoais (86,25%), não utilizar e-mail corporativo para fins pessoais (79,58%) e utilizar softwares licenciados (72,92%). Em relação aos dois menores graus somados, os três itens que mais receberam essas avaliações foram: Instalar só aplicativos homologados pela instituição (10,83%), usar VPN para trabalho (10,42)% e usar sistemas de gerenciamento de senhas (10%).

Figura 32 - Análise do nível de conhecimento sobre a importância dos itens citados na questão 31.

Nível de conhecimento e importância dos itens de segurança listados na questão 31



Fonte: Elaborada pelo autor (2023).

4.6 Discussão sobre os resultados

Esta subseção apresentará os pontos mais relevantes para pesquisa após a observação dos resultados presentes nas seções 4.2, 4.3, 4.4 e 4.5. Cada tópico será discutido separadamente.

Perfil do público-alvo

Com o objetivo de restringir quais indivíduos faziam parte do público-alvo, foram filtrados dos dados brutos só respostas de participantes que trabalham remotamente tanto no regime 100% remoto quanto no modelo híbrido, dentro desse grupo se observou que a maior parte eram compostos de jovens e adultos nas faixas entre 18 até 24 (26,7%) e de 25 até 34 anos (52,1%), levando em conta essa parcela da população representada na pesquisa cerca de 79,4% tinham como grau de instrução minimamente o nível superior. De acordo com o IPEA (Instituto de Pesquisas Econômicas), em um pesquisa Intitulada “Os condicionantes do Teletrabalho Potencial no Brasil” de 2023, a faixa etária que ocupa o maior número de vagas de teletrabalho com cerca de 70% das vagas no Brasil é a entre 20 a 49 anos, além disso nessa pesquisa também se verificou que pessoas que têm um nível de escolaridade maior são mais suscetíveis a alcançar essas vagas, onde foi observado que pelo menos 58,2% das vagas eram ocupadas por pessoas com pelo menos o ensino superior completo, dados esses que foram de certa forma representado neste trabalho do Instituto de Pesquisa Econômica Aplicada (IPEA) [67].

Outra característica observada foi que cerca de 81,3% do público-alvo tinham como área de formação a área de tecnologia e computação, sendo as outras áreas somadas correspondentes a cerca de 18,7% dos dados da pesquisa. Com números próximos em torno de 84,6% dos participantes declararam que atuam na área de tecnologia e computação. Essa abrangência de pessoas da área de tecnologia e computação na pesquisa pode ser explicada por dois fatores, o primeiro é relacionado aos lugares onde o questionário da pesquisa foi divulgado, como grupos em redes sociais que o pesquisador fazia parte e a divulgação no âmbito da própria universidade onde o pesquisador estuda, ou seja, o ciclo social do pesquisador pode ter sido um fator relevante para a incidência de muitos participantes que faziam parte do mesmo contexto de trabalho e área de formação.

Um outro aspecto que colabora com a incidência de tantas pessoas da área de tecnologia trabalhando remotamente é a flexibilidade que a área permite quanto a isso. Durante a pandemia houve um crescimento do número de vagas oferecidas neste regime, segundo uma pesquisa realizada pela Flexjobs, uma plataforma que divulga e facilita a busca por vagas com modelo de trabalho flexível, durante esse período, entre 2021 e 2022, houve um crescimento de cerca de 20% no número de vagas ofertadas para o modelo remoto e segundo esse levantamento para 2023 após o período pandêmico a área de TI é uma das que têm mais tendência de continuar adotando o modelo híbrido [46], essa perspectiva também foi divulgada pela InfoJobs para o primeiro semestre de 2023 no Brasil, destacando que a área com mais anúncios de vagas remotas para o primeiro semestre de 2023 foi a de tecnologia com cerca de 991 anúncios divulgados por eles, a InfoJobs é uma plataforma de divulgação de vagas de emprego [46][47].

Outro dado relevante para pesquisa é que a maior parte dos participantes atuam no setor privado correspondendo a cerca de 82,15% do público-alvo, tendo sido o setor mais representado na pesquisa. Cerca de 68,8% informaram que trabalham em instituições de grande porte com mais de 100 funcionários. E em relação ao tempo de trabalho dos participantes em suas respectivas instituições, cerca de 84,6% tinham até 5 anos de casa. Vale salientar que atividade econômica das empresas e instituições que teve maior número de respostas foi a de tecnologia (desenvolvimento de software, consultoria de TI e serviços de TI) com o total de 67,1% do total.

Das regiões globais definidas no questionário para as quais os participantes trabalham a que teve mais destaque foi a do Brasil com cerca de 89,58% das respostas, seguida da América do Norte (11,25%) e Europa (9,58%).

Nota-se que o grupo dentro do público-alvo da pesquisa que teve uma representação mais relevante foi o de jovens e adultos com um grau de instrução relativamente alto, que trabalham em instituições e empresas privadas de grande porte na área de tecnologia atuando principalmente no Brasil.

Comportamento dos participantes

O comportamento e atitudes das pessoas no ambiente de trabalho remoto são aspectos essenciais para a promoção de um ambiente seguro tanto para os dados das empresas e instituições como para a própria privacidade dos trabalhadores. O aspecto humano na

segurança da informação é o elo mais frágil de toda a cadeia, pois mesmo com a adoção de tecnologias avançadas de monitoramento, controle e proteção dos dados por parte das empresas, basta um usuário tomar alguma atitude negligente, para que brechas sejam abertas comprometendo a integridade, confiabilidade e disponibilidade dos dados. Outro ponto importante a se observar é que levar o trabalho para o ambiente doméstico é um cenário desafiador principalmente em relação a privacidade dos funcionários, pois diferentemente dos escritórios das empresas as residências carregam em si a vida privada de cada indivíduo, ou seja, outras pessoas externas ao trabalho podem estar envolvidas nesse ambiente e a individualidade e privacidade de cada um deveria estar protegida nele.

No trabalho remoto, o uso de dispositivos de informática e equipamentos móveis, como celulares, computadores e tablets, além do uso de softwares e aplicativos, é essencial para a comunicação e o desempenho dos colaboradores. É fundamental que o uso desses recursos seja feito de forma consciente, em conformidade com as normas e as boas práticas das empresas e instituições.

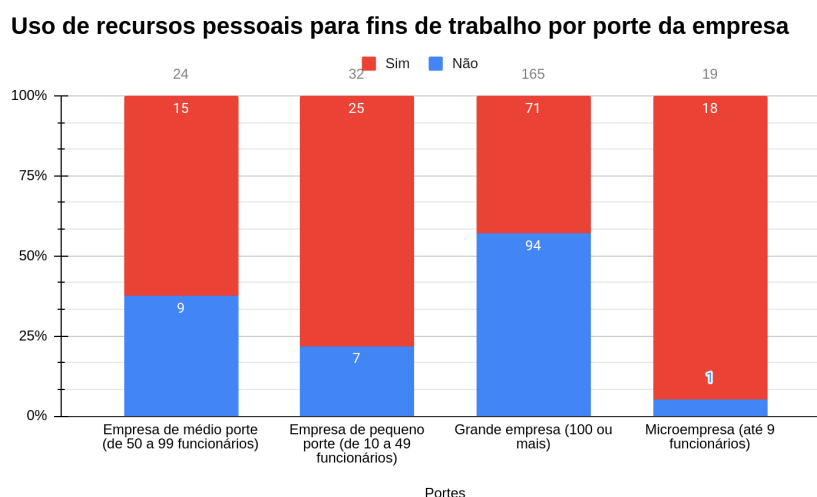
A maioria dos participantes informou que utiliza recursos pessoais para o trabalho (53,3%). Em contrapartida, 46,3% deles informaram que não o fazem. Embora a diferença entre essas duas parcelas seja pequena, ao analisar a distribuição desses dados por porte das empresas, nota-se algumas diferenças significativas. Nas microempresas, 94,7% dos participantes disseram que utilizam recursos pessoais, enquanto apenas 5,3% não o fazem. Em pequenas empresas, 78,1% responderam afirmativamente, enquanto 21,8% não o fazem. Nas empresas de médio porte, 62,5% utilizam recursos pessoais, enquanto 37,5% não o fazem. O único cenário em que a maioria dos participantes não utiliza recursos pessoais para o trabalho é nas empresas de grande porte, onde 57% não se utilizam desses tipos de recursos, enquanto 43,3% utilizam, como mostra a Figura 33.

O uso de recursos pessoais para o trabalho apresenta suas vantagens e desvantagens. As principais vantagens incluem mobilidade e comodidade para os funcionários, o que explica o alto número geral de participantes que adotam essa prática (53,3%). Outra vantagem é a redução de custos para as empresas, o que explica por que funcionários de micro, pequenas e médias empresas adotam essa prática em maior número, já que essas empresas geralmente possuem recursos financeiros limitados em comparação com empresas de grande porte.

Por outro lado, as maiores desvantagens do uso de recursos próprios para o trabalho incluem preocupações com a segurança dos dados, o controle sobre eles e a dificuldade de

separar a privacidade pessoal da vida profissional dos funcionários. Portanto, os resultados da pesquisa sugerem um cenário potencialmente mais inseguro tanto para os dados quanto para a privacidade dos participantes que trabalham em micro, pequenas e médias empresas.

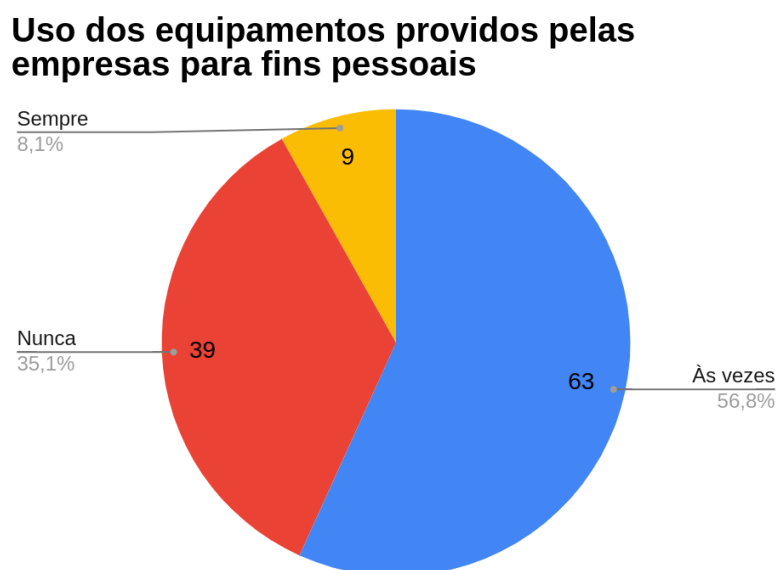
Figura 33 - Uso de recursos pessoais para fins de trabalho por porte da empresa



Fonte: Elaborada pelo autor (2023).

Outro dado relevante sobre o uso dos equipamentos de trabalho foi que cerca de 75,4% do total de participantes utilizam ao menos alguma vez eles para fins pessoais, se for desconsiderado os participantes que informaram se utilizar recursos próprios para trabalho, cerca de 64,9% utilizam ao menos uma vez equipamentos providos pelas empresas para fins pessoais como mostra a figura 34. Esse tipo de uso não é recomendável, mas geralmente não é proibido por muitas empresas, mas vale ressaltar que os funcionários devem ter atenção a política de uso de cada empresa, pois dependendo da situação os funcionários podem não estar em conformidade com as políticas, assim podendo abrir brechas de segurança devido ao uso indevido para esses fins.

Figura 34 - Uso dos equipamentos providos pelas empresas para fins pessoais



Fonte: Elaborada pelo autor (2023).

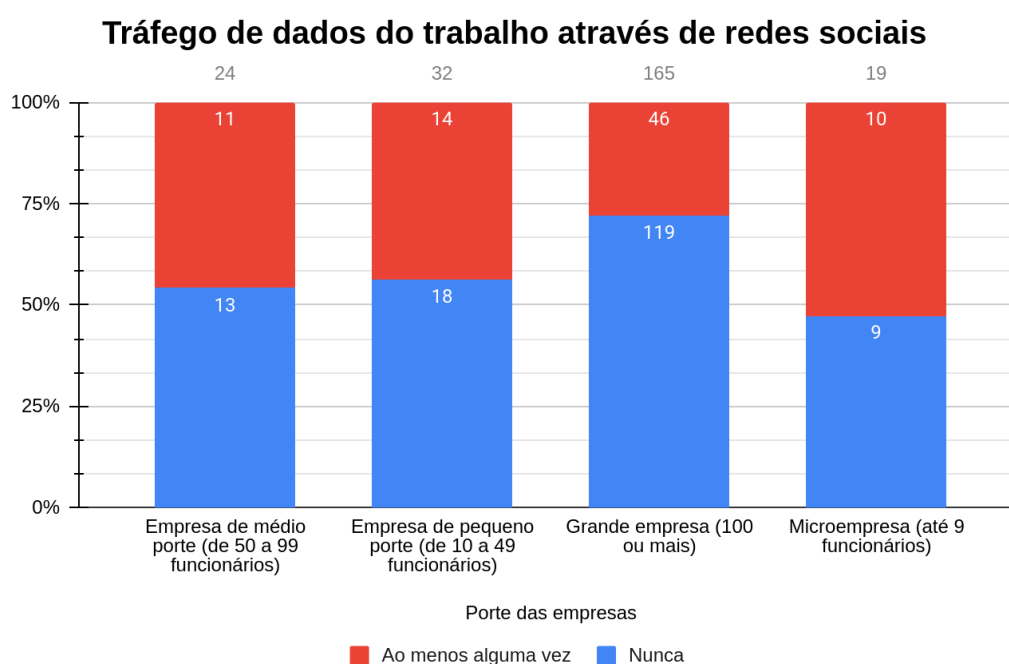
A maioria dos participantes mostraram ter alguns cuidados importantes quanto ao uso e tutela dos seus equipamentos, cerca de 92,5% deles declararam não emprestar seus equipamentos para terceiros, e 73,3% não utilizam eles em redes públicas de internet, essas medidas colaboram para que os dados armazenados nos dispositivos não sejam acessados por pessoas sem autorização, evitando também que esses equipamentos possam ser infectados por vírus e que os funcionários não tenham seus dados vazados por acessar sites falsos ou tenham seu tráfego de dados interceptado ou desviado por terceiros em redes inseguras.

Quanto ao cuidado com as credenciais de acesso aos sistemas, os resultados foram satisfatórios, os participantes demonstraram ter uma preocupação em manter suas identidades preservadas, onde a maioria (94,2%) informaram não compartilharem suas credenciais e cerca de 64,6% mantêm uma rotina periódica de troca de senhas. Num contexto de trabalho remoto onde o acesso a sistemas de informação faz parte do dia-a-dia das pessoas, medidas como essas asseguram o princípio da confidencialidade e irretratabilidade, dessa forma garantindo a autenticidade dos dados e a integridade dos mesmos.

Um dos pilares do trabalho remoto é o uso de ferramentas que colaboram para comunicação e colaboração entre os funcionários, equipes e no contato com clientes, para isso é importante utilizar ferramentas homologadas e oficiais das empresas e instituições, foi observado que os participantes que trabalhavam em empresas e instituições de grande porte em sua maioria (72,1%) não trafegam dados de trabalho através de redes sociais, isso pode ser explicado pela tendência de empresas maiores terem políticas de segurança mais rígidas quanto a isso se for comparado esse número com empresas de menores portes se observa uma diferença razoável nos números, a figura 35 ilustra a distribuição desses dados.

Embora o uso de redes sociais como meio de comunicação não seja algo incomum, deve-se priorizar o uso de ferramentas voltadas para negócios, pois o uso de redes sociais pode expor as as empresas e os funcionários a algumas vulnerabilidades já que a maior parte dessas redes como Facebook, Instagram, Twitter e outras são mais focadas para o uso pessoal.

Figura 35 - Tráfego de dados do trabalho através de redes sociais por porte das empresas e instituições.



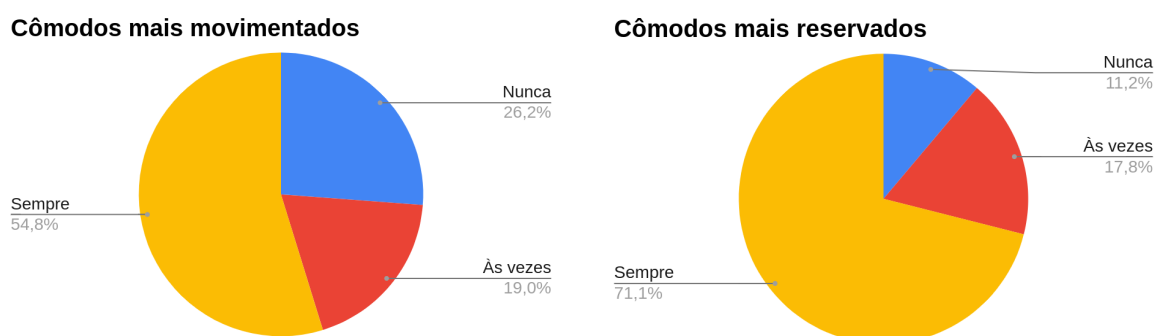
Fonte: Elaborada pelo autor (2023).

Sobre o ambiente de trabalho dos participantes em suas residências o resultados mostraram que a maioria (86,1%) prefere trabalhar em cômodos mais reservados, como quartos e escritórios, esses espaços são mais recomendados para o trabalho pois têm um

menor fluxo de pessoas e favorecem uma privacidade maior para os funcionários e para as outras pessoas da casa, além disso por ser lugares mais isolados, ao ter que tratar de assuntos mais sensíveis em reuniões o funcionário estará mais protegido quando ao vazamento de dados devido ao acesso de terceiros nesses cômodos ser menor em comparação a outros mais movimentados.

Uma análise foi realizada referente ao comportamento dos participantes em tipos de cômodos diferentes e foi observado que os participantes que preferem trabalhar em cômodos mais movimentados tem menos costume de fechar as câmeras e microfones se comparados com os que trabalham em cômodos mais reservados, como está demonstrado na figura 36. Esses dados são interessantes pois revelam que os que trabalham em cômodos mais movimentados podem estar expondo mais sua privacidade e de terceiros de sua casa se comparados ao outro grupo.

Figura 36 - Bloqueios de webcam e microfone ociosos em diferentes tipos de cômodos



Fonte: Elaborada pelo autor (2023).

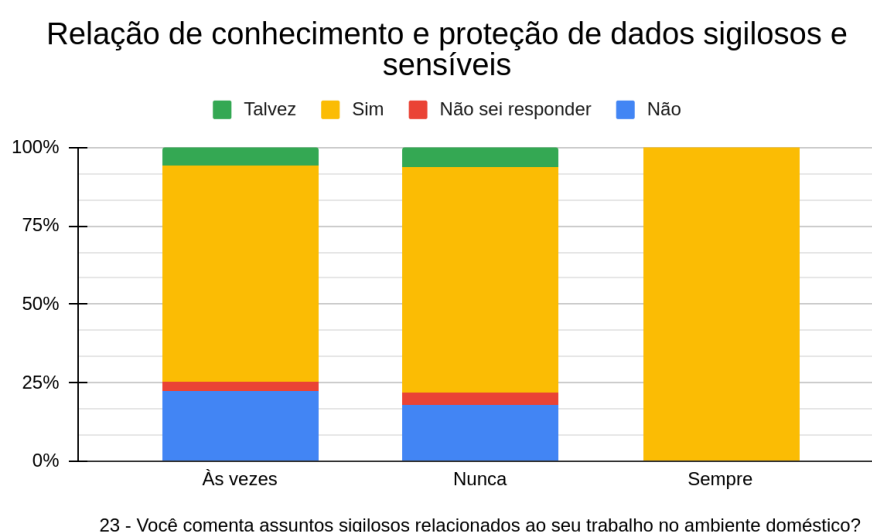
Cerca de 81,9% dos participantes declararam nunca participar de reuniões remotas sem usar fone, medida importante para evitar que pessoas sem a devida permissão alcancem dados e informações sigilosas do trabalho vazados em reuniões remotas.

Ainda em relação à proteção contra comprometimento e vazamento de dados, foi questionado se os participantes costumam comentar assuntos sigilosos do trabalho em ambiente doméstico e cerca de 68% afirmaram que nunca comentam e os outros 32% comentam ao menos uma vez. Um dado interessante é que se agrupados os participantes que informaram que não trabalham com dados sensíveis, não sabiam se trabalhavam ou informaram que talvez trabalhassem, observa-se que esse grupo corresponde a 31,4% das

peças que declaram comentar assunto sigilosos às vezes e a 27,9% dos que nunca comentam, 100% dos que sempre comentavam eram cientes dos tipos de dados que eles trabalhavam como se pode observar na figura 37.

Embora no geral os número de participantes que têm cuidado em não comentar sobre assuntos sigilosos em suas residências seja maior, é interessante observar que a maior parte dos que não têm esse cuidado podem ter ciência do risco relacionados a esse costume.

Figura 37 - Relação de conhecimento e proteção de dados sigilosos e sensíveis.

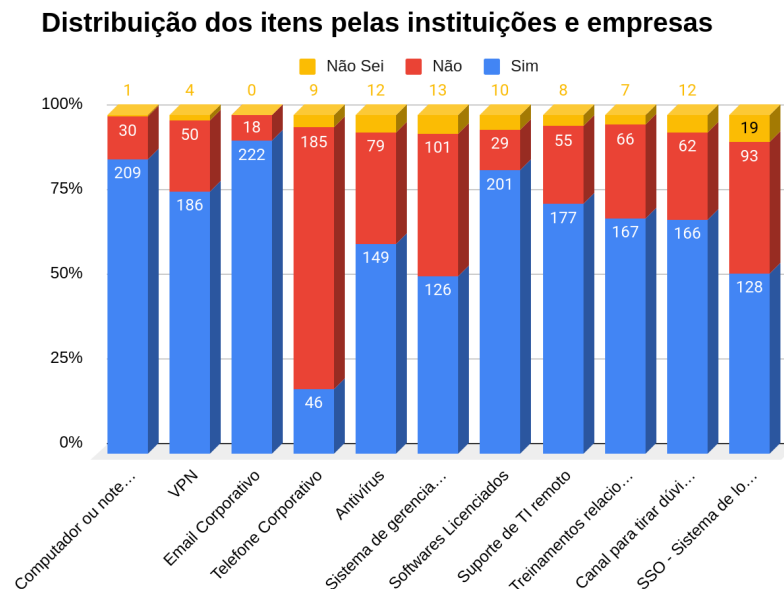


Fonte: Elaborado pelo autor (2023).

Recursos providos pelas instituições e empresas aos seus funcionários

Em relação aos recursos abordados na pesquisa, dos 11 listados 8 foram bem atendidos, dos três que tiveram um menor índice de provisão valem destacar sistema de gerenciamento de senhas, sistema de login único e telefone corporativo. Os dois primeiros itens citados anteriormente são mais relacionados à questão da proteção da identidade dos usuários, e o último está mais relacionado com o aspecto da privacidade, já que em casos onde as empresas não proveem o telefone corporativo, muitas vezes os funcionários se utilizam de seus telefones pessoais para fins de trabalho. Vale ressaltar que embora o item de antivírus tenha conseguido atingir um índice de provisão razoável, é interessante observar que 37% dos participantes informaram não receber esse recurso ou não sabem se suas instituições fornecem como se observa na figura 38.

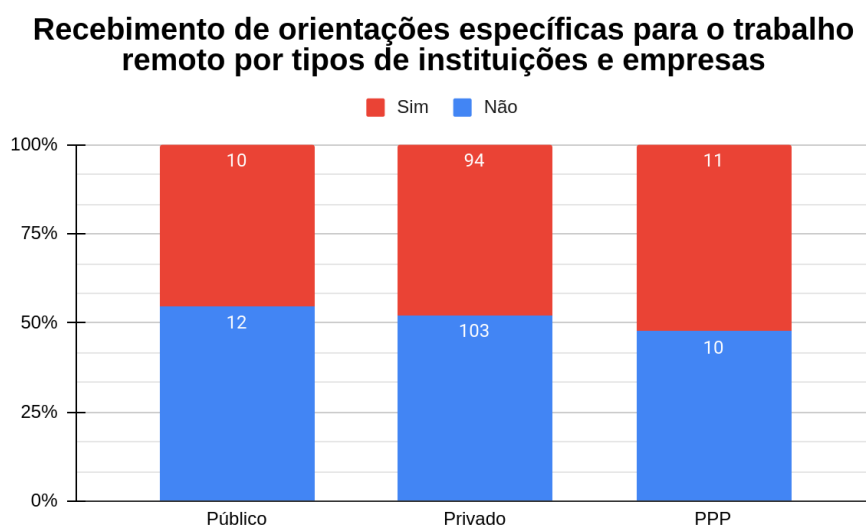
Figura 38 - Distribuição dos itens pelas instituições e empresas



Fonte: Elaborado pelo autor (2023).

Em relação a disseminação de orientações específicas por parte das empresas aos seus funcionários para o trabalho remoto, os resultados mostraram um cenário de quase meio a meio, se for levado em consideração a importância desse tópico, o cenário pode ser considerado não favorável já que isso é uma medida essencial para que os funcionários tenham ciência de quais medidas devem ser tomadas para a sua proteção e proteção dos dados das empresas. A figura 39 mostra a distribuição equilibrada das respostas para setores diferentes das instituições e empresas.

Figura 39 - Relação de disseminação de orientações específicas para o trabalho remoto



Fonte: Elaborado pelo autor (2023).

Nível de conhecimento sobre a importância de alguns tópicos relacionados a segurança e privacidade no trabalho remoto

Os resultados mostraram que a maior parte dos participantes consideram os 9 itens listados no questionário na pergunta 31 como muito importantes para a manutenção de um ambiente mais seguro para o teletrabalho, alguns itens valem ser destacados por serem bastante utilizados nesse ambiente, são eles: VPN com 58,33% dos participantes que declararam o maior grau de importância para esse item; utilização de softwares licenciados com 72,5% do maior grau de importância, esse último item é de suma importância para manter as empresas em conformidade com a lei e também assegurar a proteção dos seus dados já que softwares licenciados são menos vulneráveis a questões de segurança; não utilização de email corporativo para fins pessoais teve 79,58% das respostas para o maior grau de importância, esse item está relacionado ao de uso de recursos providos pelas instituições aos seus funcionários, e sendo um meio oficial de comunicação das empresas a boa prática é não misturar informações pessoais com de trabalho, principalmente para salvaguardar a identidade do funcionário.

5. Conclusões finais e trabalhos futuros

O conceito de trabalho remoto não é recente; no entanto, nos últimos tempos, com os avanços nas tecnologias da informação e comunicação, juntamente com fatores externos como a pandemia de Covid-19, muitas empresas sentiram a necessidade de expandir seus negócios e atender a públicos diversos. Isso impulsionou a busca por um modelo de trabalho mais flexível e viável, permitindo que as pessoas trabalhassem em casa ou em locais distantes dos escritórios. Esse modelo de trabalho tem se tornado cada vez mais difundido por instituições, empresas e trabalhadores.

No entanto, apesar dos benefícios que esse modelo de trabalho oferece, como flexibilidade e comodidade para os funcionários, bem como economia na manutenção dos escritórios, ele também traz consigo desafios, sendo um dos principais relacionado à segurança da informação e à privacidade. Atualmente, a segurança da informação é um aspecto crucial para as empresas, pois qualquer problema relacionado ao comprometimento dos dados de seus clientes e funcionários pode resultar em prejuízos financeiros e problemas jurídicos, devido às leis de proteção de dados vigentes em todo o mundo. Portanto, é fundamental encontrar maneiras de garantir a proteção dos dados das empresas e instituições, ao mesmo tempo em que se preserva a privacidade dos funcionários, especialmente em seus ambientes domésticos.

O primeiro passo para avaliar se o ambiente de trabalho remoto é seguro ou não é compreender o comportamento e as medidas adotadas pelos funcionários em seus ambientes de trabalho remotos e verificar quais recursos são disponibilizados pelas empresas e instituições às quais eles pertencem.

Este estudo tem como objetivo contribuir para a análise desse ambiente, coletando dados por meio de uma pesquisa *survey*. Os dados coletados foram analisados com o propósito de obter *insights* para a obtenção das conclusões sobre os resultados. Nas próximas seções, serão abordadas as conclusões finais, algumas contribuições e sugestões de trabalhos futuros.

5.1 Conclusões

A pesquisa teve como público alvo pessoas que trabalhavam no regime de trabalho 100% remoto ou híbrido, após o tratamento e filtragem dos dados brutos se chegou a um número de 240 respostas de participantes que faziam parte do público da pesquisa. Foi possível notar que maior parte deles eram jovens e adultos com um grau de instrução elevado, e em sua maioria eram formados e trabalham na área de TI o que trouxe a expectativa de um cenário um pouco mais favorável em relação a segurança da informação já que em tese esse grupo está mais próximo das questões relativas a essa temática.

No geral notou que a maior parte dos participantes tinham ciência da importância do uso de alguns recursos e ferramentas para a proteção dos seus dados como o uso de VPN, utilização de antivírus, uso de softwares licenciados, sistemas e gerenciamento de senhas, entre outros. Em relação a esses recursos a maior parte deles foram declarados pelos participantes como fornecidos pelas empresas e instituições, porém vale ressaltar que alguns deles tiveram um índice de não fornecimento um pouco maior, como por exemplo, telefone corporativos com o maior índice (77,08%), recurso esse que muitas empresas não oferecem aos seus funcionários e geralmente esses acabam utilizando seus telefones pessoais para fins de trabalho, uma prática que pode comprometer a privacidade dessas pessoas, esse número pode ter contribuído para os números referentes ao uso de recursos pessoais para fins de trabalho onde a maioria respondeu que sim (53,8%).

Outros dois recursos que tiveram um índice de não fornecimento um pouco maior em relação a outros foram sistemas de gerenciamento de senhas (42,08%) e sistemas de autenticação única (SSO) (38,7%), esses dois últimos itens são de grande importância para a proteção da identidade dos funcionários e controle de permissões por parte das empresas, em contrapartida a maior parte dos usuários demonstraram ter um cuidado maior em relação as suas credenciais pois o números mostraram que a maioria dos participantes não compartilham suas senhas com terceiros (94,2%) e cerca de 64,% têm o costume de trocar suas senhas periodicamente essas duas medidas positivas podem contribuir e em partes para compensar algumas lacunas referentes a falta de provisão de ferramentas próprias para essa finalidade e nos casos onde elas são providas sugere uma possível uso e adoção por parte dos funcionários.

Ao analisar os comportamentos dos participantes, foi observado uma boa adoção em relação à maior parte das boas práticas abordadas na pesquisa, grande parte delas estavam

relacionadas a proteção dos dados e cuidados com uso dos seus equipamentos, porém em algumas situações específicas se observaram números consideráveis ligados a alguns descuidos principalmente em relação a privacidade dos próprios funcionários como por exemplo, quando os funcionários trabalham em cômodos das suas residências com mais movimentação, embora 54,8% disseram ter o cuidado de fechar a câmera e microfone de seus computadores nesses lugares cerca de 45,2% deles não tinham toda essa preocupação, sendo considerado um número expressivo, grande parte deles também declararam utilizar recursos próprios e usar equipamentos providos por suas empresas para fins pessoais.

Um outro dado interessante é que 75,4% dos participantes informaram já ter realizado treinamentos de segurança da informação porém quase metade (47,9%) declararam que suas empresas e instituições não os instruíram a tomarem medidas específicas para o trabalho remoto, esses podem sugerir que o conhecimento em relação a boas práticas adotadas pelos funcionários podem terem sido obtidos pelos próprios funcionários, onde quem deveria estar mais preocupado em tomar a frente disso eram as próprias empresas e instituições.

Em termos gerais os resultados demonstraram um cenário relativamente positivo pois a maior parte dos participantes adotaram grande parte das boas práticas abordadas na pesquisa, porém existem ainda lacunas a serem trabalhadas, principalmente relacionadas ao aspecto da privacidade dos funcionários no ambiente de trabalho domésticos, pois os resultados demonstraram uma preocupação positiva deles referente a proteção dos dados relacionados aos seus trabalhos porém alguns atitudes e práticas sugeriram um certo descuido em relação privacidade e individualidade deles no ambiente de trabalho remoto.

Em relação às empresas e instituições a maior parte delas forneceram grande parte dos recursos necessários para um trabalho seguro por parte dos funcionários, porém em relação a disseminação do conhecimento notou-se uma relativa omissão, pois um número expressivo de funcionários declararam não receber instruções específicas para o trabalho remoto, e nesses cenário desafiador para o controle dos dados e proteção deles as empresas deveriam ter um cuidado maior com a capacitação dos seus funcionários.

Mesmo com pesquisa apontando um cenário relativamente favorável nota-se muitas lacunas principalmente em relação a questões de privacidade dos funcionários, é necessário que as empresas trabalhem mais na disseminação do conhecimento sobre a temática de segurança da informação e privacidade e também que elas não só trabalhem sobre os cuidados em relação a proteção dos seus dados mas que também tenham um zelo em relação a

preservação a individualidade e privacidade dos seus funcionários nos seus contextos privados.

Sobre os funcionários é muito importante que eles se engajem em uma cultura de segurança de informação, que busquem seguir as medidas de segurança recomendadas pelas suas empresas e que se utilizem dos recursos e ferramentas fornecidos por elas. É importante mencionar que as pessoas também devem ter uma atenção especial na separação da vida pessoal, da profissional, pois no contexto do teletrabalho muitas vezes elas se misturam sendo um dos grandes desafios para preservação da privacidade das pessoas nesse contexto.

5.2 Contribuições do trabalho

A seguir estão algumas das contribuições deste trabalho:

- Uma investigação de um cenário mais atual de segurança da informação e privacidade no ambiente de trabalho remoto, baseando-se em pesquisas pré-existentes de assuntos correlacionados citados na seção 1.3;
- Elaboração de um mecanismo de avaliação, questionário, para a coleta de dados necessários para a compreensão do cenário atual de trabalho remoto, abordando questões práticas e objetivas;
- Aplicação do questionário como mecanismo de avaliação que ficou disponível por quase 1 ano para a coleta dos dados com objetivo de aglutinar o maior número de dados possível;
- Caracterização do contexto atual de segurança da informação e privacidade dos dados a partir dos dados coletados, percebendo um cenário relativamente positivo porém com algumas lacunas ainda existentes a serem trabalhadas como a privacidade dos funcionários e a necessidade de uma melhor disseminação de informação sobre medidas específicas de segurança para o contexto de trabalho remoto.

5.3 Trabalhos futuros

Como sugestões de possíveis novos passos para melhoria ou compreensão mais apurada em determinados cenários, seguem algumas sugestões:

- Forçar em captar mais dados sobre participantes que não fazem parte do contexto de tecnologia, já que esta pesquisa teve majoritariamente a participação de pessoas dessa área;
- Promover uma pesquisa direcionada para as empresas, ou seja, captando as informações do lado delas, já que este trabalho teve foco no lado dos funcionários obtendo os dados sobre elas a partir deles;
- Divulgar a pesquisa em outros países, pois embora a pesquisa tenha recebido respostas de pessoas que trabalham para outras regiões globais, em sua maioria elas trabalhavam alocadas no Brasil;
- Desenvolver e aplicar a pesquisa restringida a funcionários de empresas de segmentos de atuação específicos, como indústria, saúde, consultoria, entre outras.

REFERÊNCIAS

- [1] TELETRABALHO traz economia de quase R\$ 1,5 bilhão aos cofres públicos. Brasil: Ministério da Economia, 16 ago. 2021. Disponível em: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/08/teletrabalho-tra-z-economia-de-quase-r-1-5-bilhao-aos-cofres-publicos>. Acesso em: 20 jun. 2023.
- [2] TRABALHADORES em home office se sentem mais felizes do que no modelo presencial. Brasil, 12 mar. 2022. Disponível em: <https://mercadoeconsumo.com.br/14/03/2022/destaque-do-dia/trabalhadores-em-home-office-se-sentem-mais-felizes/>. Acesso em: 19 jul. 2023.
- [3] O ABISMO digital no Brasil. Brasil: PWC Brasil, 12 mar. 2022. Disponível em: <https://www.pwc.com.br/pt/estudos/preocupacoes-ceos/mais-temas/2022/o-abismo-digital-no-brasil.html>. Acesso em: 4 jul. 2023.
- [4] BURGUESS, Andrea. Working from Home Increases Cyberattack Frequency by 238%. [S. l.]: Alliance Virtual Office, 12 mar. 2022. Disponível em: <https://www.alliancevirtualoffices.com/virtual-office-blog/remote-work-statistics-costs/>. Acesso em: 29 set. 2023
- [5] LIMA, Kaique. Ataque de phishing crescem quase 230% no Brasil no primeiro semestre de 2022. Brasil, 3 set. 2022. Disponível em: <https://canaltech.com.br/seguranca/ataque-de-phishing-crescem-quase-230-no-brasil-no-primeiro-semester-de-2022-226637/>. Acesso em: 13 set. 2023.
- [6] SANTOS, Pedro Vinícius de Lima. Avaliação da Cultura de Segurança da Informação: A Aplicação de um Survey sobre Cultura de Segurança da Informação nas Organizações. 2020. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Universidade Federal de Pernambuco, Recife.
- [7] GEORGIADOU, A., MOUZAKITIS, S., & ASKOUNIS, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 35(2),

486-505. Disponível em: <https://doi.org/10.1057/s41284-021-00286-2>. Acesso em: 26 jul. 2023.

[8] FERNANDES, Maria Luiza Azevedo *et al.* TELETRABALHO: Análise da jurisprudência como fonte integradora do direito. *Teletrabalho*, [S. l.], p. 212-226, 8 ago. 2022. DOI <https://doi.org/10.5752/P.1678-3425.2022v7n12p212-226>. Disponível em: <http://periodicos.pucminas.br/index.php/virtuajus/article/view/28731>. Acesso em: 20 jul. 2023

[9] DA ROCHA, Cháris Telles Martins *et al.* O teletrabalho: conceituação e questões para análise. *FGV Cadernos EBAPE*, [S. l.], p. 152-162, 1 jan. 2018. DOI <https://doi.org/10.1590/1679-395154516>. Disponível em: <https://www.scielo.br/j/cebape/a/xdbDYsyFztnLT5CVwpXGm3g/?lang=pt#>. Acesso em: 20 jul. 2023.

[10] DA SILVA, Andréia Ana Paula *et al.* Teletrabalho: Origem, conceito, fundamentação legal e seus desafios. *In: Teletrabalho: Origem, conceito, fundamentação legal e seus desafios*. [S. l.], 14 abr. 2020. Disponível em: https://jus.com.br/artigos/81185/teletrabalho-origem-conceito-fundamentacao-legal-e-seus-desafios#google_vignette. Acesso em: 20 jul. 2023.

[11] ALLEN, Nathan *et al.* The Pioneers of Modern Remote Work. *In: The Pioneers of Modern Remote Work*. [S. l.], 10 nov. 2020. Disponível em: *The Pioneers of Modern Remote Work*. Acesso em: 20 jul. 2023.

[12] HADDON, Leslie; LEWIS, Alan. The experience of teleworking: an annotated review. *The International Journal of Human Resource Management*, [s. l.], 24 maio 2006. DOI <https://doi.org/10.1080/09585199400000010>. Disponível em: <https://www.tandfonline.com/doi/epdf/10.1080/09585199400000010?needAccess=true>. Acesso em: 20 jul. 2023.

[13] VEBBER, Thailini *et al.* IMPACTOS DO TELETRABALHO NA SAÚDE MENTAL DO TRABALHADOR. Revista sobre Excelência em Gestão e Qualidade, [s. l.], 24 maio 2006. DOI <https://doi.org/10.47591/RAC.2674-9203.2021v3n2.art1-1-17>. Disponível em: <http://www.fismaead.edu.br/seer/index.php/jemq/article/view/35>. Acesso em: 20 jul. 2023.

[14] DA SILVA PERNA, José Luiz *et al.* O trabalho híbrido: remoto e presencial, em uma instituição pública de ensino durante a pandemia da Covid-19 - um estudo de caso. Brazilian Journal of Development, [s. l.], 20 ago. 2021. DOI DOI:10.34117/bjdv7n8-499. Disponível em: <http://www.cp2.g12.br/blog/humaitaii/files/2021/08/Artigo-Jos%C3%A9-Luiz.pdf>. Acesso em: 21 jul. 2023.

[15] DE ARAÚJO, Tânia Maria *et al.* O trabalho mudou-se para casa: trabalho remoto no contexto da pandemia de COVID-19. Revista Brasileira de Saúde Ocupacional, [s. l.], 21 jul. 2023. DOI <https://doi.org/10.1590/2317-6369000030720>. Disponível em: O trabalho mudou-se para casa: trabalho remoto no contexto da pandemia de COVID-19. Acesso em: 21 jul. 2023.

[16] MELLO, Daniel *et al.* Home office foi adotado por 46% das empresas durante a pandemia. In: MELLO, Daniel *et al.* Home office foi adotado por 46% das empresas durante a pandemia. Agencia Brasil - EBC, 28 jul. 2023. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia>. Acesso em: 21 jul. 2023.

[17] ALFAGEME, Ana *et al.* O sonho do ‘home office’ vira pesadelo na pandemia. In: ALFAGEME, Ana *et al.* O sonho do ‘home office’ vira pesadelo na pandemia. El País, 9 ago. 2020. Disponível em: <https://brasil.elpais.com/sociedade/2020-08-09/o-teletrabalho-nao-era-isto.html>. Acesso em: 21 jul. 2023.

[18] EMPRESAS devem voltar ao trabalho presencial em 2022. In: Empresas devem voltar ao trabalho presencial em 2022. [S. l.], 28 abr. 2022. Disponível em:

<https://kpmg.com/br/pt/home/insights/2021/09/trabalho-presencial-home-office.html>. Acesso em: 21 jul. 2023.

[19] GRANATO, Luísa *et al.* Para 78% dos brasileiros, pandemia revelou urgência por trabalho flexível. *In: Para 78% dos brasileiros, pandemia revelou urgência por trabalho flexível.* [S. l.], 28 abr. 2022. Disponível em: <https://exame.com/carreira/para-78-dos-brasileiros-pandemia-revelou-urgencia-por-trabalho-flexivel/>. Acesso em: 21 jul. 2023.

[20] AMORIM, Gabriel *et al.* BYOD, pandemia e conscientização das equipes. [S. l.], 19 jul. 2021. Disponível em: <https://itforum.com.br/noticias/byod-pandemia-e-conscientizacao-das-equipes/>. Acesso em: 21 jul. 2023.

[21] Blizzard, Sonia. "Coming full circle: are there benefits to BYOD?" *Computer Fraud & Security*, Volume 2015, Issue 2, 2015, DOI <https://doi.org/10.1590/2317-6369000030720>, Pages 18-20, ISSN 1361-3723.

[22] Eschelbeck, Gerhard; Schwartzberg, David. "BYOD risks and rewards." *How to keep employee smartphones, laptops and tablets secure.* 2013. Disponível em: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=byod+risks&btnG=&oq=BYOD+ris. Acesso em: 21 jul. 2023.

[23] ROMER, Hormazd. Best practices for BYOD security. *Computer Fraud & Security*, Volume 2014, Issue 1, 2014, DOI [https://doi.org/10.1016/S1361-3723\(14\)70007-7](https://doi.org/10.1016/S1361-3723(14)70007-7), Pages 13-15, ISSN 1361-3723. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1361372314700077>. Acesso em: 20 jul. 2023.

[24] MCGUGAN, Patrick *et al.* To BYOD or not to BYOD. [S. l.], 3 nov. 2022. Disponível em: <https://www.myarg.com/to-byod-or-not-to-byod/>. Acesso em: 21 jul. 2023.

[25] HORMAZABAL, Renato *et al.* Segurança da Informação vs Privacidade dos Dados vs Proteção de Dados. [S. l.], 5 out. 2020. Disponível em: <https://www.linkedin.com/pulse/seguran%C3%A7a-da-informa%C3%A7%C3%A3o-vs-privacidade-dos-dados-de-renato-hormazabal/?originalSubdomain=pt>. Acesso em: 21 jul. 2023.

[26] 67% dos funcionários não receberam orientações de cibersegurança para o trabalho remoto. [S. l.], 7 maio 2020. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_67-dos-funcion-rios-n-o-receberam-orienta-es-de-ciberseguran-a-para-o-trabalho-remoto. Acesso em: 21 jul. 2023.

[27] DEMARTINI, Felipe *et al.* 67% dos funcionários não receberam orientações de cibersegurança para o trabalho remoto. [S. l.], 18 mar. 2021. Disponível em: <https://canaltech.com.br/seguranca/ciberataques-crescem-50-durante-a-migracao-para-home-office-na-pandemia-180898/>. Acesso em: 21 jul. 2023.

[28] PAN, Millena *et al.* Dados pessoais: reclamação por uso indevido mais que dobra no ano. [S. l.], 12 ago. 2021. Disponível em: <https://www.bancopan.com.br/blog/publicacoes/uso-de-dados-pessoais-sem-autorizacao-cresce-122.htm>. Acesso em: 21 jul. 2023.

[29] DONEDA, D. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 21 jul. 2023.

[30] Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd>. Acesso em: 21 jul. 2023.

[31] Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: <https://www.cgi.br/lei-do-marco-civil-da-internet-no-brasil/>. Acesso em: 21 jul. 2023.

[32] Brasil. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 21 jul. 2023.

[33] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia, Luxemburgo, 4 mai. 2016. Disponível em: <https://gdpr-info.eu/>. Acesso em: 21 jul. 2023.

[34] Coelho, C. F., Rasma, E. T., & Morales, G. (2013). Engenharia social: uma ameaça à sociedade da informação. *Exatas & Engenharias*, 3(5), 87-96. DOI: 10.25242/885X305201387. Disponível em: <https://doi.org/10.25242/885X305201387>. Acesso em: 21 jul. 2023.

[35] CORSINI, Iuri. Home office aumenta riscos de ataques virtuais; Brasil é um dos principais alvos. Brasil, 8 dez. 2020. Disponível em: <https://www.cnnbrasil.com.br/economia/home-office-aumenta-riscos-de-ataques-virtuais-brasil-e-um-dos-principais-alvos/>. Acesso em: 11 jul. 2023.

[36] PIOVESAN, Leonardo Gubert *et al.* ENGENHARIA SOCIAL: Uma abordagem sobre Phishing. *Revista Científica Faculdade de Balsas*, [S. l.], ano 2019, v. 10, n. 1, p. 45-59, 12 ago. 2021. DOI <https://doi.org/10.46761/unibalsas.v10i1.94>. Disponível em: <http://34.132.243.117/index.php/unibalsas/article/view/94>. Acesso em: 21 jul. 2023.

[37] AGUILAR, Ricardo *et al.* A IMPORTÂNCIA DOS TREINAMENTOS E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO. [S. l.], 12 set. 2022. Disponível em:

<https://www.auditsafe.com.br/a-importancia-dos-treinamentos-e-conscientizacao-em-seguranca-da-informacao/>. Acesso em: 21 jul. 2023.

[38] PEREIRA, Nicholas de Lucas Bastos *et al.* RANSOMWARE E PHISHING DURANTE A PANDEMIA DE COVID-19. Revista Tecnológica da Fatec Americana, [s. l.], v. 9, n. 1, 2021. DOI 10.47283/244670492021090167. Disponível em: <https://www.fatec.edu.br/revista/index.php/RTecFatecAM/article/view/256/231>. Acesso em: 21 jul. 2023.

[39] SAILPOINT and Proofpoint Team Up to Fight Security Threats Facing Today's Digital Workforce. In: SailPoint and Proofpoint Team Up to Fight Security Threats Facing Today's Digital Workforce. [S. l.], 4 ago. 2020. Disponível em: <https://www.proofpoint.com/us/newsroom/press-releases/sailpoint-and-proofpoint-team-fight-security-threats-facing-todays-digital>. Acesso em: 21 jul. 2023.

[40] KASUNIC, Mark. Designing an Effective Survey. Setembro de 2005. Disponível em: https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14435.pdf. Acesso em: 01 de setembro de 2023.

[41] WAINER, Jacques. Métodos de pesquisa quantitativa e qualitativa para a Ciência da computação. JAI 2007 -Jornada de Atualização em Informática, Anais do XXVII Congresso da Sociedade Brasileira de Computação. Disponível em: https://www.ic.unicamp.br/~wainer/cursos/1s2018/metodologia/Metodos_de_pesquisa_quantitativa_e_qualitativa_par.pdf. Acesso em 20 de setembro de 2023.

[42] LIMA, Vagner Carlos Marcolino; SECA NETO, Adolfo Gustavo Serra; EMER, Maria Claudia Figueiredo Pereira. INVESTIGAÇÃO EXPERIMENTAL E PRÁTICAS ÁGEIS: AMEAÇAS À VALIDADE DE EXPERIMENTOS ENVOLVENDO A PRÁTICA ÁGIL PROGRAMAÇÃO EM PAR. **Revista Eletrônica de Sistemas de Informação**, [S.l.], v. 13, n. 1, apr. 2014. ISSN 1677-3071. Disponível em:

<https://www.periodicosibepes.org.br/index.php/reinfo/article/view/1500>. Acesso em: 04 oct. 2023. doi:<https://doi.org/10.21529/RESI.2014.1301005>.

[43] TRAVASSOS, Guilherme Horta; GUROV, Dmytro; AMARAL, Edgar. Introdução à Engenharia de Software Experimental. Rio de Janeiro: COPPE/UFRJ, 2002. (Relatório Técnico, RT-ES-590/02). Disponível em: <https://www.cin.ufpe.br/~scbs/experimental/IntroducaoExperimentacao.pdf>. Acesso em: 08 de agosto de 2023.

[44] COSTA, Edson. Os Coworkings estão preparados em Segurança da Informação?. *In: Os Coworkings estão preparados em Segurança da Informação?*. Brasil, 4 abr. 2023. Disponível em: <https://studioestrategia.com.br/2023/04/26/coworkings-seguranca-informacao/>. Acesso em: 26 abr. 2023.

[45] GÓES, Geraldo; MARTINS, Felipe; ALVES, Vinícius. Os Condicionantes do Teletrabalho Potencial no Brasil. *Teletrabalho*, [S. l.], p. 1-40, 1 jan. 2023. DOI <http://dx.doi.org/10.38116/td2830>. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/11730/1/TD_2830_web.pdf. Acesso em: 18 set. 2023.

[46] HOWINGTON, Jessica. Top 100 Companies to Watch for Remote Jobs in 2023. [S. l.], 15 fev. 2023. Disponível em: <https://www.flexjobs.com/blog/post/100-top-companies-with-remote-jobs-2023>. Acesso em: 6 set. 2023.

[47] CHÉROLET, Brenda. Pesquisa mostra 10 áreas com mais vagas remotas em 2023. Brasil, 17 ago. 2023. Disponível em: <https://www.educamaisbrasil.com.br/educacao/carreira/pesquisa-mostra-10-areas-com-mais-vagas-remotas-em-2023-confira>. Acesso em: 22 mar. 2023.

APÊNDICES

APÊNDICE A - Termo de consentimento de participação

Survey - Segurança e privacidade dos dados no teletrabalho

Termo de Consentimento Livre e Esclarecido ao Responsável

Prezado participante,

Por meio deste questionário, convidamos você a participar de uma pesquisa que investiga a **segurança e privacidade dos dados no ambiente de teletrabalho**.

Esta pesquisa pertence a um trabalho de graduação do curso de ciência da computação do Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE).

O objetivo dessa pesquisa é captar dados para uma análise sobre o cenário de teletrabalho dos participantes no contexto de segurança e privacidade dos dados pós-pandemia.

Gostaríamos de enfatizar que:

1. Sua participação é totalmente voluntária e anônima.
2. Todas as informações que você fornecer serão mantidas em sigilo.
3. Não há a intenção de julgá-lo como pessoa ou a empresa. Existe apenas o interesse em investigar a sua opinião profissional perante a área coberta nesta pesquisa.
4. A qualquer momento você pode desistir de participar da pesquisa.
5. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição.
6. Os dados coletados neste formulário não serão divulgados de forma a possibilitar sua identificação.

Pesquisadores Responsáveis:

- Aluno(a): Diogo Wellyngton de Souza Barbosa (Graduando em Ciência da Computação no CIn/UFPE) - dwsb@cin.ufpe.br

- Orientador(a) do trabalho: Jéssyka Vilela (Professora Doutora no CIn/UFPE) - jffv@cin.ufpe.br

Fique à vontade para entrar em contato com esse comitê responsável.

Informações gerais sobre o questionário

1. Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa. *

☐ Sim

☐ Não

APÊNDICE B - Questionário da pesquisa

Perfil do Participante

✕

⋮

Essa seção tem como objetivo identificar o perfil do profissional que está respondendo essa pesquisa, bem como sua experiência educacional e com a área de segurança da informação e privacidade.

1 - Qual a sua faixa etária? (Assinale a alternativa correspondente) *

☐ Menor de 18

☐ 18 até 24

☐ 25 até 34

☐ 35 até 44

☐ 44 até 60

☐ Acima de 60

2 - Qual o seu maior grau de instrução? *

☐ Fundamental

☐ Médio/Técnico

☐ Superior

☐ Pós-Graduação (Especialização)

☐ Mestrado

☐ Doutorado

☐ Pós-Doutorado

☐ Outros...

3- Qual sua área de formação? *

- ☐ Tecnologia/Computação
- ☐ Engenharia (todos os cursos de engenharia exceto engenharia da computação)
- ☐ Administração/Gestão/Financeira
- ☐ Jurídico
- ☐ Saúde
- ☐ Educação
- ☐ Outros...

4 - Qual o seu tipo de vínculo de trabalho atual? *

- ☐ Empregado (Com carteira assinada)
- ☐ Pessoa Jurídica (Prestador de serviço com CNPJ)
- ☐ Autônomo/Freelancer (Pessoa física)
- ☐ Servidor Público
- ☐ Estágio Profissional
- ☐ Desempregado
- ☐ Outros...

5 - Qual a sua área de trabalho atualmente?

- ☐ Computação
- ☐ Vendas
- ☐ Marketing
- ☐ Financeiro
- ☐ Administrativo
- ☐ Saúde
- ☐ Jurídico
- ☐ Outros...

6 - Você trabalha em que setor?

- ☐ Público
- ☐ Privado
- ☐ Ambos
- ☐ Outros...

7 - Qual é o porte da instituição que você trabalha ou presta serviço?

- ☐ Microempresa (até 9 funcionários)
- ☐ Empresa de pequeno porte (de 10 a 49 funcionários)
- ☐ Empresa de médio porte (de 50 a 99 funcionários)
- ☐ Grande empresa (100 ou mais)

8 - Quanto tempo de trabalho você tem na sua instituição? *

- ☐ Menos de 1 ano
- ☐ De 1 a 2 anos
- ☐ De 2 a 5 anos
- ☐ De 5 a 10 anos
- ☐ De 10 a 20 anos
- ☐ Mais de 20 anos

9 - Você trabalha em qual setor da instituição? *

- ☐ TI (Suporte ao usuário e Infraestrutura)
- ☐ Administrativo
- ☐ Financeiro
- ☐ Vendas
- ☐ Recursos Humanos
- ☐ Operacional (Setor responsável diretamente pelo ramo de atuação da empresa)
- ☐ Outros...

10 - Qual seu regime de trabalho? *

- ☐ Teletrabalho (Trabalha em tempo integral remotamente)
- ☐ Híbrido (Trabalha tanto no escritório como remotamente)
- ☐ Presencial (Trabalha em tempo integral no escritório)

11 - Você trabalha para quais dessas regiões globais? *

- ☐ Brasil
- ☐ América central e Caribe
- ☐ América do Norte
- ☐ América do Sul (exceto Brasil)
- ☐ Ásia
- ☐ Europa
- ☐ Oceania
- ☐ Oriente Médio/África
- ☐ Global
- ☐ Outros...

12 - Qual o principal ramo de atividade econômica da instituição onde você trabalha? *

- ☐ Tecnologia da informação (Desenvolvimento de software, consultoria de TI, Serviços de TI)
- ☐ Educação
- ☐ Consultoria
- ☐ Indústria
- ☐ Comércio
- ☐ Saúde e Bem-Estar
- ☐ Serviços
- ☐ Beneficência
- ☐ Outros...

Recursos, Atitudes e Conhecimento



Essa seção tem como objetivo colher dados sobre o conhecimento dos participantes sobre segurança e privacidade dos dados no contexto de teletrabalho e também tem como objetivo entender quais os recursos que são disponibilizados pelas empresas e instituições aos seus funcionários.

13 - Você trabalha com dados pessoais ou sensíveis? *

- ☐ Sim
- ☐ Não
- ☐ Talvez
- ☐ Não sei responder

14 - Você utiliza recurso pessoal para fins de trabalho? Exemplo: Computador pessoal, celular pessoal, licença de software pessoal, etc... *

- ☐ Sim
- ☐ Não

15 - Quando você trabalha na sua casa, geralmente você trabalha em qual cômodo?

- ☐ Não trabalho em casa
- ☐ Quarto
- ☐ Sala
- ☐ Escritório
- ☐ Terraço/varanda

16 - Você costuma trabalhar em ambientes de coworking?

☐ Sim

☐ Não

17 - Você compartilha suas credenciais de sistemas com outras pessoas? *

☐ Sim

☐ Não

18 - Você bloqueia seu computador ao se ausentar de sua mesa? *

☐ Nunca

☐ Às Vezes

☐ Sempre

19 - Você costuma trabalhar com seus equipamentos conectados em redes de internet públicas (por exemplo: Wifi de shoppings, aeroportos, cafés) ?

☐ Nunca

☐ Às vezes

☐ Sempre

☐ Outros...

20 - Você troca suas senhas com qual frequência? *

- ☐ Não costumo trocar senha
- ☐ Semanalmente
- ☐ Mensalmente
- ☐ Trimestralmente
- ☐ Semestralmente
- ☐ Anualmente
- ☐ Outros...

21 - Você usa seu computador ou equipamentos de trabalho para fins pessoais? *

- ☐ Nunca
- ☐ Às vezes
- ☐ Sempre

22 - Você empresta seu computador ou equipamento de trabalho para terceiros? *

- ☐ Nunca
- ☐ Às vezes
- ☐ Sempre

23 - Você comenta assuntos sigilosos relacionados ao seu trabalho no ambiente doméstico?

- ☐ Nunca
- ☐ Às vezes
- ☐ Sempre

24 - Você participa de reuniões sem fones de ouvido mesmo quando há outras pessoas próximas?

- ☐ Nunca
- ☐ Às vezes
- ☐ Sempre

25 - Você costuma fechar a Webcam e o microfone dos seus equipamentos quando não está utilizando?

- ☐ Nunca
- ☐ Às vezes
- ☐ Sempre

26 - Você costuma trafegar informações de trabalho em redes sociais como Facebook, WhatsApp etc?

- ☐ Nunca
- ☐ Às Vezes
- ☐ Sempre

27 - Você já participou de treinamentos sobre segurança da informação? *

☐ Sim

☐ Não

28 - Você foi instruído a tomar medidas de segurança específicas para trabalhar remotamente?

☐ Sim

☐ Não

29 - Se a resposta anterior foi sim, quais foram as medidas que você foi orientado?

Texto de resposta longa

.....

30 - Esses recursos são providos pela a instituição onde você trabalha? *

	Sim	Não	Não sei
Computador ou Notebook	☐	☐	☐
VPN	☐	☐	☐
Email corporativo	☐	☐	☐
Telefone corporativo	☐	☐	☐
Antivírus	☐	☐	☐
Sistema de gerenciame...	☐	☐	☐
Softwares licenciados	☐	☐	☐
Suporte de TI remoto	☐	☐	☐
Treinamentos relaciona...	☐	☐	☐
Canal para tirar dúvidas ...	☐	☐	☐
SSO - Sistema de login ú...	☐	☐	☐

31 - Em um grau de 1 a 5, qual o seu nível de conhecimento sobre a importância de cada um desses itens abaixo listados para a segurança e privacidade dos dados no seu ambiente de trabalho? *

OBS:

- 1 significa que você não tem conhecimento algum;

- 5 significa que você tem total conhecimento sobre a importância daquele recurso.

	1	2	3	4	5
Não compartil...	☐	☐	☐	☐	☐
Usar VPN para ...	☐	☐	☐	☐	☐
Usar sistemas ...	☐	☐	☐	☐	☐
Usar autentica...	☐	☐	☐	☐	☐
Utilizar antivírus	☐	☐	☐	☐	☐
Ler as normas ...	☐	☐	☐	☐	☐
Instalar só apli...	☐	☐	☐	☐	☐
Utilizar softwar...	☐	☐	☐	☐	☐
Não utilizar em...	☐	☐	☐	☐	☐

32 - Você utiliza outras práticas de segurança que não foram listadas nesta pesquisa? Se sim, * qual (is)?

Texto de resposta longa

33 - Você gostaria de realizar algum comentário sobre esta pesquisa?

Texto de resposta longa