UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE ENGENHARIA DE SOFTWARE

BRUNO RAMOS RODRIGUES

UM ESTUDO PARA IDENTIFICAR OS DESAFIOS ENFRENTADOS PELAS ORGANIZAÇÕES COM RELAÇÃO A SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DE HOME OFFICE

Itacoatiara – Amazonas
Abril – 2022

BRUNO RAMOS RODRIGUES

UM ESTUDO PARA IDENTIFICAR OS DESAFIOS ENFRENTADOS PELAS ORGANIZAÇÕES COM RELAÇÃO A SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DE HOME OFFICE

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia de Software.

Orientador: Prof. Christophe Saint-Christie de Lima Xavier

Coorientadora: Shermam Tácia da Costa Lima

Itacoatiara – Amazonas
Abril – 2022

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Rodrigues, Bruno Ramos
R696e Um estudo para identificar os desafios enfrentados pelas organizações com relação a segurança da informação no ambiente de home office / Bruno Ramos Rodrigues . 2022
80 f.: il. color; 31 cm.

Orientador: Christophe Saint-Christie de Lima Xavier
Coorientadora: Shermam Tácia da Costa Lima
TCC de Graduação (Engenharia de Software) - Universidade Federal do Amazonas.

1. Home Office. 2. Segurança da Informação. 3. Vulnerabilidades. 4. Práticas de Segurança da Informação. I. Xavier, Christophe Saint-Christie de Lima. II. Universidade Federal do Amazonas III. Título

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Curso de Bacharelado de Engenharia de Software

FOLHA DE APROVAÇÃO

BRUNO RAMOS RODRIGUES

UM ESTUDO PARA IDENTIFICAR OS DESAFIOS ENFRENTADOS PELAS ORGANIZAÇÕES COM RELAÇÃO A SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DE HOME OFFICE

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia de Software.

Aprovada em 25 de Abril de 2022

BANCA EXAMINADORA

Prof. Me. Christophe Saint-Christie de Lima Xavier, Presidente
Universidade Federal do Amazonas

Profa. Dra. Odette Mestrinho Passos, Membro
Universidade Federal do Amazonas

Prof. Me. Jhonatan Araujo Oliveira, Membro
Universidade do Estado do Amazonas

Folha de Aprovação assinada pela Profa. Dra. Odette Mestrinho Passos, responsável pela disciplina de Trabalho de Conclusão de Curso (Período: 2021.1), onde atesta a defesa do(a) aluno(a) e a presença dos membros da banca examinadora.

Documento assinado eletronicamente por **Odette Mestrinho Passos**, **Professor do Magistério Superior**, em 28/04/2022, às 13:56, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alternei de Souza Brito**, **Coordenador de Curso**, em 28/04/2022, às 18:29, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0962587** e o código CRC **0C975125**.

Rua Nossa Senhora do Rosário - Bairro Tiradentes nº 3836 - Telefone: (92) (92) 99318-2549
CEP 69103-128 Itacoatiara/AM - ccesoicet@ufam.edu.br

O sucesso é alcançado com muita perseverança.

Que a força esteja com você... Sempre!!!

Star Wars

AGRADECIMENTO

Primeiramente gostaria de agradecer a Deus, por ter ajudado a concluir mais uma etapa, agradecer a minha família que contribuiu grandemente para o meu processo acadêmico. A minha mãe Angelândia Ramos, minha avô Suely Ramos e o Inácio Farias, que sabiam a importância do estudo e que fizeram o possível para que eu tivesse a oportunidade de continuar nele.

Gostaria também de agradecer ao professor orientador Christopher Xavier, por ter aceitado a me orientar e caminhar junto comigo para a conclusão deste trabalho, dedicando seu tempo para com que esse trabalho pudesse ser finalizado e permitir a conclusão de mais uma etapa.

Agradeço também em especial a minha namorada Shermam Tácia da Costa Lima que durante o curso de engenharia sempre me ajudou, fizermos vários trabalhos em equipe, onde pude aprender grandes coisas sobre dedicação, companheirismo, empenho e capricho. Sendo está uma peça fundamental para o meu crescimento acadêmico e profissional.

O sentimento é de gratidão por concluir minha graduação em uma instituição que busca sempre apoiar o aluno para que seu momento formativo chegue. Agradeço a todos que me ajudaram nesse caminho, o final dessa fase é uma conquista incrível.

RESUMO

A segurança da informação é essencial para os negócios e a cada dia torna-se mais presente nas organizações públicas e privadas. Durante a pandemia muitas organizações tiveram que trabalhar em home office, e com isso, houve uma necessidade crescente de segurança da informação dentro das organizações. Na atualidade não se é novidade que ocorram diversos ataques nas organizações de forma virtual, porém devido a Corona Vírus Disease-19 e a adaptação da nova forma de trabalho, o número de ataques aumentou significativamente. Com esse cenário, este trabalho proposto tem como objetivo analisar os problemas enfrentados pelas organizações em relação à segurança da informação no ambiente home office. A metodologia adotada está baseada em um estudo secundário, neste caso um mapeamento sistemático, além de uma análise quantitativa através de uma pesquisa de opinião. Como resultados obtidos do mapeamento sistemático, foi possível identificar 8 vulnerabilidades, 8 ameaças e 9 práticas de segurança da informação em ambiente home. Através da pesquisa de opinião, foi possível validar as práticas identificadas com profissionais que tenham atuado no ambiente home office, e as práticas com maior nível de relevância com 97% foram treinamento para o trabalho home office, usar antivírus e uso seguro de senhas. Espera-se que este trabalho ajude no home office organizações e profissionais que trabalham em ambiente de escritório mantêm a proteção das informações e minimizam a possibilidade de erros graves.

Palavras-Chave: Home Office, Segurança da Informação, Vulnerabilidades, Práticas de Segurança.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANS	Análise do Núcleo de Sentidos
CCTA	Central Computer and Telecommunications Agency
COBIT	Control Objectives for Information and related Technology
COVID-19	Corona Vírus Disease-19
DNS	Domain Name System
GDPR	General Data Protection Regulation
ISACA	Information Systems Audit and Control Association
ISSO	Organização Internacional de Normalização
ITIL	Information Technology Infrastructure Library
LGPD	Lei Geral de Proteção de Dados
MS	Mapeamento Sistemático
PO	Pesquisa de Opinião
PWC	Price Waterhouse Coopers
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo serão apresentados o contexto e a descrição do problema, e a motivação desta pesquisa. São também apresentados os objetivos, a metodologia científica e a organização deste projeto.

1.1 Contextualização

A Tecnologia da Informação (TI) é um conjunto de todas as atividades que visam o uso da informação e sua segurança. Até recentemente, o setor de TI era visto apenas como uma simples área de suporte para algumas atividades das organizações. No decorrer do tempo a importância desse setor foi crescendo e o ritmo em que ele se desenvolvia foi bastante acelerado. Atualmente se tornou um setor de negócios responsável por atender às organizações auxiliando no alcance de metas e objetivos (GONÇALVES, 2022; BUOGO; FACHINELLI e GIACOMELLO, 2019).

A segurança da informação é essencial para os negócios e a cada dia torna-se mais presente nas organizações públicas e privadas. Cotidianamente as organizações investem na proteção de suas informações, onde o papel da segurança da informação é garantir que somente pessoas autorizadas tenham acesso às informações. As organizações se esforçam muito no crescimento dos departamentos de TI devido ao perigo constante de ataques virtuais e a exposição de seus dados (SOARES S.; SOARES, A. e ALVES, 2021).

É notável os grandes problemas em relação à segurança da informação nas organizações. Desse modo, as organizações brasileiras investem ainda mais em TI para manter seus dados protegidos (REUTERS, 2019).

Pesquisa realizada pela PWC apontou que, quando bem-sucedidos, os ataques custaram em média 1,35 milhões de dólares para as companhias no primeiro semestre de 2019. Como resultado, o investimento em segurança da informação no país cresce a um ritmo anual de 30% a 40%, enquanto no restante do mundo, esse crescimento é entorno de 10% a 15% ao ano (REUTERS, 2019).

Durante a pandemia muitas organizações tiveram que aderir ao home office e isso ocorreu em larga escala, sendo assim houve uma necessidade crescente de segurança da informação dentro das organizações. Os índices mostram um grande aumento no número de ataques de *phishing*, *ransomware* e fraudes que são cada vez mais baseados em Corona Vírus Disease-19 (COVID-19) para melhorar a eficácia do ataque (SOBERS, 2021).

Organizações do mundo estão adotando modelos remotos de trabalho, incentivando a cultura do home office como jamais visto antes. No entanto, embora essa seja uma prática para dar continuidade ao trabalho de forma remota, é importante que as organizações se coloquem em alerta para fazer com que este processo aconteça de maneira segura, também do ponto de vista dos negócios (RODRIGUES JR., 2021).

Segundo Alves (2020), afirma que devido ao COVID-19, o trabalho flexível ou home office está sendo apoiado por mais organizações, que pesquisas estão sendo desenvolvidas sobre como implementá-lo com segurança, observando também que o trabalho remoto será mais frequente no após a pandemia, e que as organizações continuarão a aumentar seu apoio investindo ainda mais nesse método de trabalho remoto.

1.2 Justificativa

Para garantir a segurança não é necessário somente pensar em barrar a entrada e saída dos dados, mas sim monitorar o que está acontecendo dentro e fora da organização (OTTONICAR *et al.*, 2020). As falhas mais frequentes na segurança são a falta de experiência e má qualificação de profissionais responsáveis pela segurança dos dados. Por outro, deve ser observado também a conduta dos funcionários atuando dentro e fora do ambiente de trabalho (LEÃO, 2012).

O home office é uma modalidade de trabalho que vem crescendo, impulsionado pelas organizações com o objetivo de flexibilizar o trabalho. Como é uma modalidade que está sendo bastante utilizada, ainda não existe um padrão de implantação, resultando nos problemas de segurança da informação, pois há vários riscos no que diz respeito à confidencialidade dos dados. Devido ao fato de não possuir um padrão de implantação definido, os funcionários que trabalham remotamente são alvos frequentes de ataques cibernéticos, com potencial de causar enormes prejuízos à organização (RODRIGUES JR., 2021).

Na atualidade, não se é novidade que ocorram diversos ataques às organizações de forma virtual, porém devido à pandemia e as organizações ainda estarem se adaptando para essa nova forma de trabalho, o número de ataques aumentou significativamente. Uma pesquisa realizada pela CyberArk diz que 77% dos funcionários remotos estão utilizando dispositivos inseguros e não gerenciados para acessar sistemas corporativos (NEC, 2020).

Sem boas práticas de segurança, os funcionários podem experimentar muito descuido em um ambiente doméstico. Sem a ajuda e os recursos adequados fornecidos pela organização, os colaboradores ficam vulneráveis a diversos ataques por falta de conhecimento, como manter softwares, sistemas e firewalls atualizados e evitar o uso de *pendrives* de terceiros nos dispositivos de trabalho (NEC, 2020). Neste contexto, a justificativa deste trabalho proposto dar-se pela importância de identificar e descrever as principais ameaças e vulnerabilidades na utilização do home office e quais práticas devem ser seguidas para manter a segurança dos dados da organização.

1.3 Objetivos

Geral

Analisar os problemas enfrentados pelas organizações em relação à segurança da informação no ambiente home office.

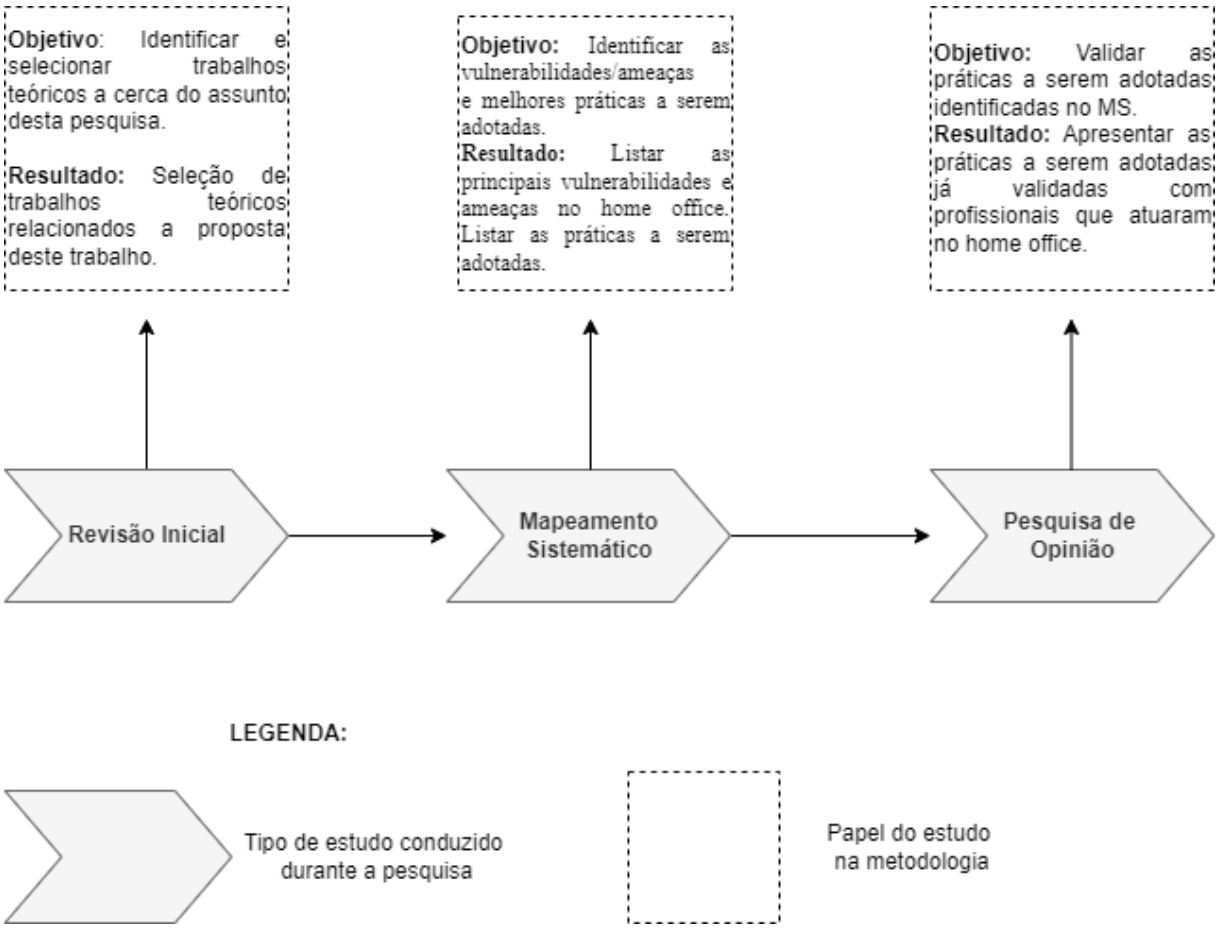
Específicos

- Identificar as vulnerabilidades/ameaças e melhores práticas a serem adotadas pelas organizações para manter a segurança da informação no ambiente home office.
- Validar as práticas já identificadas com os profissionais que atuaram no ambiente home office.

1.4 Metodologia

A metodologia deste trabalho proposto é dividida em três etapas, como pode ser observado na Figura 1, que são: revisão inicial, busca descrever uma pesquisa que sirva como base, mapeamento sistemático, processo que objetiva alcançar resultados com valores científico e pesquisa de opinião, que buscar validar as informações do mapeamento sistemático através de pesquisa que pode ser formulários ou entrevista com participantes.

Figura 1 - Metodologia



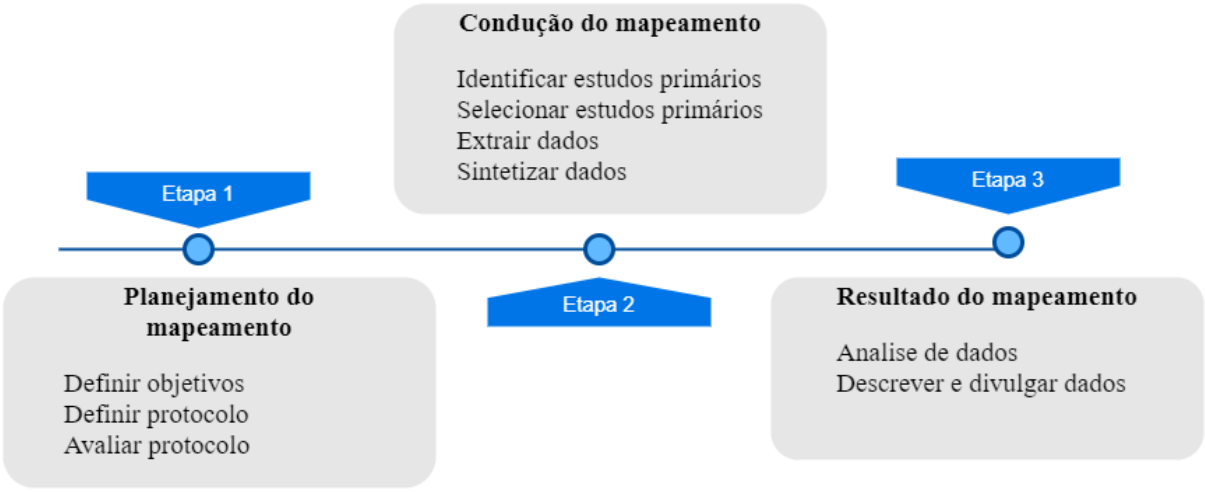
Fonte: O autor (2022).

- **Revisão Inicial**: O objetivo é identificar os conceitos básicos para apoiar a definição de um protocolo de MS mais preciso e abrangente.
- **Mapeamento Sistemático**: O MS tem como objetivo fornecer uma visão geral de uma área de pesquisa, identificando a quantidade, os tipos de pesquisas realizadas, os resultados disponíveis, além das frequências de publicações ao longo do tempo para identificar tendências (KITCHENHAM e CHARTERS, 2007). Nessa atividade o protocolo é elaborado e executado. O MS será aplicado para identificar os desafios enfrentados pelas organizações em relação à segurança da informação. De acordo com Kitchenham e Charters (2007), o processo do MS divide-se em três principais etapas, na qual elas são coordenadas de maneira interativa, que dizer, um processo irá se reiniciar até alcançar algum resultado.
- **Pesquisa de Opinião**: A pesquisa de opinião será aplicada para avaliar com os profissionais que tenham trabalhado no ambiente home office. Consiste em três etapas: planejamento, execução e análise dos dados. Na etapa de planejamento é descrito os

participantes, as perguntas, o meio onde será publicada a pesquisa, a fase de execução é quando está realizando a pesquisa com os participantes selecionados, e pôr fim a análise é a fase em que é descrito a caracterização dos participantes, a verificação dos dados relacionados ao tema pesquisado e as principais ameaças que validam a pesquisa.

A Figura 2 apresenta as etapas que serão seguidas para realizar o mapeamento sistemático.

Figura 2 - Mapeamento Sistemático



Fonte: O autor (2022).

Planejamento do Mapeamento: Na etapa de planejamento tem como objetivo identificar a motivação para a execução de um MS. O primeiro passo nessa fase é buscar identificar se já existem estudos publicados acerca do mesmo tema de pesquisa, depois de feito este passo é identificado à necessidade para realizar o MS, é definido o protocolo que é crucial para a realização do mapeamento (KITCHENHAM e CHARTERS, 2007).

Condução do Mapeamento: Com o protocolo definido e avaliado, tem-se início a etapa de condução do MS. Nesta fase, são identificados os estudos que podem ser utilizados no trabalho usando a estratégia de busca definida pelo protocolo. Em posse desses estudos, serão aplicados critérios de seleção (critérios de inclusão, exclusão e de qualidade) (KITCHENHAM e CHARTERS, 2007).

Resultado do Mapeamento: Essa é a última etapa, onde os dados extraídos serão analisados conforme o protocolo para serem divulgados aos potenciais interessados (KITCHENHAM e CHARTERS, 2007).

1.5 Organização do Trabalho

O Capítulo 1 apresentou os principais aspectos deste trabalho, descrevendo o seu contexto, motivação, justificativa, objetivos, metodologia adotada e a organização do trabalho. Além desta Introdução, outros dois capítulos compõem este trabalho, organizados da seguinte forma:

- Capítulo 2 – Fundamentação Teórica: é apresentado o referencial teórico que fundamenta os conceitos básicos utilizados nesta pesquisa e os trabalhos relacionados.
- Capítulo 3 – Segurança da Informação no Home Office: Este capítulo apresenta o resultado do mapeamento sistemático.
- Capítulo 4 – Percepção dos Profissionais ao Home Office: Este capítulo apresenta o resultado da pesquisa de opinião.
- Capítulo 5 – Considerações Finais e Perspectivas Futuras: Este capítulo apresenta as considerações finais, resultados obtidos, contribuição do trabalho, as limitações e trabalhos futuros direcionados para continuidade desta pesquisa**.**

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão apresentados os conceitos relacionados sobre os principais assuntos de segurança da informação, como também, serão apresentados os trabalhos relacionados.

2.1 Conceitos Relacionados

2.1.1 Tecnologia da Informação

A inovação é resultado do desvio de algo que, no processo adquire novas características que conseguem realizar coisas que anteriormente não eram imaginadas. As inovações surgem, quando acontecem fatos inesperados que colocam novos problemas e necessidades, abrindo novas possibilidades, por mudanças no mercado, que criam exigências e novas tecnologias (TEIXEIRA e SOUZA, 2016).

Os avanços tecnológicos têm conquistado espaço em tempo veloz no mundo globalizado, estabelecendo modificações e impactando vários setores da sociedade. Nesse contexto, estamos vivendo em uma sociedade da informação, onde o acesso à informação e ao conhecimento está amplamente disponível. Diante disso tem-se a pergunta o que seria tecnologia, o que se nota na literatura é variadas dimensões, resultando em interpretações diversificadas (CASTRO, BERNARTT e GODOY, 2017).

O conhecimento é um ativo de uma organização e proporciona grande vantagem competitiva em relação às outras, sendo este o único recurso econômico de valor sendo reconhecido como a fonte primária de vantagem competitiva de uma empresa (RAMOS, YAMAGUCHI e COSTA, 2020). A TI é universalmente considerada uma ferramenta essencial para aumentar a competitividade da economia de um país. É notório que a TI possui efeitos significativos na produtividade das empresas (ATTATSITSEY e OSEI-BONSU, 2021).

A TI é definida como a totalidade de ativos investidos na tecnologia ligada à gerência de informação, que é determinada por hardware, software e recursos humanos (RAMOS, YAMAGUCHI e COSTA, 2020). Já Belmiro (2018), define que os principais componentes essenciais são hardware, software e recursos de telecomunicações. Fazendo uma união do exposto podemos definir:

- **Hardware**: Dispositivos físicos digitais, com função de receber, armazenar e processar dados.

- **Software:** Programas, aplicativos ou sistemas operacionais, cuja função é: dirigir, organizar e controlar o hardware.
- **Recursos Humanos**: são as pessoas que interagem com o software e hardware.
- **Telecomunicações:** são transmissões eletrônicas de sinais para comunicação. A arquitetura é formada por computadores que fazem a recepção e o envio de dados através de meios de comunicação, com fios telefônicos ou ondas de rádio.

Com o uso da TI em uma organização há grandes efeitos benéficos, pois estimula à sua capacidade de inovar devido à influência positiva na velocidade de adoção de novas técnicas e processos. Empresas que adquirem a TI são capazes de se infiltrar mais facilmente em novos segmentos do mercado, facilitando o contato com novos fornecedores, além de criar uma relação mais próxima com seus clientes (MOHAMAD *et al*., 2017).

Com o crescente avanço tecnológico, grandes e pequenas empresas tornam-se cada vez mais competitivas exigindo dos sistemas de informação um alto grau satisfatório de desempenho (LIMA, PASSOS e XAVIER, 2019). A utilização das tecnologias é essencial para o sustento das organizações, é de suma importância que as empresas estejam preparadas e organizadas para a utilização imprescindível dos sistemas de informação (ROZA, 2020).

A crescente utilização de novas tecnologias tem feito com que as organizações sejam dependentes dos atuais sistemas informatizados. Essa dependência é consequência da quantidade e complexidade dos sistemas computacionais que controlam os mais variados tipos de operações e o próprio fluxo de informação das organizações (LAUDON, K. e LAUDON, J., 2014).

Os sistemas de informação têm como características a responsabilidade de realizar o tratamento, a transmissão e o armazenamento de toda a informação existente na organização. As organizações necessitam dos sistemas, sejam para o gerenciamento da informação, para manter em segurança os dados de negócio, para dar suporte às áreas e departamentos, utilizando sistemas e subsistemas (BELMIRO, 2018).

Dentro de um sistema de informação a tomada de decisão, a coordenação e o controle da organização são auxiliados pela coleta (ou recuperação), processo, armazenagem e distribuição da informação, esse conjunto de componentes ajudam os gerentes e colaboradores a analisar problemas, visualizar assuntos complexos e criar produtos (BELMIRO, 2018). Os principais conceitos ligados ao sistema de informação são:

- **Dados**: são itens referentes a uma descrição primária de objetos, atributos, propriedades que não estão organizados e sem um significado.
- **Informação**: é o conjunto de dados organizados para terem um sentido e valor para tomada de decisão.
- **Conhecimento:** são as informações organizadas e processadas para transmitir compreensão, experiência, aprendizado que podem ser aplicados a determinado problema ou atividade.

2.1.2 Segurança da Informação

As ameaças, vulnerabilidades da tecnologia, códigos de sistemas, sistemas operacionais, os processos e as pessoas possibilitam uma grande oportunidade para o desenvolvimento e a evolução prática da segurança da informação. Devido ao fato do ambiente corporativo e de negócios ficarem mais dependentes da tecnologia e dos processos automatizados, a prática adequada da segurança da informação tem se tornado cada vez mais importante (OLIVEIRA; MOURA e ARAÚJO, 2012).

Dentre essa importância da segurança dos dados no ambiente corporativo, cada vez mais vem sendo exigido dos executivos de segurança mais do que conhecimento técnico e por isso, esses profissionais vêm investindo em suas carreiras e tornando cada vez mais versáteis e completos. A busca pela segurança da informação deve ser algo contínuo no contexto empresarial, buscando a conscientização dos usuários das informações tanto no ambiente corporativo quanto no trabalho remoto ou ambiente domiciliar, e os quais devem entender que mais que um ato a segurança da informação precisa tornar-se um hábito (LEÃO, 2012).

Mesmo com organizações adotando muitas medidas de segurança, ainda é fato que o trabalho em rede caseira ou home office deixa as informações das organizações mais vulneráveis do que no ambiente organizacional por diversos motivos. Devido ao atual estado global, muitas organizações tiveram que se adaptar a essa nova realidade levando muitas a terem sua primeira experiência com o home office, surgindo a necessidade do aprimoramento tanto nas tecnologias de comunicação quanto na TI para melhorar a proteção dos dados da organização (RODRIGUES JR. *et al*., 2021).

A utilização da TI para manipulação e armazenamento de dados tem adquirido um caráter crítico na medida em que são introduzidos novos riscos e aumenta-se a fragilidade de

algumas atividades. Com isso torna-se essencial a atenção às questões relacionadas à segurança da informação, qualidade de software (LEÃO, 2012).

O principal objetivo da segurança da informação é minimizar ao máximo qualquer tipo de risco referente ao vazamento de dados, sabendo-se que na maioria dos casos o invasor pode estar dentro da própria organização. Portanto, é necessário um conjunto de procedimentos e ferramentas para garantir a proteção da informação (BARBOSA e SILVA, 2016).

A Segurança da Informação tem como objetivo proteger os sistemas de informação contra a invasão e modificação dos dados por acessos não autorizados. Garante que as informações armazenadas em processamento ou em trânsito estejam protegidas, assegura a segurança das áreas e instalações computacionais (OLIVEIRA; MOURA e ARAÚJO, 2012).

A segurança da informação é possível de ser alcançada com a implantação de um conjunto de controles apropriados. Entretanto, estes controles precisam ser predeterminados e monitorados constantemente para que quando necessário receber ajustes e aperfeiçoamentos sem comprometer a segurança dos dados armazenados. A segurança da informação pode ser comprometida por diversos fatores como (GALVÃO, 2015).

- Comportamento indevido dos próprios usuários ou proprietários da informação;
- Problemas no ambiente em que a informação se encontra;
- Falhas na infraestrutura da organização;
- Indivíduos mal-intencionados, que tem como objetivo alterar, destruir ou danificar as informações.

Outro fator que compromete a segurança da informação é o que chamado intempéries que são desastres naturais que podem ou não afetar infraestruturas como: alagamentos, furacões, incêndios, problemas elétricos e até mesmo poeira, podendo colocar em riscos o ambiente em que a informação está armazenada (GALVÃO, 2015).

A segurança da informação é alcançada através da implementação de um conjunto adequado de controles incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software de hardware (HINTZBERGEN *et al.*, 2018).

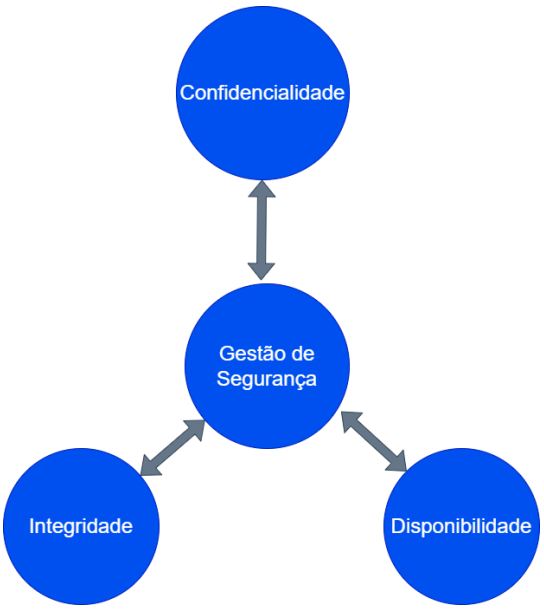
As informações são geradas pelas organizações, com isso elas devem ser classificadas e organizadas. Com o objetivo de manter seus dados protegidos e que haja continuidade dos negócios, o ambiente em que os dados estão armazenados deve estar seguro de fatores que

possam causar perdas indevidas dos dados. A seguir estão listados os principais fatores que causam perda dos dados armazenados (BARBOSA e SILVA, 2016).

- Problemas ambientais (variação térmica, umidade, fumaça)
- Interrupção de serviços (queda de energia elétrica, falha nos equipamentos, problemas nos sistemas operacionais, falhas de software)
- Ataque de *crackers* (há vários vírus que excluem dados e danificam o sistema operacional)
- Erros involuntários de usuários
- Treinamento inadequado
- Erro de cópias de dados ou esquecimento da realização de backup

Um sistema de segurança da informação pode ter diversos objetivos, mas os princípios em todos os programas de segurança são a confidencialidade, integridade e disponibilidade (veja a Figura 3). Estes são referidos como triângulo CID, o nível de segurança requerido para executar esses princípios difere para cada empresa, pois cada um tem suas próprias combinações de objetivos e requisitos de negócio de segurança (HINTZBERGEN *et al.*, 2018).

Figura 3 - Triângulo CID



Fonte: Hintzbergen *et al.* (2018).

- **Confidencialidade:** A confidencialidade também chamada de exclusividade refere-se aos limites em termos de quem pode obter que tipo de informação. A confidencialidade pode ser fornecida através da criptografia de dados à medida que são armazenados e transmitidos, usando preenchimento de tráfego na rede, estrito

controle de acesso, classificação dos dados e treinamento de pessoal nos procedimentos apropriados.

- **Integridade:** A integridade refere-se a consistente com o estado ou a informação pretendida. Qualquer modificação não autorizada de dados, seja for acidental ou não, torna-se uma violação da integridade dos dados. Ambientes que reforçam e fornecem esse princípio de segurança asseguram que atacantes, ou erros de usuários, não comprometam a integridade dos sistemas ou dados. Quando um invasor insere um vírus em um sistema, a integridade é comprometida.
- **Disponibilidade**: A disponibilidade tem três características: Oportunidade, Continuidade e Robustez. Oportunidade é quando a informação está disponível quando necessário e Continuidade é quando a equipe consegue continuar trabalhando no caso de falha e por fim Robustez é quando existe a capacidade suficiente para permitir que toda a equipe trabalhe no sistema. Por exemplo, tanto uma falha de disco como um ataque de negação de serviço causam violação da disponibilidade.

Além dos três principais princípios básicos da segurança da informação, podem ser adicionados outros como, Autenticação, Não repúdio, Legalidade, Privacidade e Auditoria. Os conceitos itens mencionados são:

- **Autenticação:** é a confirmação de autoria do usuário;
- **Não repúdio:** é a capacidade do sistema de provar que um usuário realizou uma tarefa específica;
- **Legalidade:** objetiva garantir que o sistema esteja aderente à legislação pertinente;
- **Privacidade:** é a capacidade de um sistema em garantir o sigilo das informações e ações de um usuário;
- **Auditoria:** caracteriza-se como a capacidade do sistema em registrar e identificar tudo o que um usuário realiza.

Para entender sobre segurança da informação é necessário conhecer alguns conceitos importantes, como “vulnerabilidade”, “ameaça”, “ataque”, “risco” e “exposição” são termos frequentemente usados (KONZEN, 2013).

Vulnerabilidade

A vulnerabilidade é caracterizada por ser uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Pode ser considerada como ausência ou fraqueza de uma proteção que pode ser explorada. Alguns exemplos de vulnerabilidades que podem ser citadas são um serviço rodando em um servidor, aplicações ou sistemas operacionais desatualizados, acesso irrestrito para entrada de chamadas no modem, uma porta aberta no firewall, uma segurança física fraca que permita a qualquer pessoa entrar em uma sala de servidores ou a não aplicação de gestão de senhas em servidores e estações de trabalho (HINTZBERGEN *et al*., 2018).

Em uma organização podem existir diversas vulnerabilidades, porém elas sozinhas não causam nenhum tipo de incidente, no entanto caso ela seja encontrada por pessoas com objetivos ilícitos elas podem tornar-se uma ameaça (KONZEN, 2013).

Ameaça

Uma ameaça é um potencial causador de incidente não desejado, o que pode resultar em prejuízos ao sistema ou a organização. Quem tira a vantagem de uma vulnerabilidade é entendido como agente ameaçador. Um agente ameaçador são indivíduos não autorizados que buscam acesso a computadores de terceiros, acessando dados de uma forma que viole a política de segurança (HINTZBERGEN *et al*., 2018).

Com o objetivo de blindar-se de contra-ataques ou acessos não autorizados, deve ser identificado todas as ameaças e analisá-las individualmente buscando descrever suas intenções, se o agente tem possibilidade de realizar ameaça e qual seria o dano causado por ele. Com isto, é possível listar todas as ameaças que cada ativo pode estar suscetível e a vulnerabilidade que este ativo pode possuir (SANTOS e SOARES, 2019).

Ataque

Kim e Solomon (2014) destacaram que os ataques podem ser divididos em: Ataques ativos, que possuem alguma modificação na informação do usuário e ocorre por intrusão física e ataques passivos, onde não há nenhuma modificação, o intruso apenas observa ou intercepta a informação.

Segundo Kim e Solomon (2014) os programas maliciosos mais utilizados em ataques são vírus, vermes, Cavalo de Tróia, *rootkit* e programa espião. Os conceitos dos itens citados serão descritos a seguir:

- **Vírus:** É um tipo de programa que age criando cópias de si mesmo e alocando-os pelo sistema e aumentar o tamanho de arquivos, desativar funções do antivírus, entre outros.
- **Verme:** Similar ao vírus, mas se replica e envia cópias de si mesmo a outros computadores e não a outros programas no mesmo computador.
- **Cavalo de Tróia:** O cavalo de Tróia é bastante conhecido e começa agir no momento que é executado no computador, ele pode coletar informações confidenciais, baixar arquivos e ocultar programas.
- ***Rootkit*:** Utilizado para ocultar vestígios deixados pelo invasor após um ataque bem-sucedido. O *rootkit* modifica ou substitui outros programas no sistema para esconder o programa malicioso.
- **Programa Espião:** Similar ao cavalo de Tróia, porém ele tem uma única função, roubar informações dos usuários sem que eles saibam. Agindo por meio da internet monitorando as atividades dos usuários e colhendo informações.

Risco

Quando há probabilidade de um agente ameaçador possuir alguma vantagem sobre uma vulnerabilidade e o correspondente impacto no negócio é chamado de risco. Os firewalls têm a sua maior vulnerabilidade quando possuem diversas portas abertas, o que facilita um ataque bem-sucedido de um invasor permitindo o acesso não autorizado. Caso a rede não possua algum sistema de detecção de intrusão, pode gerar problemas de alta relevância que serão detectados depois de muito tempo (HINTZBERGEN *et al.,* 2018).

Exposição

A exposição é quando há algo exposto e com isso pode surgir algum agente ameaçador que permita com haja perdas. Uma ameaça pode surgir quando as vulnerabilidades de uma organização estão expostas (KONZEN, 2013).

2.1.3 Boas Práticas que Auxiliam as Organizações

ABNT trata-se de uma entidade privada e sem fins lucrativos e de utilidade pública, fundada em 1940 que possui a responsabilidade de administrar a normalização técnica no Brasil, em diversos setores. A entidade é membro fundadora da Organização Internacional de Normalização (ISO), na qual agrega todos os órgãos de normas técnicas do mundo (GOGONI, 2019).

Organizações de qualquer segmento precisam utilizar meios para preservar as informações, requerendo que seus gestores sigam alguns procedimentos, estratégias e diretrizes para garantir a sobrevivência da empresa (TUYIKEZE e FLOWERDAY, 2014). A importância de uma Política de Segurança da Informação (PSI) surge para fornecer critérios, diretrizes e normas que representam os princípios básicos de segurança da informação e do funcionamento de uma organização (RIOS, O.; RIOS, V. e TEIXEIRA FILHO, 2017).

A norma ABNT NBR ISO/IEC 27002:2013 consiste em uma norma de boas práticas para a segurança da informação. Onde aborda sobre a necessidade de preservar a informação de ameaças para minimizar o risco, enquanto maximiza retornos dos investimentos e torna possível a continuidade da organização. É necessária a aplicação dos controles adequados, esses sendo processos, procedimentos, políticas, a fim de garantir a segurança da informação (BANDEIRA, 2017).

A ABNT NBR ISO/IEC 27002 teve como embasamento um documento que foi divulgado pelo governo do Reino Unido, onde se tornou um padrão em 1995, chamado BS7799. Em 2000 foi anunciado como uma norma que foi chamada de padrão ISO 17799, até que em 2005 foi atualizada e fez parte da série de normas internacionais 27000, onde foram divulgados alguns documentos acerca do tema, para serem usados em conjunto. Foi lançada uma nova versão e publicada em 2013, a ISO 27002:2013 consta com 114 controles, diferindo da versão de 2005 que possuía 133 controles documentados (BANDEIRA, 2017).

Control Objectives for Information and related Technology (COBIT), é um conjunto de orientações e ferramentas que auxilia as organizações atingirem seus objetivos de governança da T.I., criada pela ISACA (*Information Systems Audit and Control Association*) para manter o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos. O COBIT não determina de que forma os processos serão executados, mas proporciona controles básicos para que a TI alcance seus objetivos alinhados aos objetivos de

negócio da organização (RIOS, O.; RIOS, V. e TEIXEIRA FILHO, 2017; GEHRMANN, 2012).

Segundo (ISACA, 2012) sua estrutura de controles possui padrões aceitos internacionalmente como os mais bem praticados para o estabelecimento de controles e padrões de segurança para a área de TI das organizações de diferentes segmentos de negócio. O COBIT está dividido em 34 processos incluídos em 4 grandes domínios que são:

- **Planejamento e Organização**: envolve as estratégias e táticas, buscando identificar modos pelos quais a TI pode auxiliar o negócio a atingir seus objetivos.
- **Aquisição e Implementação**: garante que as mudanças nos sistemas atenderão os objetivos do negócio.
- **Entrega e Suporte**: esse domínio responsabiliza-se pela entrega dos serviços solicitados e pela continuidade e segurança dos dados.
- **Monitoração e Avaliação**: abrange a gestão do desempenho, monitoração de controles internos, consonância regulatória. Os processos de TI devem ser auditados frequentemente.

2.1.4 Vulnerabilidades nas Organizações

Na segurança da informação, o *hacker* é um indivíduo ou grupo que possui grandes habilidades e conhecimento na informática, buscando explorar fraquezas em um sistema informático ou rede informática. Como desafio ou mesmo por seus princípios, procura formas de ganhar acesso não autorizado ao computador ou sistema corporativo revelando suas falhas para a organização. Por outro lado, o *cracker* são *hackers* que obtiveram acesso não autorizado, mas para fins maliciosos como obter informações para ganho financeiro, derrubar hardware, piratear software ou destruir dados (UGOCHUKWU-IBE e ONYEMACHI, 2014).

Criminosos digitais são *crackers* que praticam crimes por meio de dispositivos eletrônicos, que em sua grande maioria realizam ataques com o objetivo de obter recurso monetário, as infrações mais frequentes são: cibergrilagem (*cybersquatting*), prática na qual ocorre a apropriação de domínios virtuais registrados em nome de terceiros. Outra conduta corriqueira é o “sequestro” (*hijacking*) ou desvio de DNS (*Domain Name System*), que consiste em inserir alteração no endereço de uma determinada página com finalidade de direcionar a outro site, diferente daquele a que se procura a acessar (SIQUEIRA *et al*., 2021; FAVERO, A. e FAVERO, B., 2021).

Os dados de clientes recolhidos pelas empresas são muito valiosos e tem diversas finalidades como pesquisas sobre o público-alvo e campanhas de marketing, por isso esses dados recebem bastante segurança. O problema ocorre que os criminosos digitais também perceberam a importância desses dados valiosos, e é por isso que acontece um dos cibercrimes *(cybercrimes)* mais prejudiciais atualmente: o vazamento de dados (FAVERO, A. e FAVERO, B., 2021).

Pequenas empresas estão sujeitas a ataques de criminosos digitais, porém o foco principal é o ataque a grandes companhias, alguns casos de vazamento tiveram um grande impacto no Brasil e no mundo, como os ataques bem-sucedidos a Netflix, LinkedIn, Runescape e Minecraft em 2017 onde foi encontrado um arquivo que reunia mais de 1,4 bilhões de nomes de usuários e senhas, esse arquivo era constantemente atualizado e disponibilizado para download (UOL, 2017).

No início do ano de 2021, no Brasil houve um mega vazamento de informação onde foi disponibilizado para download um pacote de dados que incluía número de CPF, informações sobre veículos cadastrados no Brasil, foto do rosto, endereço completo, score de crédito, salário, nome completo e data de nascimento sobre mais de 223 milhões de brasileiros, o número chamou atenção devido a ultrapassar até mesmo o da população brasileira (MAZZO, 2021).

2.2 Trabalhos Relacionados

Este tópico apresenta algumas publicações científicas que mostram resultados significativos, que estão relacionados com o tema deste trabalho, apresentando os estudos de Rodrigues Jr. *et al*. (2021), Souza *et al*. (2018), Almubayedh *et al*. (2018), Iakovakis *et al*. (2021), Lallie *et al.* (2021) e Nurse *et al.* (2021) e por fim sendo exposto um comparativo dos estudos abordados.

2.2.1 Rodrigues Jr. *et al*. (2021)

O trabalho teve como objetivo informar e apresentar práticas que possam auxiliar na manutenção da segurança cibernética no home office, utilizando como metodologia a revisão de literatura (RODRIGUES Jr. *et al*.,2021).

Com as novas regulamentações, Lei Geral de Proteção de Dados (LGPD) e *General Data Protection Regulation* (GDPR – regulamentada pela União Europeia) as empresas têm

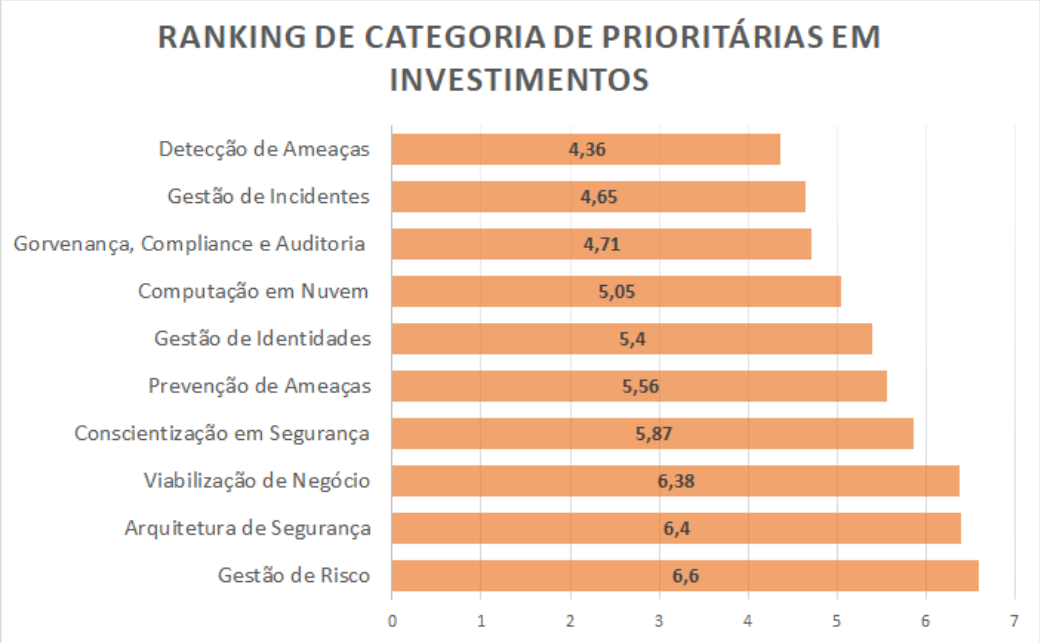
se importado cada vez mais com a questão da segurança cibernética, mas ainda possui um longo caminho a ser percorrido (RODRIGUES Jr. *et al*.,2021).

Utilizou um levantamento feito pela *Tempest Security Intelligence*, no Brasil, publicado no site *cryptoid.com.br*, em mais de 15 segmentos do mercado brasileiro (RODRIGUES Jr. *et al*.,2021).

Segundo a pesquisa, mais da metade das empresas declaram que o orçamento anual para segurança da informação representa até 2% do faturamento anual. Destas, 34.5% afirmam que o investimento não ultrapassa 1%. Porém, em 2019, 38,8% das empresas ouvidas afirmaram a expectativa no incremento dos investimentos em até 20%. Por outro lado, 30,9% afirmam que a variação positiva não deve passar dos 5% (RODRIGUES Jr. *et al*.,2021).

A gestão de riscos está no topo das prioridades de investimentos entre os participantes do estudo como visto na Figura 4. Seguido da Arquitetura de Segurança e Prevenção de Ameaças (RODRIGUES Jr. *et al*.,2021).

Figura 4 - Ranking de Categorias Prioritárias em Investimentos



Fonte: Rodrigues Jr. *et al.* (2021).

Destaca-se que com a pandemia COVID-19 empresas de vários segmentos de diversas partes do mundo têm adotado o home office como modelo de trabalho, porém é necessário realizar este processo de maneira segura do ponto de vista empresarial. Compreendendo isto, muitas empresas têm suas primeiras experiências neste modo de trabalho agora, em um cenário cheio de desafios e modelos diferentes (RODRIGUES Jr. *et al*.,2021).

Teve como resultado, a lista de fatores que estão ligados à segurança da informação para o trabalho em home office e que devem ser observados, que são eles: O uso de diferentes credenciais para laptops com finalidades diferentes (pessoal e trabalho) para proporcionar maior segurança nas informações da empresa, utilização de antivírus e mantê-lo atualizado, evitar uso de pendrives e HD's externos com o objetivo preservar os dados contidos no laptop pois os mesmo podem ser a causa de uma infecção e por isso devem ser evitadas e utilizar somente software originais (RODRIGUES Jr. *et al*.,2021).

2.2.2 Souza *et al.* (2018)

Souza *et al.* (2018) em seu artigo teve como objetivo geral compreender os mecanismos de segurança de informação utilizados na atuação de possíveis ameaças no ambiente organizacional de uma empresa que atua oferecendo serviços de planos de saúde na cidade de Mossoró, Rio Grande do Norte.

A pesquisa possui natureza descritiva e qualitativa, realizada por meio de entrevistas, utilizando a Análise do Núcleo de Sentidos (ANS) como método de análise dos dados (SOUZA *et al*., 2018).

Para a realização da pesquisa os autores elaboraram um questionário contendo 10 questões, objetivando identificar os mecanismos de segurança utilizados e as possíveis ameaças presentes na organização. A pesquisa foi realizada por meio de um dos pesquisadores, onde foi realizada uma entrevista presencial com um analista de sistemas e um gestor do departamento de TI. A coleta dos dados se deu por meio de gravações das falas, sendo realizadas no mês de setembro de 2017. Na Tabela 1 é apresentado as características dos participantes (SOUZA *et al*., 2018).

Tabela 1 - Caracterização dos sujeitos e pesquisa

Código do entrevistado	Sexo	Idade	Escolaridade	Cargo	Tempo de Trabalho na Organização
E1	M	38	Pós-Graduado	Gerente de TI	14 anos e 2 meses
E2	M	37	Graduado em SI	Analista de Sistemas	3 anos e 5 meses

Fonte: Souza *et al*., (2018).

Com a realização do presente estudo foi possível concluir que a organização alvo da pesquisa utiliza mecanismos de segurança comuns, os quais se encontram presentes na maioria das organizações, porém ela possui limitações em demonstrar que não inovam em recursos de segurança, e acabam dependendo apenas dos já existentes (SOUZA *et al*., 2018).

O setor de TI da organização também não realiza tarefas importantes para diminuir a exposição de riscos que venham a surgir com mudanças nos requisitos das atividades do negócio, não seguindo nenhum conjunto de normas, e apresentando também pouco conhecimento sobre o assunto conforme mostram as falas dos entrevistados, mantendo assim um processo informal de segurança de informação, e mostrando a necessidade de aprofundamento no assunto por parte do setor de TI da organização (SOUZA *et al*., 2018).

2.2.3 Almubayedh *et al*. (2018)

Almubayedh *et al*. (2018) no seu trabalho considera uma pequena organização saudita para realizar um estudo de caso, o propósito de sua pesquisa é de auditar o estado e descrever os possíveis cenários de risco que possam ocorrer. Sua coleta de dados ocorreu principalmente por meio de entrevistas com o CEO da empresa.

A auditoria foi realizada em várias fases e segue os padrões da ISACA. A principal metodologia seguida na auditoria foi entrevista, comunicação por e-mail e telefonemas com o CEO da organização XYZ. Com o objetivo de visualizar a política da organização XYZ para verificar os controles de segurança atuais, detectar quais são os cenários de risco, coletar informações para verificar a conscientização dos funcionários sobre as políticas e procedimentos e encontrar as questões relacionadas à segurança da informação na organização (ALMUBAYEDH *et al*., 2018).

A auditoria tem início pela análise das informações coletadas do processo da organização e do sistema de informação, para realizar uma avaliação de risco qualitativa ou quantitativa, identificando quais são os possíveis fatores de risco que influenciam um cenário de risco para garantir que as áreas-chave da organização sejam afetadas. Com base nas informações fornecidas pelo CEO da organização XYZ (ALMUBAYEDH *et al*., 2018).

A auditoria encontrou cinco cenários de risco possíveis, nomeados à falta de política de segurança, vazamento de informações pessoais do site, o risco de danos no dispositivo do CEO e dois cenários relacionados a empresas de terceirização (ALMUBAYEDH *et al*., 2018).

Os resultados da análise mostram que existem muitos problemas relacionados às práticas de segurança na organização. Conforme mostrado no primeiro cenário de risco, a organização carece de uma política de segurança formal o que a expõe a muitas ameaças diferentes (ALMUBAYEDH *et al*., 2018).

Almubayedh *et al*. (2018) teve como resultado, recomendações para que as pequenas empresas tenham políticas e procedimentos de segurança abrangentes e formais documentados de acordo com os padrões ISO / IEC 27001 atualizados, revisados e formalmente aprovados pelo CEO com a ajuda de especialistas em segurança. Algumas áreas importantes recomendadas para serem cobertas pelas políticas e procedimentos de segurança:

- **Política antivírus**
- **Política de senha**
- **Uso aceitável de ativos**
- **Uso da política de internet**

2.2.4 Iakovakis *et al.* (2021)

O trabalho tem como objetivo, analisar e classificar ferramentas que facilitarão a mitigação e a prevenção de riscos relacionados à segurança da informação no home office. Utilizou a metodologia de pesquisa bibliográfica (IAKOVAKIS et al., 2021).

O surto de COVID-19 forçou as empresas a recorrer a um ambiente de negócios de "trabalho em casa" sem precedentes. Embora isso traga benefícios para funcionários e empresas, também leva a várias desvantagens, sendo a mais comum o surgimento de riscos de segurança adicionais. Antes do surto, a rede de computadores da empresa estava confinada principalmente às suas instalações. A pandemia agora fez com que a rede “se espalhasse”, já que a maioria dos funcionários trabalha remotamente. Isso abre todos os tipos de novas vulnerabilidades, pois a proteção cibernética dos funcionários é diferente em casa e no escritório (IAKOVAKIS et al., 2021).

Desta forma, este trabalho tem como resultado fornecer uma classificação detalhada de grupos de ferramentas automatizadas totalizando 25 ferramentas de vulnerabilidade, 25 ferramentas de monitoramento e registro, 14 ferramentas de software antivírus. Também descreveu vantagens, desvantagens, custo e outras características de cada ferramenta recomendada. Além disso, foi implementada árvores de decisão para cada categoria de ferramentas, na tentativa de auxiliar na navegação da grande quantidade de informações presente no trabalho (IAKOVAKIS et al., 2021).

2.2.5 Lallie *et al.* (2021)

O trabalho tem como objetivo, analisar a pandemia do Covid-19 a partir de uma perspectiva de crimes cibernéticos e destacam a gama de ataques cibernéticos experimentados globalmente durante a pandemia. Usando como metodologia uma revisão da literatura para identificar ataques cibernéticos no período de março a maio de 2020 (LALLIE *et al.*,2021).

O home office durante a pandemia ocorreu de forma massiva. O que resultou no nível de problemas e desafios de segurança cibernética que a indústria e as pessoas nunca enfrentaram antes. Os cibercriminosos aproveitam as oportunidades. Para tanto, em 8 de abril de 2020, o Centro Nacional de Segurança Cibernética do Reino Unido e o Padrão Departamental dos EUA destacando ataques e atividades cibernéticas em todos os lugares do mundo, fica claro que o crime cibernético assume a forma de engenharia social para criar essas vulnerabilidades (LALLIE *et al.*,2021).

Como resultado, foram obtidos padrões de ataques cibernéticos ocorridos nesse período. Foi identificado que os criminosos usufruíram da mídia e do governo para aumentar as chances de sucesso por meio de campanhas de phishing (LALLIE *et al.*,2021).

2.2.6 Nurse *et al.* (2021)

O trabalho teve como objetivo fazer uma análise das questões de segurança cibernética e privacidade do trabalho remoto durante o período da pandemia. Verificou como as organizações trabalhavam em home office antes da pandemia e o que mudou durante a pandemia (NURSE *et al.*,2021).

A metodologia utilizada foi a revisão da literatura. Foram considerados particularmente relatórios da indústria antes da pandemia, para identificar o que verdadeiramente mudou em relação ao risco da informação e da privacidade no que diz respeito ao home office pré e pós -COVID-19 (NURSE *et al.*,2021).

Como resultado, obteve uma série de riscos relacionados com o home office. As organizações, com a finalidade de dar continuidade aos negócios, adotaram o home office de modo muito apressado, o que ocasionou no vazamento de informações corporativos durante o período de pandemia. Porém foi identificado que muitos dos riscos foram corrigidos ao passar do tempo, e como outras organizações se adaptaram muito bem ao trabalho em ambiente doméstico. Uma parcela das corporações indicou que continuará com o home office mesmo no pós-COVID-19 (NURSE *et al.*,2021).

2.2.7 Comparativo dos Trabalhos Relacionados

A **Tabela 2** apresenta a diferença entre os trabalhos relacionados com a proposta deste trabalho. A tabela possui um total de 6 (seis) trabalhos relacionados que foram classificados

de acordo com sua importância para este trabalho proposto sendo que o trabalho de Rodrigues Jr. a principal base para as questões do home office.

Tabela 2- Comparativo nos trabalhos relacionados

Trabalhos Relacionados	Comparativo
Rodrigues Jr. *et al.* (2021)	Rodrigues Jr. *et al.* (2021), teve como objetivo informar e apresentar práticas que possam auxiliar na manutenção da segurança cibernética no home office, utilizando como metodologia a revisão de literatura. Este trabalho busca identificar os principais desafios enfrentados na segurança da informação no ambiente de home office, utilizando MS.
Souza *et al.* (2018)	Souza *et al.* (2018), teve como objetivo geral compreender os mecanismos de segurança de informação utilizados na atuação de possíveis ameaças no ambiente organizacional de uma empresa que atua oferecendo serviços de planos de saúde na cidade de Mossoró, Rio Grande do Norte. Enquanto este trabalho irá identificar os principais desafios que as organizações enfrentam com relação à segurança da informação.
Almubayedh *et al.* (2018)	Almubayedh *et al.* (2018), considera uma pequena organização saudita para realizar um estudo de caso, para auditar seu estado e descrever os possíveis cenários de risco que possam ocorrer. A principal metodologia seguida na auditoria foi entrevista, comunicação por e-mail e telefonemas com o CEO da organização. Ao passo que este trabalho busca identificar as principais dificuldades que as organizações brasileiras enfrentam em relação à segurança da informação, utilizando metodologias como MS.
Iakovakis *et al.* (2021)	Iakovakis *et al.* (2021), teve como objetivo fornecer uma gama de ferramentas que auxiliam na mitigação e na prevenção de risco relacionado a segurança da informação no home office. Enquanto este trabalho busca detectar os problemas que ocorrem tanto dentro do ambiente de trabalho e realizar uma pesquisa de opinião para validar.
Lallie *et al.* (2021)	Lallie *et al.* (2021), possui como objetivo fornecer padrões de ataques que criminosos virtuais mais utilizaram na pandemia. Enquanto este trabalho irá focar nas dificuldades que as organizações enfrentam em relação a segurança da informação no ambiente organizacional e no home office, utilizando MS e pesquisa de opinião.
Nurse *et al.* (2021)	Nurse *et al.* (2021), possui o objetivo de identificar as mudanças reais no home office na pré e pós pandemia. Ao passo que este trabalho busca identificar os principais desafios enfrentados pelas organizações em relação a segurança da informação tanto no ambiente organizacional quanto no home office, utilizando MS e pesquisa de opinião.

Fonte: O autor (2022).

3. SEGURANÇA DA INFORMAÇÃO NO HOME OFFICE

Neste capítulo são descritos os resultados parciais, onde é definida a primeira etapa do MS, onde são listadas as questões de pesquisa, fonte, idioma, expressão de busca, critérios de seleção e a extração dos dados.

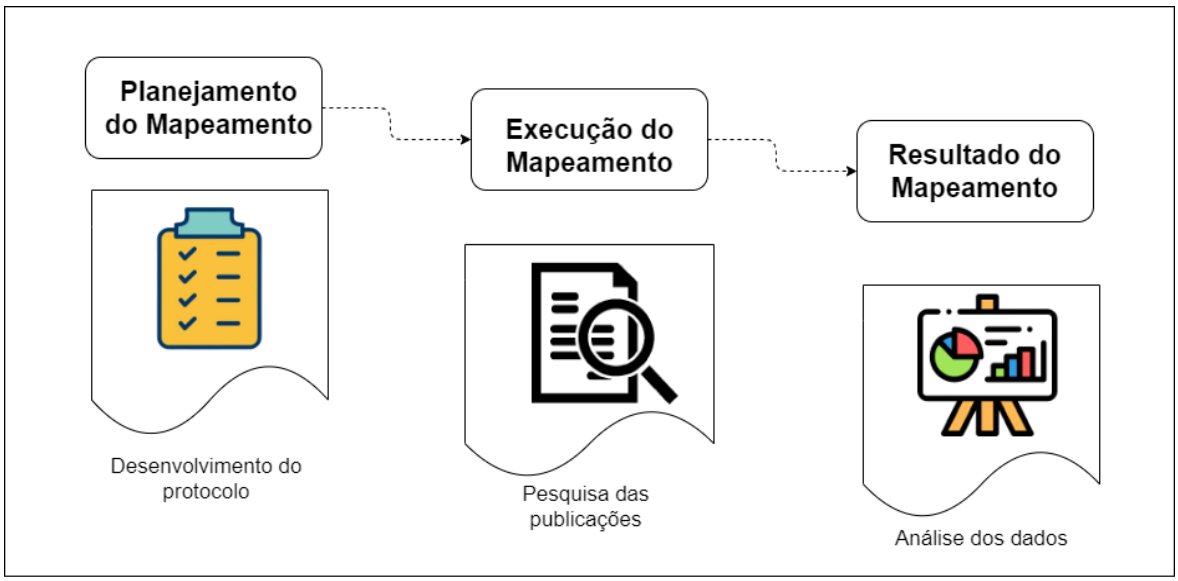
3.1 Mapeamento Sistemático

O MS fornece uma visão geral de uma área de pesquisa, identificando a quantidade, os tipos de pesquisas realizadas, os resultados disponíveis, além das frequências de publicações ao longo do tempo para identificar tendências (PETERSEN *et al.*, 2008).

Tomando como base os *guidelines* desenvolvido por Kitchenham e Charter (2007) o processo é desenvolvido em três etapas: Planejamento do Mapeamento, Condução do Mapeamento e Resultado do Mapeamento, conforme apresentado na Figura 5.

O planejamento do mapeamento é a parte em que o objetivo de pesquisa é listado e o protocolo do mapeamento é definido. A condução do mapeamento é a sequência que é selecionada as fontes para o mapeamento, os estudos primários identificados, selecionados e avaliados de acordo com os critérios de inclusão, exclusão, e de qualidade estabelecidos durante o protocolo. O resultado do mapeamento, nessa fase os dados do estudo são extraídos e sintetizados para serem publicados.

Figura 5 - Etapas do mapeamento sistemático



Fonte: O autor (2022).

Estudos de MS, em Engenharia de Software, têm sido recomendados, principalmente nas áreas de pesquisa onde há falta de importância de estudos relevantes e de alta qualidade (KITCHENHAM e CHARTERS, 2007).

3.2 Planejamento do Mapeamento Sistemático

Nesta etapa é definido a estrutura do protocolo que foi baseada nos trabalhos de Kitchenham e Charters (2007), neste processo é necessário definir o objetivo do estudo, especificar as questões da pesquisa, expressão de busca, além de mencionar os procedimentos de extração dos dados e os critérios de seleção de cada publicação conforme descrito a seguir.

3.2.1 Objetivo e Questão de Pesquisa

O objetivo deste MS é analisar as publicações científicas com o propósito de identificar os desafios enfrentados pelas organizações em relação à segurança da informação.

- **[QP1]:** Quais são as vulnerabilidades/ameaças encontradas nas organizações no modo home office a respeito da segurança da informação?
- **[QP2]:** Quais são as práticas de segurança da informação mais adotadas nas organizações com relação em home office?

3.2.2 Idiomas e Fontes de Publicação

Para a realização da pesquisa serão selecionados os idiomas inglês e português. O idioma inglês justifica-se pela maioria das publicações relacionada ao tema pesquisado ser deste idioma. A escolha do idioma português deve-se pelas principais conferências nacionais da área da segurança da informação.

As fontes de busca são definidas em fontes digitais e manuais. As fontes digitais são acessadas via web, através de expressões de busca pré-estabelecidas. As publicações das fontes não digitais serão analisadas manualmente, quando disponíveis e considerando a expressão de busca definida. A seguir é apresentado as fontes digitais e manuais:

Fontes Digitais:

- Scopus < https://www.scopus.com/>
- Google Acadêmico < https://scholar.google.com.br>

Fontes Manuais:

- Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais (SBSeg)
- Simpósio Brasileiro de Sistemas de Informação (SBSI)

3.2.3 Expressão de Busca e Critério de Seleção

A busca foi restringida usando-se palavras-chave específicas para encontrar as publicações de interesse. A expressão de busca é apresentada na Tabela 3, enquanto a seleção das publicações será realizada em duas etapas.

Tabela 3 - Palavras-Chave

Português
“Segurança da Informação” OR “Segurança de dados” OR “Segurança da Organização” OR “Segurança Digital” OR “Ameaças de Segurança da Informação” OR “Vulnerabilidades a Segurança da Informação” OR “Políticas de Segurança da Informação” OR “Home Office” OR “Segurança no Home Office”.
Inglês
"Information Security"OR "Data Security"OR "Organization Security"OR "Digital Security" OR "Information Security Threats" OR "Information Security Vulnerabilities" OR "Information Security Policies" OR “Security Home Office” OR “Home Office”.

Fonte: O autor (2022)

- 1ª Etapa: Das publicações selecionadas conforme a busca nas fontes, serão lidos o resumo e as palavras-chave. Portanto, será aplicado o critério de seleção 1: *CS1: Estudos que relatam, citam ou analisam aspectos sobre segurança da informação*.
- 2ª Etapa: Conforme o resultado das publicações da 1ª etapa serão lidos na íntegra e somente serão selecionadas aquelas que atenderem ao critério de seleção 2: *CS2: A publicação deve citar as ameaças/vulnerabilidades e/ou práticas de segurança da informação no ambiente home office.*

3.2.4 Extração de Dados

O procedimento de extração de dados é o passo essencial, dessa forma serão extraídas informações de publicações relevantes, que foram registradas em tabelas, conforme descritos na Tabela 4.

Tabela 4 - Extração dos dados

IDENTIFICADOR	Indica o ID da publicação
A. DADOS DA PUBLICAÇÃO:	
Título	Indica o título do trabalho
Autor(es)	Nome dos autores
Fonte de Publicação	Local de publicação
Ano de Publicação	Ano de publicação
Resumo:	Texto contendo uma descrição do resumo
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	Descrição das ameaças à segurança
Vulnerabilidades nas organizações	Descrição das vulnerabilidades a segurança
Práticas adotadas para a segurança da informação	Práticas adotadas pelas organizações para proteção da segurança dos dados
C. DADOS ADICIONAIS:	
Metodologia adotada	Descrição do método usado na pesquisa para atingir o objetivo

Fonte: O autor (2022).

3.3 Condução do Mapeamento Sistemático

Finalizado a etapa de planejamento, foi executado expressão de busca nas fontes definidas no mês agosto de 2021 a setembro de 2021 e as publicações foram selecionadas de acordo com os critérios de seleção estabelecidos durante o protocolo do Mapeamento Sistemático. O período dos trabalhos publicados foi dos últimos 10 anos.

A Tabela 5 apresenta as informações do 1º Filtro e 2º Filtro para as 4 fontes definidas. Como é possível notar foram retornadas 270 publicações, sendo que a fonte que retornou mais publicações durante o período de 2011-2021 foi a Scopus com 152, seguida do Google Acadêmico com 110.

Tabela 5 - Publicações encontradas por etapa

Nome	Busca	1º Filtro	2º Filtro
Scopus	152	10	5
Google Acadêmico	110	12	4
SBSeg	5	2	0
SBSI	3	1	0
TOTAL	270	25	9

Fonte: O Autor (2022).

Para essas 270 publicações, foram lidos o resumo e as palavras-chaves e 25 publicações foram selecionadas de acordo com o CS1: “Estudos que relatam, citam ou analisam aspectos sobre segurança da informação.”. A partir disso, as 25 publicações foram lidas na íntegra e somente foram selecionadas as que atendiam o CS2: “A publicação deve citar as ameaças/vulnerabilidades e/ou práticas de segurança da informação no ambiente home office.”, retornando 9 publicações. A Tabela 6 Tabela 6 - Publicações selecionadasapresenta a lista das publicações que foram analisadas para responder às duas questões de pesquisa definidas no protocolo do mapeamento, a tabela possui: ID (identificação), Título, Autores, e Ano e Fonte.

Tabela 6 - Publicações selecionadas

ID	Título	Autores	Ano	Fonte
A01	Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review	Khando, K.; Gao, S.; Islam, S. e Salman, A.	2021	Google Acadêmico
A02	Remote Working Pre and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy	Nurse, J.; Williams, N.; Collins, E.; Panteli, N.; Blythe, J. e Koppelman, B.	2021	Scopus
A03	Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime	Lallie, H.; Shepherd, L.; Nurse, J.; Eola, A.;	2021	Scopus

	and Cyber-Attacks During the Pandemic	Epiphaniou, G.; Maple, C. e Bellekens, X.		
A04	Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era	Iakovakis, G.; Xarhoulacos, C.; Giovas, K. e Gritzalis, D.	2021	Scopus
A05	Home Office e a Segurança da Informação em Tempos de Pandemia	Rodrigues, JR.; Nogueira, E.; Mendes, G. & Campos, L.	2021	Google Acadêmico
A06	Securing your Remote Workforce Against new Phishing Attacks. Computer Fraud & Security	Sarginson, N.	2020	Scopus
A07	Network Attacks and Prevention Techniques - A Study	Kandan, A.; Kathrine, G., & Melvin, A.	2019	Scopus
A08	Information Security Strategy and Teleworking (in)security	Ampomah, M., De Silva, Y., Li, H., Pahlisa, P., Yang, Q., & Zhang, Q.	2013	Google Acadêmico
A09	Security Risks in Teleworking: A Review and Analysi	Yang, H.; Zheng, C.; Zhu, L.; Chen, F.; Zhao, Y. & Valluri, M.	2013	Google Acadêmico

Fonte: O Autor (2022).

3.4 Resultado e Análise do Mapeamento Sistemático

Após a etapa da condução do mapeamento sistemático, foi realizada a última fase, que se trata da apresentação da análise dos resultados. Com as informações obtidas nas 9 publicações selecionadas, foi possível responder às questões de pesquisa definidas no protocolo. Todas as publicações foram analisadas de forma manual preenchendo as lacunas sugeridas, é possível verificar a extração do mapeamento sistemático no Apêndice A.

Com relação à 1ª questão de pesquisa: "Quais são as vulnerabilidades/ameaças encontradas nas organizações no modo home office a respeito da segurança da informação?"

Para responder a primeira questão de pesquisa o resultado foi dividido em duas tabelas: a primeira apresenta o resultado da identificação das vulnerabilidades e a segunda apresenta a identificação das ameaças.

A Tabela 7, apresenta as 8 vulnerabilidades identificadas no mapeamento sistemático e que foram citadas, por no mínimo, em 3 publicações. Em segurança da informação a vulnerabilidade ou falha de segurança é uma fraqueza que permite que um invasor consiga acesso a tal informação (KHANDO *et al*., 2021).

Tabela 7 - Vulnerabilidades Identificadas

ID	Vulnerabilidades	Artigos	%
[VN1]	Dispositivo pessoal para trabalho	[A02], [A04], [A05], [A06], [A08], [A09]	67%
[VN2]	Acesso a sites inseguros	[A04], [A05], [A06], [A07], [A09]	56%
[VN3]	Rede de acesso insegura	[A05], [A06], [A08], [A09]	44%
[VN4]	Dificuldades de comunicação	[A02], [A08], [A09]	33%
[VN5]	Falta de treinamento de segurança para trabalho remoto	[A02], [A08], [A09]	33%
[VN6]	Comprometimento organizacional deficiente	[A01], [A03], [A08]	33%
[VN7]	Descarte inapropriado de dados confidenciais	[A01], [A02], [A09]	33%
[VN8]	Divulgação de informações sigilosas	[A05], [A08], [A09]	33%

Fonte: O Autor (2022).

De acordo com os dados obtidos na Tabela 7, a vulnerabilidade “dispositivo pessoal para trabalho” ([VN1]), foi citada em 6 (67%) das publicações selecionadas, tornando-se a vulnerabilidade de maior importância, pois os computadores podem conter muitas informações confidenciais da organização ou projeto, o que o torna em alvo de possíveis ataques como o roubo e fraudes virtuais.

Os dispositivos de trabalho podem ser roubados da área de trabalho remota. Se esses dispositivos não forem criptografados adequadamente, eles podem representar um risco para as organizações tendo o potencial de ter seus serviços, acessos e informações expostas. Durante a pandemia da COVID-19, essa vulnerabilidade tornou-se um motivo de muita preocupação pois os criminosos, invasores e pessoas mal-intencionadas sabem que a maioria das pessoas trabalhará remotamente e, portanto, provavelmente terão mais tecnologia móvel em casa (NURSE *et al*., 2021).

A segunda vulnerabilidade mais citada é “acesso a sites inseguros” ([VN2]), foi citada em 5 (56%) das publicações selecionadas. Em sites inseguros os dados do dispositivo podem ser comprometidos e o navegador pode ser infectado possibilitando acesso não autorizado ao computador.

Os ataques de rede baseados em navegador são um tipo de ataque muito frequente e comum, tentam comprometer uma máquina através de um navegador da web. Os invasores comprometem um site e o infectam com malwares. Quando novos indivíduos chegam (através de qualquer navegador da web), os sites infectados tentam forçar o malware em seus sistemas manipulando pontos fracos no navegador (KANDAN; KATHRINE e MELVIN, 2019).

A vulnerabilidade “rede de acesso insegura” ([VN3]), foi a terceira mais citada com 4 (44%) das publicações selecionadas. Quando não há uma rede configurada e com todos os protocolos para impedir acessos não autorizados, a rede se torna insegura o que possibilita monitoramento não autenticado e vazamentos de dados.

Trabalhadores remotos de pequenas empresas que armazenam dados na nuvem e usam *wi-fi*, conexões de internet sem fio, são comuns pois não requer grandes investimentos para o uso, porém sem conhecimento técnico apropriado para a manter segura e confiável proporcionará oportunidades para hackers acessarem o sistema e introduzir vírus por meio de uma conexão de internet insegura ou *pendrives* usados por outros na casa (YANG *et al*., 2013).

A vulnerabilidade “dificuldades de comunicação” ([VN4]), foi citada em 3 (33%) das publicações selecionadas. O home office permitiu a continuidade do trabalho, porém quando o assunto é reunião, manter contato ou realizar um vídeo chamada urgente, muitos imprevistos podem acontecer como, por exemplo, interrupção no fornecimento de energia.

Dificuldade em discutir rapidamente os comportamentos de segurança apropriados com colegas quando confrontados com decisões relacionadas a informações sigilosas podem permitir uma má prática de segurança da informação. O problema é agravado pelo tempo que os funcionários têm para trabalhar remotamente e pela diferença psicológica de "aparecer" na mesa de um colega de trabalho ou "interromper seu trabalho" solicitando uma videochamada (NURSE *et al*., 2021).

A vulnerabilidade “falta de treinamento de segurança para trabalho remoto” ([VN5), foi citada em 3 (33%) das publicações selecionadas. A ausência no preparo dos funcionários para lidar com a segurança de informações confidenciais da organização no ambiente doméstico é uma grande preocupação pois esse despreparo é a causa de muitas oportunidades de ataques ou vazamentos de informações privilegiadas.

A maioria das violações de segurança da informação é causada pela falta de conhecimento dos funcionários. Os trabalhadores remotos muitas vezes não sabem que são uma fonte potencial de vulnerabilidade à segurança da informação da organização. Por exemplo, um indivíduo no home office pode reforçar suas credenciais para acessar os sistemas de uma organização em um pedaço de papel deixado em cima da mesa de trabalho, sem saber dos perigos de fazê-lo (YANG *et al*., 2013).

A vulnerabilidade “comprometimento organizacional deficiente” ([VN6]), foi citada em 3 (33%) das publicações selecionadas. A organização busca proteger seus dados sensíveis de ataques externos, porém muitas vezes não consegue fornecer uma estrutura segura para seus funcionários que estão no home office, devido a isso é comum que ocorram violações na segurança dos dados por terceiros.

A assistência técnica insuficiente aos trabalhadores remotos por parte das organizações contribuiu muito para a intercepção de dados válidos e causa uma grave perda de informação, o que pode levar a défices financeiros. Isso ocorre porque as equipes de suporte de TIC podem priorizar problemas relacionados a TIC, como ataques de vírus a funcionários que são realmente visíveis para a equipe de suporte em vez de trabalhadores remotos. Como resultado, indivíduos que trabalham no home office podem não receber o mesmo nível de suporte de segurança que os trabalhadores do local de trabalho (AMPOMAH *et al.*, 2013).

A vulnerabilidade “descarte inapropriado de dados confidenciais” ([VN7]), foi citada em 3 (33%) das publicações selecionadas. Essa vulnerabilidade teve seu auge durante a pandemia, pois para muitos trouxe a sensação de isolamento e isto foi mais agravante para os que tiveram que trabalhar no modo home office pois tal sentimento contribuiu com o descuido no descarte seguro de informações.

Os trabalhadores remotos são facilmente isolados da organização e dos colegas, podem ficar frustrados ou descuidados com os interesses da organização e podem não ter o cuidado de proteger as informações confidenciais, por exemplo, realizar o descarte inapropriado de informações sigilosas, o que significa que podem mais vulnerável a ataques, ser hackeado ou ter seus equipamentos de trabalho roubados (KHANDO *et al.*, 2021).

A vulnerabilidade “divulgação de informações sigilosas” ([VN8]), foi citada em 3 (33%) das publicações selecionadas. No ambiente de trabalho na organização, só transitam pessoas previamente autorizadas, mas no home office isso não ocorre já que pessoas confiáveis e não confiáveis podem transitar no ambiente de trabalho doméstico podendo ter acesso a várias informações de dados sigilosos.

Indivíduos confiáveis e não confiáveis em um ambiente de trabalho remoto podem aproveitar o novo acesso a dados ou serviços da organização, por exemplo, usando um laptop ou telefone desbloqueado ou ouvindo chamadas confidenciais. A realidade é que esses ambientes podem ser compartilhados com colegas de quarto mal-intencionados ou outros que

podem estar aproveitando esse período prolongado de trabalho em casa para fins malévolos (NURSE *et al*., 2021).

A Tabela 8 apresenta as 8 ameaças identificadas no mapeamento sistemático e que foram citadas, por no mínimo, em 3 publicações. Uma ameaça à segurança da informação é uma ação capaz de interferir e causar danos à integridade, à confidencialidade, à autenticidade e a disponibilidade das informações (KHANDO *et al*., 2021).

Tabela 8 - Ameaças identificadas

ID	Ameaças	Artigos	%
[AM1]	Interceptação de dados por meio da engenharia social	[A01], [A03], [A06], [A07], [A08]	56%
[AM2]	Ataque malwares	[A03], [A04], [A05], [A07], [A08]	56%
[AM3]	*Hacking*	[A02], [A03], [A05], [A08], [A09]	56%
[AM4]	E-mails fraudulentos	[A03], [A04], [A05], [A06]	44%
[AM5]	*Phishing*	[A03], [A04], [A05], [A06]	44%
[AM6]	*Ransomware*	[A03], [A04], [A07], [A08]	44%
[AM7]	Ataques a portas do firewall	[A02], [A05], [A07], [A09]	44%
[AM8]	Sites fraudulentos	[A03], [A04], [A05]	33%

Fonte: O Autor (2022).

De acordo com os dados obtidos na Tabela 8, a ameaça "interceptação de dados por meio da engenharia social" ([AM1]), foi citada em 5 (56%) das publicações selecionadas. Atualmente novos métodos de ataques a informações confidenciais surgem a todo dia, porém métodos como a engenharia social ainda são bastante utilizados visando indivíduos com pouco ou nenhum conhecimento sobre a importância das informações que possuem.

Embora os métodos de roubo de informação tenham se tornado mais sofisticados e direcionados a vítimas específicas, ataques oportunistas não direcionados também são muito prevalentes. Estes são definidos como ataques que selecionam os indivíduos com base em sua suscetibilidade de ser uma potencial vítima. Os criminosos virtuais encontram alguma vulnerabilidade na vítima e usam métodos como a engenharia social, para criar oportunidades (LALLIE *et al.*, 2021).

A ameaça "Ataque malwares" ([AM2]), foi citado em 5 (56%) das publicações selecionadas. Malware refere-se a softwares maliciosos e podem ser usados para interromper serviços, extração de dados e entre outras formas de uso, eles podem ser propagados por diversos meios como *pen drive*, e-mails, sites.

Sem dúvidas ataques de malwares obteve elevado aumento durante a pandemia. Softwares disfarçados de aplicativos relacionados ao COVID-19 desfrutavam do momento de muita desinformação sobre o novo patógeno, desse modo diversos indivíduos e organizações

foram afetados. Os principais malwares eram SpyMax, Pysa e outros que estavam disfarçados como aplicativos, por exemplo, (Corona Live 1.1, CoronaVirus Map e COVIDLOCK) (IAKOVAKIS *et al.*, 2021).

A ameaça "*Hacking*" ([AM3]), foi citado em 5 (56%) das publicações selecionadas enquanto "Ransomware" ([AM6]), foi citado em 4 (44%) das publicações citadas. Durante o período de pandemia os ataques de *hackers* aumentaram bastante e esses ataques em sua grande maioria estavam direcionados para grandes centros de pesquisa e muitos desses tinham como objetivo o sequestro de dados valiosos para posteriormente exigirem resgate.

Hacking envolve comprometer a confidencialidade e integridade de um sistema e requer um nível razoável de habilidade, cujas técnicas podem envolver a exploração de uma vulnerabilidade do sistema para invadir. *Ransomware* é um tipo de ataque malicioso que combina malware com uma tentativa de extorsão. Durante a pandemia do COVID-19, muitos casos de *ransomware* ficaram conhecidos, como o COVIDLock, um aplicativo Android disfarçado que fornece mapas de calor, pontos críticos de surtos e estatísticas sobre a pandemia, o aplicativo requer algumas permissões, entre elas o bloqueio tela do usuário e posteriormente a tela do dispositivo era bloqueada e exigia pagamento para desbloquear (LALLIE *et al.*, 2021).

A ameaça "phishing" ([AM5]), foi citada em 4 (44%) dos artigos selecionados, "sites fraudulentos" ([AM8]), foi citado 3 (33%) dos artigos selecionados e a ameaça "E-mails fraudulentos" ([AM4]), foi citado em 4 (44%) dos artigos selecionados. O *pshishing* tem uma alta capacidade de se diversificar e evoluir continuamente por utilizar sites fraudulentos e estar sempre dentro de assuntos da atualidade para se propagar. Com o objetivo de roubar dados pessoais, dados bancários ou dados confidenciais, os *cibercriminosos* usam o método de *phishing*, que é essencialmente uma forma de roubo de identidade da vítima. Os criminosos usam e-mails, sites e aplicativos projetados para o roubo de dados (IAKOVAKIS *et al.*, 2021).

Com a COVID-19, muitas pessoas ao redor do mundo buscaram informações para prevenir, combater ou tratar os sintomas. Em meio a essa procura por informações muitos ataques cibernéticos começaram com campanhas de *phishing* que direcionam as vítimas para baixar um arquivo ou visitar *url*. Os e-mails são muito utilizados como um meio de transmissão para enviar *links* ou arquivos maliciosos. Para aumentar sua credibilidade muitos *phishing* tentavam se passar por sites confiáveis como o da organização mundial de saúde

(OMS). Os *phising* e sites fraudulentos são uma combinação bastante usada por criminosos virtuais, pois são de baixo custo e têm uma taxa de sucesso razoável (SARGINSON, 2020).

A ameaça "ataques a portas do firewall" ([AM7]), foi citada 4 (44%) das publicações selecionadas. O firewall é uma proteção que fica entre o computador e o link de comunicação tem como objetivo filtrar e impedir o acesso de conteúdos maliciosos sem impedir o fluxo normal de dados, pode ocorrer que alguma porta fique aberta o que possibilita um acesso não autorizado ou a quebra de firewall.

Os invasores costumam usar a varredura de portas como um passo inicial para atacar a rede, portanto, a varredura de portas é usada para avaliar o nível de segurança de várias organizações e descobrir firewalls fortes e servidores ou redes mais vulneráveis. Quando encontram uma porta aberta, seja porque alguém utilizou aquele canal específico e descuidou-se, o invasor tem acesso livre ao sistema do computador (KANDAN; KATHRINE e MELVIN, 2019).

Com relação à 2ª questão de pesquisa: "Quais são as práticas de segurança da informação mais adotadas nas organizações com relação em home office?"

A Tabela 9, mostra as 9 práticas a serem adotadas para a segurança da informação em ambiente home office que foram citados 3 ou mais vezes, das 9 publicações selecionadas. Boas práticas em segurança da informação é adotar comportamentos com que tenha objetivo de manter a confidencialidade, integridade e a disponibilidade dos dados, permitindo com que não venha ter prejuízos futuros tanto pessoais quanto para as organizações públicas e privadas (RODRIGUES JR., 2021).

Tabela 9 - Práticas a serem adotadas para segurança da informação

ID	Práticas a Serem Adotadas para a Segurança da Informação	Artigos	%
[PS1]	Treinamento com os funcionários no home office	[A01], [A04], [A05], [A08], [A09]	56%
[PS2]	Uso da VPN	[A05], [A06], [A07], [A08], [A09]	56%
[PS3]	Programa *Antimalware*	[A04], [A05], [A08]	33%
[PS4]	Evitar acesso a links não confiáveis	[A03], [A04], [A06]	33%
[PS5]	Uso seguro das senhas	[A05], [A06], [A08]	33%
[PS6]	Adoção de políticas de segurança organizacional	[A05], [A06], [A08]	33%
[PS7]	Medidas de autenticação	[A05], [A06], [A08]	33%
[PS8]	Medida de proteção no ambiente	[A05], [A06], [A08]	33%
[PS9]	Ferramenta de monitoramento de *Logging*	[A01], [A04], [A05]	33%

Fonte: O Autor (2022).

A prática a ser adotadas para a segurança da informação “treinamento com os funcionários no home office” ([PS1]), foi citado em 5 (56%) das publicações selecionadas. A organização que adota o modelo de home office deve preparar seus funcionários para esse novo meio, deve informar seus funcionários a importância da segurança dos dados da empresa diante da tecnologia da informação, considerando que a informação é um bem inestimável e caso informações sigilosas caiam em mãos de terceiros, pode ser muito prejudicial.

No ambiente home office os funcionários estão mais expostos a ataques, em vista disso, a organização tem o dever de criar campanhas de educação e boas maneiras para a manipulação de dados corporativos, já que o treinamento permite uma proteção mais eficaz dos dados (KHANDO *et al*., 2021).

A prática a ser adotada para a segurança da informação “utilização de VPN” (Virtual Private Network) ([PS2]), foi citada em 5 (56%) das publicações selecionadas. Considerada uma das medidas fundamentais para as operações de qualquer organização em ambiente virtual, a rede privada impacta e influencia questões relacionadas à segurança e disponibilidade segura das informações (RODRIGUES JR., 2021).

As VPNs são usadas principalmente para informações privadas e confidenciais. Ele cria um túnel criptografado. A VPN cria um canal seguro que deixa as informações online oculta de qualquer um que tenha acesso a rede mais não tenha a chave de criptografia, o que torna um processo mais dificultoso para os atacantes maliciosos (KANDAN, KATHRINE e MELVIN, 2019).

A prática a ser adotada para a segurança da informação “Programas *antimalware*” ([PS3]), foi citado em 3 (33%) das publicações selecionadas. O uso de software antivírus é essencial para computadores pessoais e de trabalho, este permite identificar algumas ameaças que podem comprometer os dados que contêm na máquina (RODRIGUES JR., 2021).

Evite o uso de *pendrives* e discos rígidos externos como forma de proteger o ambiente de trabalho, pois eles podem se tornar um meio de infecção e devem ser evitados. Mesmo que a rede seja segura, é muito difícil se proteger de malware que tem acesso direto ao computador da vítima pela porta USB. Um software antivírus com monitoramento ativo pode ajudar a bloquear possíveis ameaças (RODRIGUES JR., 2021; ALVES, 2020).

A prática a ser adotada para a segurança da informação “medidas de autenticação” ([PS7]), foi citado em 3 (33%) das publicações. Medidas de autenticação devem ser adotadas para evitar acesso não autorizado mesmo que o invasor tenha uma senha verdadeira.

Práticas fortes de autenticação devem se concentrar na usabilidade, pois a adoção de novas tecnologias e métodos será aprimorada se forem convenientes e fáceis de usar. Independentemente de os funcionários estarem ou não trabalhando em casa, eles precisam de uma maneira fácil e segura de criar, armazenar e gerenciar senhas, e chaves de segurança de hardware integradas a gerenciadores de senhas de nível empresarial podem ajudar a fazer isso acontecer (SARGINSON, 2020).

A autenticação de dois fatores pode não ser infalível, mas na ausência de autenticadores mais fortes, é uma abordagem de prática recomendada que pode criar uma boa barreira contra invasores indesejados (RODRIGUES JR., 2021).

A prática a ser adotada para a segurança da informação "adoção de política de segurança organizacional" ([PS6]), foi citada em 3 (33%) das publicações**.** As organizações precisam identificar os erros que impactam o home office e informar seus funcionários, assim como auxiliar no compartilhamento de informações para evitar que esses erros ocorram (AMPOMAH *et al.,* 2013).

Os riscos que influenciam no home office devem ser identificados pela organização. Isso permitirá desenvolver políticas para controlar os riscos baseado nas diferentes estratégias de segurança. Elas precisam ser criadas de uma maneira que incentive a conformidade e, em seguida, essas políticas precisam ser comunicadas aos trabalhadores remotos. Após a implementação das políticas, a eficácia precisa ser medida (AMPOMAH *et al.,* 2013).

A prática a ser adotada para a segurança da informação "evitar acesso a links não confiáveis" ([PS4]), foi citada em 3 (33%) das publicações selecionadas. Muitos criminosos utilizam sites para infectar o navegador ou até mesmo o computador das vítimas, o método mais comum é enviar *URLs* disfarçados de links seguros e autênticos.

Os invasores normalmente enviam links por meio de e-mail, SMS, redes sociais para suas potenciais vítimas e como medida de segurança as organizações devem oferecer recursos para seus funcionários como, por exemplo, adotar um dispositivo exclusivo para o trabalho com restrições para ter o máximo de segurança sobre seus dados importantes, conscientizar seus funcionários sobre links de fontes duvidosas, criar uma assinatura segura para enviar informações aos seus funcionários e evitar acesso a links do domínio HTTP (KANDAN; KATHRINE e MELVIN, 2019; LALLIE *et al.*, 2021).

A prática a ser adotada para a segurança da informação "uso seguro das senhas" ([PS5]), foi citada em 3 (33%) das publicações selecionadas. Deve ser adotados senhas fortes com números, letras maiúsculas e minúsculas, conter caracteres especiais para dificultar que

programas quebrem a senha de acesso. Também é importante ressaltar que a senha não deve ser compartilhada com colegas de trabalho e não deve deixar a senha escrita em algum lugar acessível a todos.

Uma política de senha corporativa aborda as regras que todos os usuários devem seguir para garantir que os padrões mínimos de segurança sejam seguidos ao acessar sistemas e dispositivos corporativos. Os funcionários devem ser conscientizados sobre a não utilização da mesma senha em todas as contas e a troca periódica das senhas (LALLIE *et al.*, 2021).

A prática adotada para a segurança da informação “medida de proteção no ambiente” ([PS8]), foi citada em 3 (33%) das publicações selecionadas. Nessa prática de segurança a organização deve fornecer suporte e recurso para os funcionários e estes devem seguir as normas estabelecidas pela organização assim como ter cuidados extras como, por exemplo, evitar presenças de outras pessoas no ambiente de trabalho remoto.

Sempre que possível, as organizações precisam fornecer computadores e softwares compatíveis com as atividades que cada funcionário precisa exercer, pois concede tranquilidade saber que um trabalho importante é feito em um computador dedicado a ele e não compartilhado com outras pessoas. Caso não seja possível fornecer computadores, então deve realocar as licenças que a organização já possui para os funcionários usarem em seus computadores (SARGINSON, 2020).

4. PERCEPÇÃO DOS PROFISSIONAIS AO HOME OFFICE

Neste capítulo são descritos os estudos realizados e os resultados obtidos com a pesquisa de opinião com profissionais que atuaram no home office a respeito da segurança da informação.

4.1 Planejamento da Pesquisa de Opinião

Este trabalho apresentou como segundo objetivo, realizar uma pesquisa de opinião com os profissionais que atuaram no home office a respeito da segurança da informação. Com o objetivo de validar as práticas a serem adotadas na segurança da informação no home office. Dessa forma, foi aplicado um questionário com vários profissionais que tenham tido a experiência de trabalhar em ambiente doméstico. Abaixo, estão relatados o planejamento e os resultados encontrados com esta pesquisa. O planejamento da pesquisa foi organizado através de três aspectos descritos na Tabela 10: Objetivos, Participantes e Instrumentação.

Tabela 10 - Planejamento da pesquisa de opinião

Objetivo: Analisar através da percepção dos profissionais que atuaram no home office a respeito da segurança da informação. Como referência as ameaças/vulnerabilidades e práticas adotadas no mapeamento sistemático.
Participantes: Os participantes selecionados para este estudo são profissionais que atuam em organizações que tenham adotado o trabalho em home office e que tiveram disponibilidade para participar da pesquisa. Alguns e-mails foram coletados por funcionários da empresa e outros obtidos por meio de outros participantes.
Instrumentação: Como instrumentação do estudo um questionário foi desenvolvido no idioma português e criado pelo Formulário Google, foi elaborado com objetivo de responder as três etapas: I. **Caracterização da Pesquisa**: Os participantes que aceitaram foram questionados sobre seus dados pessoais (idade, empresa, formação, área de atuação, tempo de trabalho). II. **Seleção das Práticas Adotadas na Segurança da Informação**: Os participantes responderam se eles tinham atuado no ambiente home office e depois deviam informar três características que julgavam ser importante para manter a segurança da informação no home office das 8 práticas identificadas no mapeamento. III. **Identificação do Nível de Relevância de acordo com as Práticas de Segurança da Informação**: Os participantes responderam 13 questões, para cada questão o participante indicou o nível de relevância que variava de 1 a 5 (5 tem o maior grau de relevância). Conforme a sua experiência no trabalho de home office, as 13 questões foram aplicadas com base no mapeamento sistemático de acordo com melhores práticas a serem adotadas em ambiente home office.

Fonte: O Autor (2022).

Primeiramente foi enviado um e-mail para os participantes explicando o objetivo da pesquisa e esclarecendo que a participação era voluntária conforme a Tabela 11. Neste e-mail tinha o link de acesso ao questionário, porém, antes do seu preenchimento era necessário aceitar um Termo de Consentimento Livre e Esclarecido, como mostra a Tabela 12. O

questionário está disponível no Apêndice B, e ele ficou ativo no período de 21/03/2022 a 25/03/2022.

Tabela 11 - Texto explicativo

Prezado(a) Senhor(a), Meu nome é Bruno Rodrigues, sou aluno do curso de Engenharia de Software da Universidade Federal do Amazonas - UFAM. Estou realizando uma pesquisa como resultado do meu Trabalho de Conclusão de Curso, sob a orientação da Prof. Christophe Saint-Christie de Lima Xavier. O objetivo da pesquisa é verificar e analisar a percepção dos profissionais que atuaram no home office com relação a segurança da informação. Sua participação na pesquisa consistirá em responder as questões de um questionário disponível no link: https://forms.gle/41M5SBuEgrVxJzC36. O tempo para responder as questões é em torno de 5 minutos e o questionário ficará aberto até o dia 25/04/2022 Esta pesquisa está inserida em um estudo estritamente acadêmico, em nível de graduação, sem fins comerciais. A sua participação é voluntária e você poderá desistir a qualquer momento. Serão omitidas todas as informações que permitam identificá-lo(a). Os pesquisadores responsáveis pelo estudo poderão fornecer qualquer esclarecimento, assim como tirar dúvidas, bastando entrar em contato pelos seguintes e-mails: Bruno Rodrigues: brunoramosro@gmail.com - ICET/UFAM (Discente) Christophe Xavier: christophe@ufam.edu.br - ICET/UFAM (Orientador)

Fonte: O Autor (2022).

Tabela 12 - Termo de compromisso livre esclarecido

Antes de começarmos é necessário você aceitar o Termo de Compromisso Livre e Esclarecido (TCLE). Eu declaro que li as informações contidas no e-mail. Compreendo que minha participação nesta pesquisa é inteiramente voluntária e que tenho total liberdade para recusar ou retirar meu consentimento, sem sofrer nenhuma penalidade. Os dados obtidos através da minha participação nesta pesquisa serão analisados, sendo do meu consentimento que haverá divulgação de seus resultados apenas em contexto acadêmico e publicações científicas, sem citar o meu nome.

Fonte: O Autor (2022)

4.2 Resultado e Análise da Pesquisa de Opinião

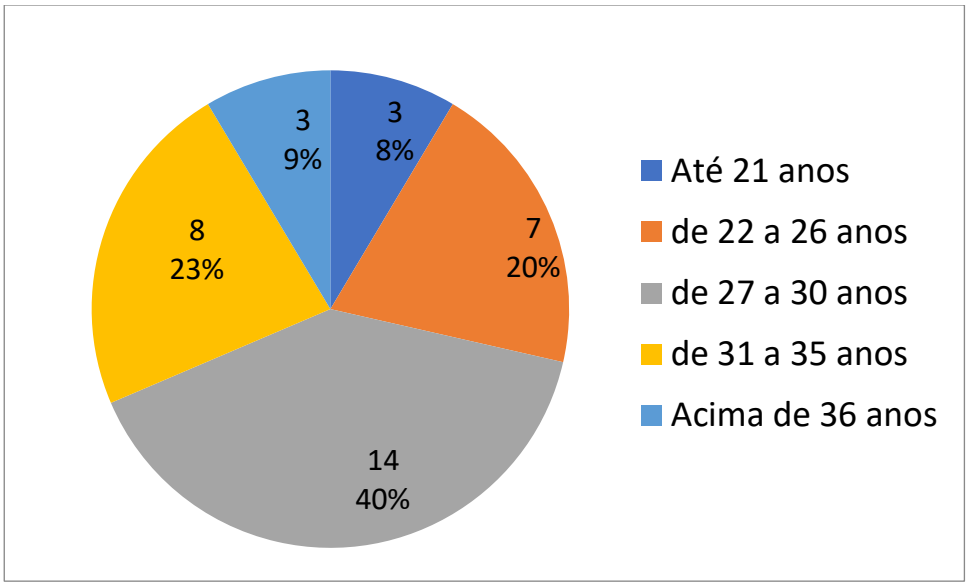
4.2.1 Caracterização dos Participantes

Os participantes da pesquisa de opinião sobre práticas adotadas da segurança da informação, foram profissionais que atuam no mercado de trabalho em empresas públicas ou privadas e que tenham exercido sua profissão em ambiente home office.

A coleta de dados resultou no total de 35 respondentes, com relação às perguntas que tinham o objetivo de conhecer características dos participantes, primeiramente em relação à faixa etária de idade, a maior participação foi de profissionais de 27 a 30 anos o que representa 40% (14) respondentes, seguido pela faixa de 31 a 35 anos com 23% (8)

respondentes. Conforme a Figura 6, nota-se que 71% dos participantes têm mais de 27 anos de idade.

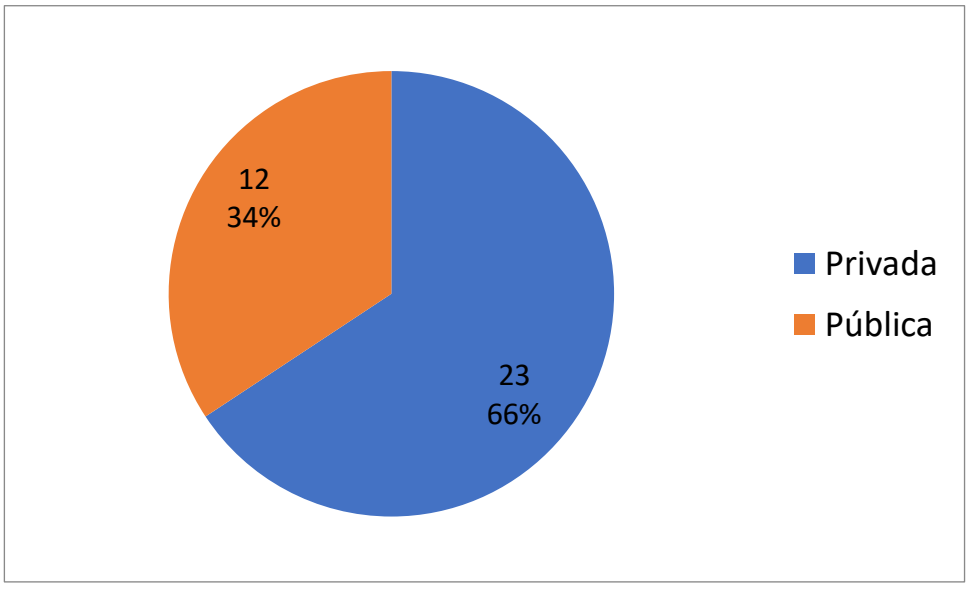
Figura 6 - Faixa etária de idade



Fonte: O Autor (2022)

Com relação ao tipo de organização que atua, conforme apresentado na Figura 7, a maioria dos profissionais que responderam esta pesquisa, são de organização pública, com 66% (23) respondentes e 34% (12) são de organizações privadas. Nota-se que tanto organizações públicas e privadas adotaram o modelo home office, sendo essencial este estudo da segurança da informação organizacional.

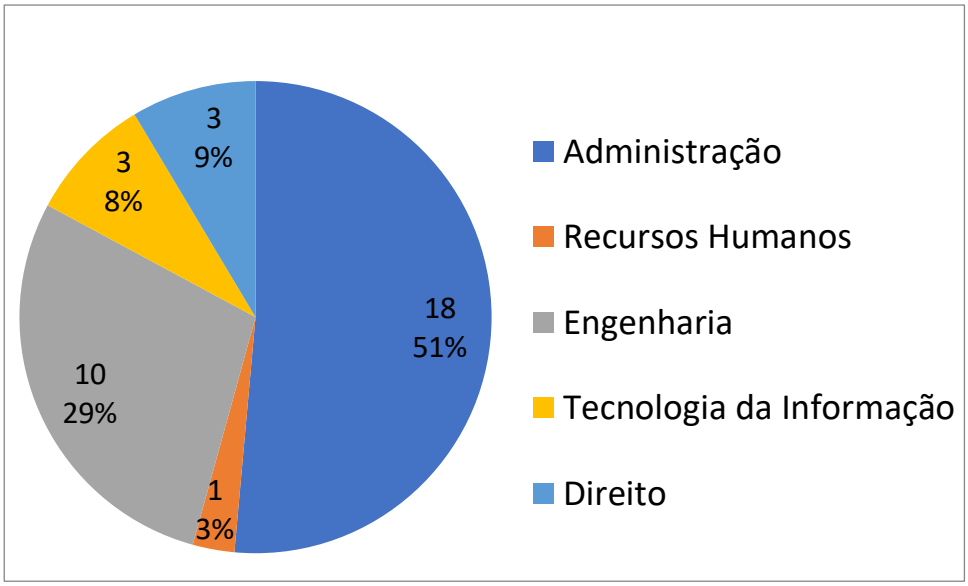
Figura 7 - Tipo de organização que atua



Fonte: O Autor (2022).

Na pesquisa de opinião, foi perguntado aos participantes qual era sua formação acadêmica e 51% (18) dos respondentes são formados em administração, em segundo lugar com 29% (10) dos respondentes são de engenharia e somente com 3% (1) tem formação em recursos humanos. Conforme a Figura 8, é possível identificar que os participantes têm formação em umas das seguintes áreas (Administração, Recursos Humanos, Engenharia, Tecnologia da Informação e Direito).

Figura 8 - Formação acadêmica

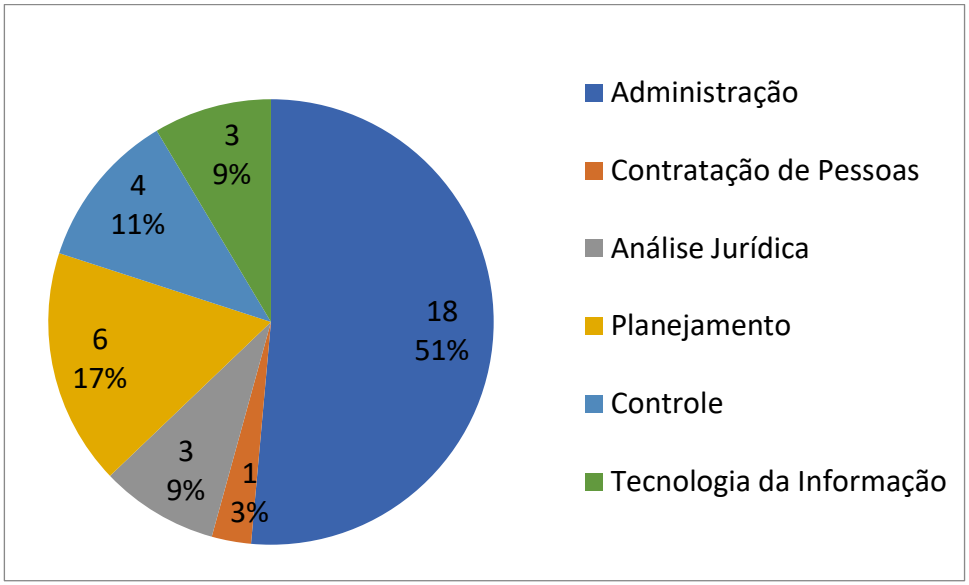


Fonte: O Autor (2022).

A Figura 9, apresenta a área de atuação que o profissional exerce na organização.

Vale destacar que a maioria dos participantes atuava na área administrativa, com 51% (18) dos respondentes, esse resultado está relacionado positivamente com a questão anterior, formação acadêmica, que 51% dos respondentes tinham experiência na área administrativa. formação acadêmica de campo e esses profissionais atuais na área de gestão organizacional. Em segundo lugar tem-se a área de planejamento com 17% (6) e em seguida com 11% (4) tem-se controle, ou seja, os 10 participantes que são de engenharia eles atuam na organização como planejamento ou na área de controle e com menor porcentagem é contratação de pessoas com apenas 3% (1) dos respondentes.

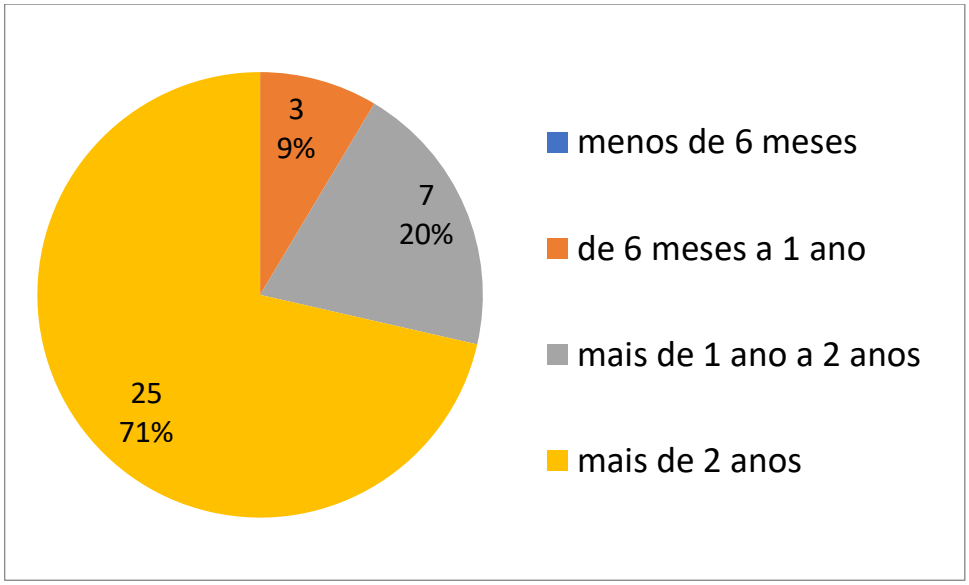
Figura 9 - Área de atuação na organização



Fonte: O Autor (2022).

A última pergunta feita com base na caracterização do participante foi sobre o tempo de experiência que ele possui na organização. O resultado é apresentado na Figura 10, onde 71% (25) dos respondentes, ou seja, mais da metade, possui experiência de mais de 2 anos na organização. Observa-se que na pesquisa nenhum dos participantes possui menos de 6 meses, e somente 9% (3) possui tempo de experiência de 6 meses a 1 ano.

Figura 10 - Tempo de trabalho que possui na organização

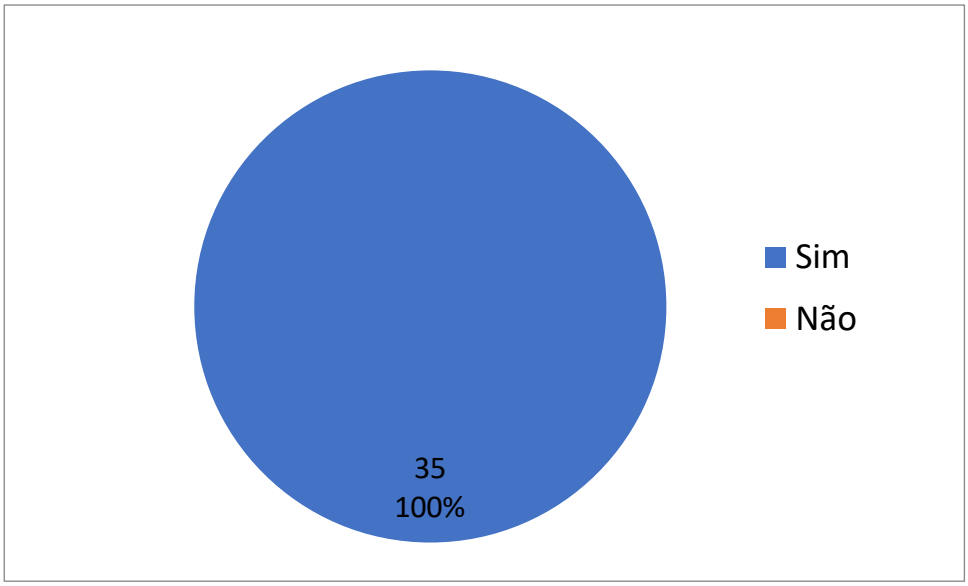


Fonte: O Autor (2022).

4.2.2 Seleção das Práticas a Serem Adotadas na Segurança da Informação

As próximas perguntas feitas aos participantes foram direcionadas sobre segurança da informação. A primeira pergunta foi “exerceu o seu trabalho em ambiente home office?”, como apresentado na Figura 11, onde 100% (35) dos respondentes exerceu seu trabalho em ambiente doméstico, o que era necessário para participar da análise desta pesquisa, pois este trabalho é voltado para segurança da informação em ambiente home office, logo os participantes deveriam ter vivenciado esse ambiente para poder responder às demais questões.

Figura 11 - Exerceu trabalho em home office



Fonte: O Autor (2022).

A segunda pergunta foi sobre as práticas de segurança da informação identificadas no mapeamento sistemático. No total foram 9 práticas identificadas e foram apresentadas para os respondentes de forma aleatória. Cada participante teve que selecionar exatamente três práticas as quais julgaram sendo as mais importantes.

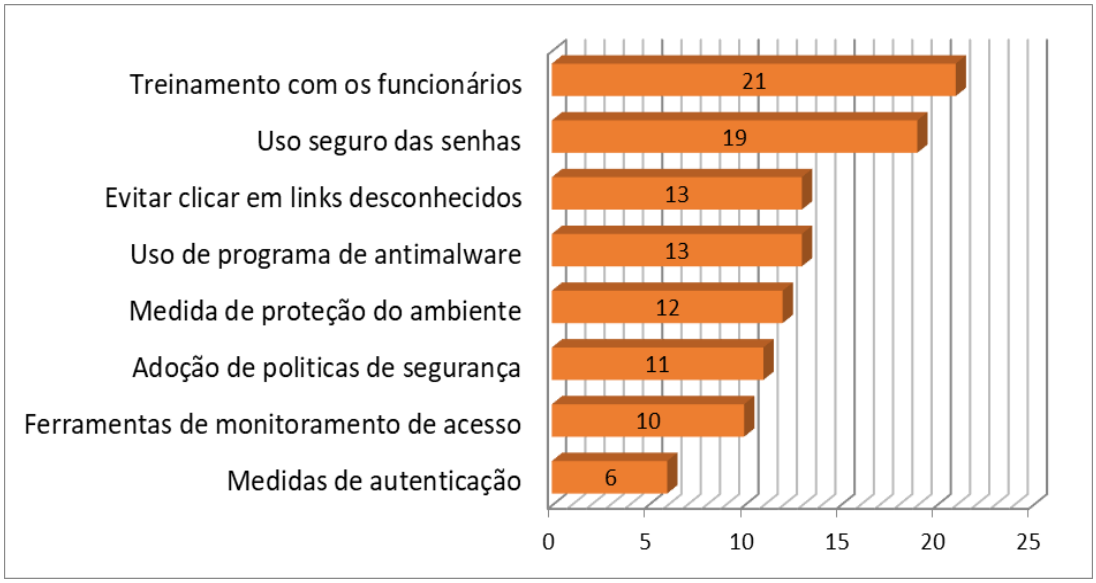
Com mostra a Figura 12, em primeiro lugar tem-se “Treinamento com os funcionários” com 60% (21) dos respondentes, ou seja, das práticas identificadas no mapeamento sistemática, esta prática está entre as três que os participantes julgam ser importante. Fazendo uma comparação com o mapeamento sistemático, está prática também ficou em primeiro lugar no mapeamento, ou seja, tanto na literatura como na pesquisa de opinião, é essencial que a organização treine seus funcionários da melhor forma para com que eles trabalhem em home office de forma segura.

Os top 3 das práticas foram em 1º lugar “Treinamento com os funcionários”, em 2º lugar “Uso seguro das senhas”, e em 3º lugar, juntos foram “Evitar clicar em links

desconhecidos” e “Uso de programa *antimalware*”. Com relação ao uso seguro de senha, é necessário evitar reutilizar senhas. Caso faça isso, e a senha seja descoberta, todas as outras contas estarão expostas.

Com relação a evitar clicar em links desconhecidos e uso de programa *antimalware*, o *hacker* precisa que você clique no link para cair no golpe. Então, é necessário evitar clicar em link que pareça urgente e difícil de ignorar, este tem maior probabilidade de ser perigoso e falso. Ou mesmo, quando baixar algo da internet ele pode vir com algum malware, por isso é necessário ter na máquina programas *antimalware* (ROHR, 2021).

Figura 12 - Práticas de segurança da informação



Fonte: O Autor (2022).

4.2.3 Identificação e Análise do Nível de Relevância das Práticas

Nesta etapa, os participantes tiveram 13 questões referentes as práticas para a segurança da informação em ambiente home office, responderem a seguinte pergunta “Marque o quão relevante você considera as práticas a seguir para a segurança da informação em ambiente home office”, com opções de uma escala que variava de 1 a 5 (Sem Relevância, Baixa Relevância, Média Relevância, Alta Relevância e Altíssima Relevância). Abaixo está descrito cada nível de relevância:

- **Sem Relevância:** É o nível de relevância mais baixo. Ele significa que essa prática não teria qualquer influência para a segurança da informação
- **Baixa Relevância:** Indica que a prática não afetaria significativamente a segurança da informação.

- **Média Relevância:** Indica que a prática possui efeito considerável para a segurança da informação. Em certos ambientes, seria afetada com a ausência dessa prática.
- **Alta Relevância:** Indica que essa prática deve ser considerada que traz consigo grande relevância e a falta dela pode prejudicar a segurança da informação.
- **Altíssima Relevância:** indica que a prática é absolutamente necessária para ser considerada para segurança da informação. A ausência dessa prática acarreta fracasso.

A Tabela 13 apresenta o resultado geral da pesquisa de opinião. Com ID (Identificação), Questão (Pergunta que foi feita), Sem R. (Sem Relevância), Baixa R. (Baixa Relevância), Média R. (Média Relevância), Alta R. (Alta Relevância) e altíssima R. (Altíssima Relevância), % (Porcentagem com relação às 35 respostas). Nesse resultado é possível perceber que uma das práticas com mais "Altíssima Relevância" que os participantes responderam foi "Treinamento para o trabalho home office", "Usar antivírus" e "Uso seguro de senhas".

Das 13 práticas nenhuma foi classificada como "Sem Relevância" pelos participantes, e somente 1 prática foi classificada como "Baixa Relevância", sendo "Treinamento para o trabalho em home office", essa prática dos 35 participantes, somente 1 considerou com baixa relevância. Com "Média Relevância" 5 práticas foram selecionadas, a com maior frequência foi a [Q7] "Usar rede privada virtual (VPN)", e realizando uma soma de "Alta Relevância" com "Altíssima Relevância", é possível perceber que a VPN, de todas as práticas é a menos considerada relevante.

Tabela 13 - Nível de relevância geral dos fatores

ID	Questão	Sem R.	%	Baixa R.	%	Média R.	%	Alta R.	%	Altíssima R.	%
Q1	Evitar usar dispositivo pessoal para o trabalho	0	0%	0	0%	1	3%	2	6%	32	91%
Q2	Não acessar sites inseguros	0	0%	0	0%	0	0%	3	9%	32	91%
Q3	Comunicação com a empresa	0	0%	0	0%	0	0%	7	20%	28	80%
Q4	Treinamento para o trabalho em home office	0	0%	1	3%	0	0%	0	0%	34	97%
Q5	Comprometimento organizacional	0	0%	0	0%	1	3%	6	17%	28	80%
Q6	Descarte seguro de dados confidenciais empresarial	0	0%	0	0%	2	6%	1	3%	32	91%
Q7	Usar rede privada virtual (VPN)	0	0%	0	0%	3	9%	8	23%	24	69%
Q8	Usar antivírus	0	0%	0	0%	0	0%	1	3%	34	97%
Q9	Uso seguro de senhas	0	0%	0	0%	0	0%	1	3%	34	97%

Q10	Política de segurança organizacional	0	0%	1	3%	0	0%	1	3%	33	94%
Q11	Medidas de autenticação	0	0%	0	0%	0	0%	3	9%	32	91%
Q12	Proteção do ambiente de trabalho em casa	0	0%	0	0%	0	0%	4	11%	31	89%
Q13	Ferramenta de monitoramento de logging	0	0%	0	0%	2	6%	4	11%	29	83%

Fonte: O Autor (2022). Legenda: R.: Relevância.

A **Tabela 14**, apresenta uma comparação do resultado da pesquisa de opinião com o mapeamento sistemático. Das 9 práticas identificadas no MS, foram acrescentadas mais 04 práticas, conforme analisadas do resultado da vulnerabilidade/ameaças, para enfim compor 13 práticas de segurança da informação em ambiente home office. Com as 13 práticas, foi realizada uma nova ordenação, de acordo com a quantidade de artigos que citou tal prática de segurança.

Conforme o resultado da PO, o fator mais relevante classificado pelos participantes foi "Treinamento para o trabalho em home office", enquanto no MS este ocupou a 2ª posição. Tal prática é considerada essencial para a segurança da informação organizacional. Pois o ambiente doméstico, não é um ambiente que está sendo controlado pela organização considerando que cada funcionário esteja em sua residência, esse risco só aumenta, pois o funcionário pode cometer vários erros como usar dispositivo pessoal, acessar dados importantes da organização sem o devido cuidado, ou mesmo, permitir com que qualquer pessoa tenha acesso a esse ambiente.

O conhecimento de segurança da informação por parte do funcionário é um dos principais determinantes para manter os dados importantes seguros, sendo necessário aumentar o conhecimento de aplicações básicas de segurança. É imprescindível que as organizações do setor público e privado incluam programas de educação em segurança da informação e conscientização, para que os funcionários desenvolvam suas competências e habilidades necessárias para estar ciente dos potenciais riscos e ameaças à segurança (KHANDO *et al*, 2021).

A prática "Usar antivírus" e "Uso seguro de senhas" também ficou em 1º lugar na PO, com 97%, e no MS ficou em 3º lugar, mostrando que principalmente por estar trabalhando em ambiente home office é sempre indispensável a utilização de programa *antimalware*, pois ao acessar a internet, usar dispositivo removível e entre outros, corre o risco de o computador ser infectado, e podendo ser coletado dados importantes, que podem prejudicar a organização. A utilização de um antivírus, é extremamente fundamental, principalmente em computadores de uso pessoal, que estes são usados para várias atividades, tanto pessoais como para o trabalho.

Também é indispensável manter seguro o uso de senhas, evitar usar a mesma senha para vários acessos, e diferenciar senhas pessoais das senhas utilizadas para o trabalho da organização (RODRIGUES JR., 2021; YUBICO, 2020).

A "Política de segurança organizacional" obteve o 2º lugar na PO com 94%, enquanto no MS essa prática alcançou a 3ª posição. A política de segurança da informação é um fator crucial quando se trata de práticas de gerenciamento de segurança, é necessário identificar e comunicar os tópicos de maior valor para a organização. A política tem como objetivo estabelecer as orientações, normas, ações e responsabilidades relativas à proteção da informação, como exemplo os três pilares da segurança que devem ser respeitados, como a confidencialidade, integridade e disponibilidade dos dados (KHANDO *et al*., 2021).

A terceira colocação "Evitar usar dispositivo pessoal para o trabalho", "Não acessar sites inseguros", "Medidas de autenticação" e "Descarte seguro de dados confidenciais empresarial" com 91% na PO, nota-se que no MS, "Evitar usar dispositivo pessoal para o trabalho" ficou em 1º lugar na literatura. A frequência é alta em usar computador pessoal para o trabalho home office, tem como motivação a falta de conscientização por parte dos funcionários, ou mesmo, pelo acontecimento de a organização não disponibilizar o computador para exercer o trabalho. É vital que seja realizado o descarte seguro de dados confidenciais da organização, tanto físico quanto digital, algumas recomendações são, picotar os papéis impressos, e excluir permanentemente dados que não devem ser acessados do computador.

Na quarta colocação "Proteção do ambiente de trabalho em casa" com 89% na PO, e 33% no MS, Segundo Ampomah (2013) a segurança do ambiente é uma questão que está obrigada a ser abordada pelas organizações, pois os profissionais estão vulneráveis a danos pessoais ou mesmo um ataque com risco de vida devido à falta de proteção no ambiente de trabalho em casa. Os trabalhadores podem ser atacados fisicamente com o objetivo de fornecer informações confidenciais a terceiros. Dessa forma, uma solução para evitar que o problema ocorra é aplicar uma estratégia de vigilância que visa criar consciência situacional da evolução das ameaças.

Na quinta colocação "Ferramenta de monitoramento de *logging*" com 83% na PO, e no MS ficou em 3º lugar com 33%, as ferramentas de monitoramento e registro são tipos de software que supervisionam a atividade e geram arquivos de registros. Os logs de monitoramento facilitam a identificação de eventos de segurança que ocorrem ou podem ocorrer. Este tipo de software deve ser usado pelas organizações pois reúne dados de log para

fornecer insights sobre a integridade e o desempenho dos ambientes de tecnologia da informação (LAKIVAKIS *et al.*, 2021).

Na sexta colocação "Comunicação com a empresa" e "Comprometimento organizacional" ficou com 80% na PO, e no MS ficou 3º lugar com 33%, a falta de comprometimento organizacional em relação ao trabalho home office resulta em muitas violações de segurança da informação. A falta de comunicação por parte da organização contribui imensamente para a intercepção de dados válidos e perda crítica de informação, o que pode trazer grandes prejuízos financeiros. A organização deve manter o comprometimento e comunicação direta com os funcionários, pois no caso de o profissional obter assistência de outro lugar que não seja da organização, este podem ser vítimas de engenharia social, e passar as credenciais de acesso importantes, comprometendo assim dados importantes (AMPOMAH, 2013).

Em última colocação ficou "Usar rede privada virtual (VPN)" com 69%, destaca a importância de ter uma proteção extra, uma VPN permite com que os funcionários autorizados acessem dados da organização, tudo isso por meio de um sistema que usa criptografia para garantir a segurança. Como os dados da organização estão sendo manipulados por funcionários que trabalham de casa, é necessário ter uma segurança para garantir a confidencialidade aos dados, isso permite incluir criptografia de ponta a ponta e uso de VPNs, uma VPN protegerá os dados do dispositivo ao servidor (YUBICO, 2020).

Tabela 14 - Práticas comparação PO x MS

Prática de Segurança da Informação em Home Office	**Pesquisa de Opinião**		**Mapeamento Sistemático**	
Treinamento para o trabalho em home office	1º	97%	2º	56%
Usar antivírus	1º	97%	3º	33%
Uso seguro de senhas	1º	97%	3º	33%
Política de segurança organizacional	2º	94%	3º	33%
Não acessar sites inseguros	3º	91%	2º	56%
Medidas de autenticação	3º	91%	3º	33%
Evitar usar dispositivo pessoal para o trabalho	3º	91%	1º	67%
Descarte seguro de dados confidenciais empresarial	3º	91%	3º	33º
Proteção do ambiente de trabalho em casa	4º	89%	3º	33%
Ferramenta de monitoramento de *logging*	5º	83%	3º	33%
Comunicação com a empresa	6º	80%	3º	33%
Comprometimento organizacional	6º	80%	3º	33%
Usar rede privada virtual (VPN)	7º	69%	2º	56%

Fonte: O Autor (2022).

5. CONSIDERAÇÕES FINAIS E PERSPECTIVAS FUTURAS

Neste capítulo são apresentadas as considerações finais sobre o trabalho realizado, as contribuições e limitações da pesquisa e as futuras linhas de pesquisa a serem realizadas.

5.1 Considerações Finais

No mundo digital, proteger os ativos de ataques maliciosos tornou-se uma das principais prioridades das organizações e existe uma correlação direta entre pessoas e segurança, as pessoas atuam como operadores ao lidar com dados e sistemas de informação. A maioria das violações de segurança é causada pela falta de reconhecimento das fraquezas de segurança dos dados.

As organizações adotaram um novo método de trabalho, o home office, devido a infecção viral do COVID-19, em suma o home office, trata-se de uma estação de trabalho, na qual os indivíduos mantêm o vínculo empregatício formal com a organização.

Dessa forma, esta pesquisa descreve os resultados de um mapeamento sistemático que teve como objetivo analisar os problemas enfrentados pelas organizações em relação à segurança da informação no modo home office e uma pesquisa de opinião para validar as práticas identificadas no mapeamento sistemático.

Como resultado do MS foi possível identificar 8 vulnerabilidades, 8 ameaças e 9 práticas. Destacando: “Dispositivo pessoal para trabalho” (Vulnerabilidade), “Interceptação de dados por meio da engenharia social” (Ameaça) e “Treinamento com os funcionários no home office” (Práticas adotadas para segurança da informação).

Como resultado da pesquisa de opinião foi possível classificar (com relação aos níveis de relevância) as práticas adotadas para segurança da informação através de um formulário com 13 questões, onde foi destacado “Treinamento para o trabalho em home office”, “Usar antivírus” e “Uso seguro de senhas”; essas práticas foram a qual tiveram maior porcentagem onde ambos têm 97% de altíssima relevância considerando as práticas essenciais para a segurança da informação, por 35 respondentes.

5.2 Contribuição da Pesquisa

Esta pesquisa tem como contribuição a identificação de vulnerabilidades, ameaças e práticas de segurança da informação em ambiente home office. Durante a pesquisa foram identificadas 8 vulnerabilidades, 8 ameaças e 9 práticas que devem ser adotadas para manter a segurança da informação em ambiente home office. Além disso, foi realizada uma pesquisa de opinião para validar as práticas de segurança da informação de acordo com o nível de relevância, junto com profissionais que tenham atuado em seu trabalho em ambiente home office.

Este trabalho pode ajudar organizações e profissionais a identificar quais são as vulnerabilidades e ameaças decorrentes do trabalho em ambiente home office e conhecer as práticas que devem ser adotadas diante desse cenário.

5.3 Limitações

A limitação deste trabalho está relacionada ao MS devido ser um tema atual, que aborda a segurança da informação em ambiente home office ao fato de existirem poucas publicações com esse tema. Além do tema pesquisado ser realizado em apenas algumas fontes de buscas.

Outra limitação é devido ao quantitativo de respondentes da pesquisa de opinião que somente 35 profissionais responderam. E o perfil de formação dos participantes eram todos com graduação, não tendo nenhum com grau de ensino médio.

5.4 Trabalhos Futuros

Com intenção de expandir e aprimorar os resultados obtidos, as perspectivas para trabalhos futuros são:

- Ampliar o mapeamento sistemático para outras fontes, como outras bibliotecas digitais e outras fontes manuais.
- Realizar um estudo de caso em alguma organização de médio ou grande porte que tenha adotado o trabalho em ambiente home office para identificar quais dificuldades essa determinada empresa sofreu com a implementação desse modelo com relação à segurança da informação.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ISO/IEC 27002: Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação**. p. 01- 99, 2013.

ABNT – Associação Brasileira de Normas Técnicas. **NBR 16167: Segurança da Informação - Diretrizes para Classificação, Rotulação, Tratamento e Gestão da Informação**. p. 01- 10, 2020.

ALBUQUERQUE JR., A. e SANTOS, E. **Adoption of Information Security Measures in Public Research Institutes**. JISTEM - Journal of Information Systems and Technology Management. v. 12, n. 02, p. 289-316, Mai./Ago., 2015.

ALMUBAYEDH, D.; KHALIS, M. A.; ALAZMAN, G.; ALABDALI, M.; AL-REFAI, R. e NAGY, N. **Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study.** *21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, Saudi Arabia, p. 01-06, 2018.

ALVES, P. **Dicas para Trabalhar em Home Office: Saiba Proteger Informações Importantes**. techtudo, 2020. Disponível em:< https://www.techtudo.com.br/listas/2020/03/dicas-para-home-office-saiba-proteger-informacoes-importantes-do-trabalho.ghtml>. Acesso em: 03 de julho de 2021.

AMPOMAH, M.; SILVA, Y.D.; LI, H.; PAHLISA, P.; YANG, Q. e ZHANG, Q. **Information Security Strategy and Teleworking (In)Security.** Melbourne, The University of Melbourne, 2013.

ATTATSITSEY M. e OSEI-BONSU N. **Assessing the Impact of Information Technology On Human Resource Practices: Evidence from Organisations in Ghana**. International Journal of Information Technology and Management, v. 20, Issue 1-2, p. 5 – 20, 2021.

BANDEIRA, J. **Avaliação da Aplicação da Norma NBR ISO/IEC 27002:2013 e a Conformidade com ITIL no Processo de Gestão de Segurança da Informação**. 2017. 60 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Universidade Federal Fluminense, 2017.

BARBOSA, G. e SILVA, M. **Segurança da Informação: A Proteção Contra o Vazamento de Dados e sua Importância para as Empresas Privadas**. e-F@tec, v. 6, n. 1, p. 1-10, 2016.

BARROS, A. M.; SILVA, J. R. G. D. **Percepções dos Indivíduos Sobre as Consequências do Teletrabalho na Configuração Home-Office: Estudo De Caso Na Shell Brasil**. Scielo, 2010. Disponível em:. Acesso em: 03 de julho de 2021.

BELMIRO, J. **Tecnologia da Informação Gerencial**. 1. Ed São Paulo: Pearson Education do Brasil, 2018.

BUOGO, M.; FACHINELLI, A. E GIACOMELLO C. **Gestão do Conhecimento e Segurança da Informação.** Atoz: Novas Práticas em Informação e Conhecimento, v. 8, n. 2, p. 49-59, 2019.

CASTRO, B.; BERNARTT, M. e GODOY, C. **A Tecnologia de Informação e Comunicação como Mecanismo para a Migração: Um Estudo Sobre os Haitianos no Brasil**. DRd – Desenvolvimento Regional em debate, v. 7, n. 2, p. 158-172, Jul./Dez., 2017.

FAVERO, A. e FAVERO, B. **Cibercriminologia: Os Meios Eletrônicos e o Policiamento em Ambientes Virtuais**. 1. Ed. Jundiaí: PACO Editorial, 2021.

GALVÃO, M. **Fundamentos em Segurança da Informação**. 1. Ed. São Paulo: Pearson Education do Brasil, 2015.

GEHRMANN, M. **Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive Information Technology for Management in Organizations**. Navus: Revista de Gestão e Tecnologia. Florianópolis, Santa Catarina, v. 2, n. 2, p. 66 - 77, jul./dez. 2012.

GOGONI, R. **O Que é ABNT?**. Tecnoblog. 2020. Disponível em: https://tecnoblog.net/312958/o-que-e-abnt. Acesso em: 22 abr. 2021.

GONÇALVES, A. **A Utilização Estratégica da Tecnologia da Informação e Comunicação para Obter Vantagem Competitiva na Indústria Hoteleira.** 2022. 97 f. Dissertação (Mestrado em Gestão e Direção Hoteleira) - A Escola Superior de Turismo e Tecnologia do Mar, Peniche, 2022.

GONZÁLEZ, M. **O que é ITIL? Entenda essa Metodologia para Gestão de TI**. Idblog. 2019. Disponível em: https://blog.idwall.co/o-que-e-itil/. Acesso em: 05 Mai. 2021.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A. e BAARS, H. **Fundamentos de Segurança da Informação com Base na ISO 27001 e na ISO 27002**. 1. Ed. Rio de Janeiro: Editora Brasport, 2018.

IAKOVAKIS, G.; XARHOULACOS, C.; GIOVAS, K. E GRITZALIS, D. **Analysis and Classification of Mitigation Tools Against Cyberattacks in COVID-19 Era.** Revista Security and Communication Networks, v. 2021, p. 1-21, 2021.

ISACA. COBIT 5 **A Business Framework for the Governance and Management of Enterprise IT**, ISACA, 2012.

KANDAN, A.; KATHRINE, G. E MELVIN, A. **Network Attacks and Prevention Techniques - A Study**. 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), p. 1-6, 2019.

KHANDO, K.; GAO, S.; ISLAM, S.; SALMAN, A. **Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review.** Computers & Security, v. 106, p. 1-22, 2021.

KIM, D.; SOLOMON, M. **Fundamentos de Segurança de Sistemas de Informação**. 1. ed. Rio de Janeiro: LTC, 2014.

KITCHENHAM, B. e CHARTERS, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering. Technical Report Eveidence-Based Software (EBSE), v. 2, n. 3, 2007.

KONZEN, M. **Gestão De Riscos De Segurança Da Informação Baseada na Norma NBR ISO/IEC 27005 Usando Padrões De Segurança**. 2013. 119 f. Dissertação (Mestrado) - Curso de Engenharia de Produção, Universidade Federal de Santa Maria, Santa Maria, 2013.

LALLIE, H.; NURSE, A.; EROLA, A.; EPIPHANIOU, A.; MAPLE, C. e BELLEKENS, X. **Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic.** Computers & Securit, v. 105, p. 1-20, 2021.

LAUDON, K. e LAUDON, J. **Sistemas de Informações Gerenciais**. 11. Ed. São Paulo: Pearson Education do Brasil, 2014.

LEÃO, P. **Auditoria de Tecnologia da Informação – A Experiência do TCE-CE**. Revista Controle – Doutrina e Artigos, v. 10, n. 1, p. 141-168, 2012.

LIMA, S.; PASSOS, O. e XAVIER, C. **Implantação de uma Fábrica de Software na Área de Tecnologia da Informação: Um Mapeamento Sistemático**. XIII Semana de Informática CESIT/UEA, Manaus, v. 7, n. 1, p. 1-12, 2019.

MARCHIORI, P. e LOPES, J. **Princípios de Informação Equitativa nas Políticas de Privacidade Online de Empresas Brasileiras**. Revista Liinc, Rio de Janeiro, v. 12, n. 1, p. 119-131, 2016.

MARTINS, E. **Pesquisa Quantitativa: Aprenda o que é e como Aplicar no seu Trabalho**. Mettzer, 2018. Disponível em: https://blog.mettzer.com/pesquisa-quantitativa. Acesso em: 18 Maio 2021.

MAZZO, B. **Relembre os 2 Principais Megavazamentos de Dados e Descubra como se Proteger das Novas Fraudes Online**. MOSP. 2021. Disponível em: https://mospadvogados.com.br/lgpd/as-principais-fraudes-decorrentes-dos-mega-vazamentos-de-dados-de-2021-e-dicas-de-como-se-proteger. Acesso em: 05 Mai. 2021.

MENEZES, D. **Tecnologlobalização e Impactos na Inovação Tecnológica**. Revista Jurídica da FA7, Fortaleza, v. 17, n. 3, p. 45-62, set./dez., 2020.

MOHAMAD, A.; RAMAYAH, T. e LO, M. **Knowledge Management in Msc Malaysia: the Role of Information Technology Capability**. International Journal of Business and Society, v. 18, p. 651–660, 2017.

NEC. **Home Office e as ameaças à Segurança da Informação**. NEC, 2020. Disponível em: https://blog.nec.com.br/home-office-e-as-ameacas-a-seguranca-da-informacao. Acesso em: 03 Julho 2021.

NURSE, J.R.C.; WILLIAMS, N.; COLLINS, E.; PANTELI, N.; BLYTHE, J. e KOPPELMAN, B. **Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy.** 23ª International Conference on Human-Computer Interaction, v.1421, p. 24-29, 2021.

OLIVEIRA, G.; MOURA, R. E ARAÚJO, F. **Gestão da Segurança da Informação: Perspectivas Baseadas na Tecnologia da Informação (T.I.).** XIX Encontro Regional de Estudantes de Biblioteconomia, Documentação, Ciência e Gestão da Informação – EREBD. 2012.

OTTONICAR, S.; BRITO, J.; SILVA, R. e ALVAREZ, E. **Competência em Informação no Contexto da Segurança da Informação: Modelo Teórico Conceitual para o Uso Seguro da Informação**. Revista Associação Catarinense de Bibliotecários, v. 25, n. 3, p. 477-492, abr./jul., 2020.

PETERSEN, K.; FELDT, R.; MUJTABA, S. e MATTSSON, M. **Systematic Mapping Studies in Software Engineering**. 12th International Conference on Evaluation and Assessment in Software Engineering. p. 71–80, 2008.

PINTO, V. **Um Modelo Conceitual para Auxiliar os Gerentes de Projetos no Gerenciamento das Lições Aprendidas**. 2019. 101 f. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Software) – Universidade Federal do Amazonas, 2019.

RAMOS, N.; YAMAGUCHI, C. e COSTA, U. **Tecnologia da Informação e Gestão do Conhecimento: Estratégia de Competitividade nas Organizações.** Brazilian Journal of Development, Curitiba, v. 6, n. 1, p. 144 – 161, Jan., 2020.

REUTERS, T. **Brasil Sofreu 15 Bilhões de Ataques Cibernéticos no 2º Trimestre, Diz Estudo**. FORBES, 2019. Disponível em: https://forbes.com.br/colunas/2019/08/brasil-sofreu-15-bilhoes-de-ataques-ciberneticos-no-2o-trimestre-diz-estudo/. Acesso em: 21 Abr. 2021.

RIOS, O.; RIOS, V. e TEIXEIRA FILHO, J. **Melhores Práticas do COBIT, Itll E ISO/IEC 27002 para Implantação de Política de Segurança da Informação em Instituições Federais do Ensino Superior**. Revista Gestão & Tecnologia, Pedro Leopoldo, v. 17, n. 1, p. 130-153, jan./abr. 2017.

RODRIGUES JR., E.; NOGUEIRA E.; MENDES, G. e CAMPOS, L. **Home Office e a Segurança da Informação em Tempos de Pandemia**. Revista eletrônica da faculdade Invest de Ciências e Tecnologias. v. 3, n. 1, p. 01-12, 2021.

ROHR, A. **Veja Dicas para Evitar Links Maliciosos e não Ser Atacado por Vírus e Páginas Clonadas.** G1 Globo,2021. Disponível em: g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/05/11/veja-dicas-para-evitar-links-maliciosos-e-nao-ser-atacado-por-virus-e-paginas-clonadas.ghtml. Acesso em: 08 de abril de 2022.

ROZA, R. **O Papel das Tecnologias da Informação e Comunicação na Atual Sociedade**. Ciência da Informação, Brasília, Distrito Federal, v. 49 n. 1, p. 1-218, jan./abr., 2020.

SANTANA, D**. Gerenciamento de Serviços de TI: O Uso das Boas Práticas de Gerenciamento de Serviços de TI com Base na Biblioteca ITIL v3**. Universidade do Vale do Rio dos Sinos. Porto Alegre, 2015.

SANTOS, E. e SOARES, T. **RISCOS, AMEAÇAS e VULNERABILIDADES: O Impacto da Segurança da Informação nas Organizações**. Revista Tecnológica da Fatec Americana, São Paulo, v. 7, n. 2, p. 43-51, Dez., 2019.

SARGINSON, N. **Securing Your Remote Workforce Against New Phishing Attacks.** Computer Fraud & Security, 2020.

SCANNAVINO, K.; NAKAGAWA, E.; FABBRI, S. e FERRARI, F. **Revisão Sistemática da Literatura em Engenharia de Software**. Elsevier Brasil, 2017.

SIQUEIRA, O.; CONTIN, A.; BARUFI, R. E LEHFELD, L. **A (Hiper)Vulnerabilidade do Consumidor no Ciberespaço e as Perspectivas da LGPD.** Revista eletrônica pesquisaduca. v. 1, n. 29, p .236-255, Jan./Abr. 2021.

SOARES, S.; SOARES, A. e ALVES, A. **A Importância da Implementação de uma Política de Segurança da Informação**. Brazilian Journal of Development, Curitiba, v. 7, n. 4, p. 37162-37171, abr., 2021.

SOUZA, M.; CAVALCANTE, A.; SILVA, A.; SOUSA, J. E SAMPAIO R. **Ameaças e Mecanismos de Segurança da Informação em um Ambiente Organizacional de Planos de Saúde.** Revista Conhecimento Contábil. Mossoró, v. 06, n. 01, p. 70-80, Jan. /Jun., 2018.

TASCHETTO, M. e FROEHLICH, C. **Teletrabalho Sob A Perspectiva dos Profissionais de Recursos Humanos do Vale do Sinos e Paranhana no Rio Grande do Sul**. Revista de Carreiras e Pessoas, v. 9, n. 3, p. 349-375, 2019.

TEIXEIRA, R. e SOUZA, R. **Empresas de Tecnologia da Informação Com Foco Na Economia Sustentável**. Revista eletrônica de biblioteconomia e ciência da informação, v. 21, n. 45, p. 100-114, Jan./Abr., 2016.

TUYIKEZE, T. e FLOWERDAY, S. **Information Security Policy Development and Implementation: A Content Analysis Approach**. 8th International Symposium on Human Aspects of Information Security and Assurance(HAISA), Plymouth, United Kingdom, p. 11-20, 2014.

UGOCHUKWU-IBE, M. e ONYEMACHI, P. **Data Security: Threats, Challenges and Protection.** Journal of Universal Development Initiative (JUDI). Owerri, v. 1, n. 1, Dez., 2014.

UOL. **Netflix, Linkedin E Minecraft: Mais De 1,4 Bilhão de Logins Vazam na Web**. TILT. 2017. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2017/12/12/netflix-linkedin-e-minecraft-mais-de-14-bilhao-de-logins-vazam-na-web.htm. Acesso em: 20 abr. 2021.

YANG, H.; ZHENG, C.; ZHU, L.; CHEN, F.; ZHAO, Y. e VALLURI, M. **Security Risks in Teleworking: A Review and Analysis.** University of Melbourne, 2013.

ZORZO, A e BERTOGLIO, D. **Um Mapeamento Sistemático sobre Testes de Penetração.** Relatório Técnico, FACIN/PUCRS, 2015. Disponível em: https://www.pucrs.br/facin-prov/wp-content/uploads/sites/19/2016/03/tr084.pdf. Acesso em: 17 Jun. 2021.

APÊNDICES

Apêndice A - Documentos do Mapeamento Sistemático

IDENTIFICADOR	Indica o ID da publicação
A. DADOS DA PUBLICAÇÃO:	
Título:	Indica o título do trabalho
Autor(es):	Nome dos autores
Fonte de Publicação:	Local de publicação
Ano de Publicação:	Ano de publicação
Resumo:	Texto contendo uma descrição do resumo
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	Descrição das ameaças à segurança
Vulnerabilidades nas organizações/funcionários	Descrição das vulnerabilidades a segurança
Práticas adotadas para a segurança da informação	Práticas adotadas pelas organizações para proteção da segurança dos dados
C. DADOS ADICIONAIS:	
Metodologia adotada:	Descrição do método usado na pesquisa para atingir o objetivo

IDENTIFICADOR	A01
A. DADOS DA PUBLICAÇÃO:	
Título:	Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic literature review
Autor(es):	Khando, K.; Gao, S.; Islam, S. e Salman, A.
Fonte de Publicação:	Google Acadêmico
Ano de Publicação:	2021
Resumo:	Revisão sistemática da literatura sobre segurança da informação com o objetivo de apresentar um conjunto de métodos e fatores que aprimorem a conscientização dos funcionários sobre a segurança da informação, além de promover boas práticas e oferecer alguns insights sobre as últimas tendências em métodos e fatores de desenvolvimento de conteúdo de segurança da informação.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Interceptação de dados por meio da engenharia social • Interceptação de documentos importantes na lixeira
Vulnerabilidades nas organizações/funcionários	• Cultura Organizacional • Período de adaptação para novas regras • Descarte inapropriado de dados confidenciais
Práticas adotadas para a segurança da informação	• Gamificação • Abordagem construtivista • Detecção de violação • Estudo de caso • Suporte de gestão • Educação e treinamento • Comportamentos dos colegas de trabalho • Congruência da mensagem e traços de personalidade
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão sistemática da literatura

IDENTIFICADOR	A02
A. DADOS DA PUBLICAÇÃO:	
Título:	Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy
Autor(es):	Nurse, J.; Williams, N.; Collins, E.; Panteli, N.; Blythe, J. e Koppelman, B.
Fonte de Publicação:	Scopus
Ano de Publicação:	2021
Resumo:	COVID-19 mudou radicalmente a sociedade como a conhecemos. Para reduzir a propagação do vírus, milhões em todo o mundo foram forçados trabalhar remotamente, muitas vezes em escritórios domésticos improvisados e usando uma infinidade de novas tecnologias digitais desconhecidas.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Maior probabilidade de ser vítima de ataques cibernéticos • Explorar um novo acesso não autorizado a dados ou serviços corporativos • Maior probabilidade de ser vítima de roubos/furtos
Vulnerabilidades nas organizações/funcionários	• Dificuldades de comunicação • Distrações causadas por um espaço de trabalho doméstico • Falta de treinamento de segurança para trabalho remoto • Não priorizar a segurança da informação devido ao isolamento • Acesso reduzido à informação • Indivíduos confiáveis/não confiáveis no ambiente de trabalho remoto • Adoção de tecnologia apressada • Uso de serviços de terceiros para arquivos de trabalho confidenciais • Falta de familiaridade com a nova tecnologia • Uso intencional ou inadvertido de dispositivos de trabalho para assuntos pessoais • Os dispositivos de trabalho podem ser roubados da casa ou do ambiente de trabalho remoto
Práticas adotadas para a segurança da informação	-
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão Bibliográfica

IDENTIFICADOR	A04
A. DADOS DA PUBLICAÇÃO:	
A. DADOS DA PUBLICAÇÃO:	
Título:	Analysis and Classification of Mitigation Tools against Cyber security
Título:	Cyberattacks in COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic
Autor(es):	Iakovakis, G.; Xanthoulacos, C.; Glovas, K. e Gritzalis, D.
Autor(es):	Lallie, H.; Shepherd, L.; Nurse, J.; Eola, A.; Epiphaniou, G.; Maple, C. e Bellekens, X.
Fonte de Publicação:	Scopus
Ano de Publicação:	2021
Resumo:	A pandemia do COVID-19 foi um evento notável e sem precedentes que alterou a vida de bilhões de cidadãos em todo o mundo. Este artigo analisa a pandemia de COVID-19 a partir de uma perspectiva de crimes cibernéticos e destaca a gama de ataques cibernéticos experimentados globalmente durante a pandemia. A análise mostra como, após o que pareciam ser grandes lacunas entre o surto inicial da pandemia na China e o primeiro ataque cibernético relacionado ao COVID 19, os ataques se tornaram muito mais prevalentes a ponto de, em alguns dias, três ou quatro ataques cibernéticos únicos. Ataques estavam sendo relatados.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Engenharia Social • Sites Fraudulentos • E-mails Fraudulentos • Links Falsos • Oportunidades Falsas • Chantagens • Phishing • Ataque Malwares • Ransomware • Hacking • Negação de Serviço • Fraude Financeira • Pharming • Extorsão • DoS
Vulnerabilidades nas organizações/funcionários	• Distração • Restrição do Tempo • Pânico • Pressão no Trabalho • Fatalidade e Catástrofe • Ansiedade • Ativos corporativos menos protegidos
Práticas adotadas para a segurança da informação	• Não acessar links duvidosos • Verificar o e-mail recebido
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão Bibliográfica

Fonte de Publicação:	Scopus
Ano de Publicação:	2021
Resumo:	O surto de COVID-19 forçou as empresas a mudar para um ambiente empresarial sem precedentes de "trabalho em casa". Na pesquisa, é fornecida uma classificação detalhada para um conjunto de ferramentas que facilitarão a mitigação e prevenção de riscos. O objetivo é fornecer uma taxonomia multifacetada e análise de ferramentas de mitigação, que apoiarão as empresas em seu esforço para proteger suas redes de computadores.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Phishing • Ransomware • Dominios Fradulentos • Sms falsos • Ataque por e-mail • Fake News • Malware
Vulnerabilidades nas organizações/funcionários	• Dispositivos pessoais • Acesso a link desconhecidos
Práticas adotadas para a segurança da informação	• Não acessar links duvidosos • Verificar o e-mail recebido • Scanners de Vulnerabilidades • Atualizar o firewall • Ferramenta de Monitoramento de *Logging* • Software de Antivírus • Conscientização dos usuários
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão Bibliográfica

IDENTIFICADOR	A05
A. DADOS DA PUBLICAÇÃO:	
Título:	Home Office e a Segurança da Informação em Tempos de Pandemia
Autor(es):	Rodrigues, W.; Nogueira, E.; Mendes, G. e Campos, L.
Fonte de Publicação:	Google Acadêmico
Ano de Publicação:	2021
Resumo:	Estamos vivendo em uma época de grandes mudanças, tanto o Brasil como outros países ao redor do mundo todo estão enfrentando a pandemia de coronavírus (COVID-19). O presente artigo tem como objetivo informar e apresentar práticas que possam auxiliar na manutenção da segurança cibernética no home office, utilizando como metodologia a revisão de literatura.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Malware • Trojans • *Rootkits* • portas do firewall • Sites maliciosos • E-mail maliciosos • *phishin*
Vulnerabilidades nas organizações/funcionários	• Uso de notebook pessoal • Falta de autenticação • *Pendrive* com vírus • Utilização de senhas comuns • Utilização de softwares piratas • Abrir e-mail desconhecido • *Spoofing* – falsificação de identidade na rede
Práticas adotadas para a segurança da informação	• Medida de proteção em ambiente de rede caseira • Medidas de autenticação • Políticas de segurança • VPN • Treinamento dos funcionários • Logins distintos para o pessoal e trabalho • Antivírus • Evitar o uso de *pendrives* • Evitar uso de HD externo • uso constante de backups do sistema
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão Bibliográfica

IDENTIFICADOR	A06
A. DADOS DA PUBLICAÇÃO:	
Título:	Securing your remote workforce against new phishing attacks. Computer Fraud & Security
Autor(es):	Sarginson, N.
Fonte de Publicação:	Scopus
Ano de Publicação:	2020
Resumo:	À medida que a disseminação do Covid-19 forçou as organizações em todo o mundo a introduzir medidas preventivas, o número de pessoas trabalhando remotamente aumentou drasticamente. No entanto, a tradução do trabalho baseado no escritório para o trabalho em casa teve que acontecer rapidamente – para alguns, literalmente da noite para o dia. Sob tais condições, a implementação de novas medidas de segurança ainda não implementadas é um desafio.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Ataques de Phishing • Engenharia Social • Golpes de e-mail
Vulnerabilidades nas organizações/funcionários	• Computadores menos seguros • Redes menos seguras • Acessar links desconhecidos
Práticas adotadas para a segurança da informação	• Uso de ferramentas de segurança adequadas • Acessar links confiáveis • Mudanças de senhas • Não compartilhar senhas • Uso de VPN • Métodos robustos de autenticação
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão Bibliográfica

IDENTIFICADOR	A07
A. DADOS DA PUBLICAÇÃO:	
Título:	Network Attacks and Prevention Techniques - A Study
Autor(es):	Kandan, A.; Kathrine, G., & Melvin, A
Fonte de Publicação:	Scopus
Ano de Publicação:	2019
Resumo:	Com as indústrias inspiradoras na estratégia traga seu próprio dispositivo, o espectro de ameaças se expandiu significativamente. Nesse caso, é imperativo monitorar e proteger os dados em trânsito, bem como no próprio dispositivo. Muitas pequenas redes domésticas/de escritório não se esforçam para configurar seus ativos com segurança, o que abre o portão para uma série variada de ataques e comprometimentos de rede.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• E-mails de phishing
Vulnerabilidades nas organizações/funcionários	• Acesso a sites não autenticados
Práticas adotadas para a segurança da informação	• Criptografia Forte • Uso de VPN • Utilizar comunicação via HTTPS • Firewall sempre atualizado para última versão
C. DADOS ADICIONAIS:	
Metodologia adotada:	Pesquisa Bibliográfica

IDENTIFICADOR	A08
A. DADOS DA PUBLICAÇÃO:	
Título:	Information Security Strategy and Teleworking (In)security
Autor(es):	Ampomah, M., De Silva, Y., Li, H., Pahlisa, P., Yang, Q., & Zhang, Q
Fonte de Publicação:	Google Acadêmico
Ano de Publicação:	2013
Resumo:	A escrita convencional de teletrabalho tende a se concentrar nos benefícios econômicos e sociais com poucos ênfase nas questões de segurança da informação. Ameaças de segurança da informação do teletrabalho, no entanto, são identificados pela maioria da literatura como uma preocupação para as organizações. As organizações precisam essencialmente implementar segurança medidas ou controles de um ponto de vista estratégico para incluir controles formais e informais.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Acesso não autorizado por terceiros • Maior chance de ser vítima de roubo/furto • Técnicas de engenharia social
Vulnerabilidades nas organizações/funcionários	• Falta de consciência de segurança por parte dos funcionários • Divulgação de informações para concorrentes • Identificação comprometida • Equipamento Físico • Roubo • Rede de acesso insegura • Comprometimento organizacional deficiente • Incapacidade de monitorar
Práticas adotadas para a segurança da informação	• Treinamento e métodos casuais de conscientização da importância de segurança da informação • Disponibilizar informações de acordo com nível de classificação do funcionário dentro da organização • Monitoramento da comunicação dos teletrabalhadores para prevenir a divulgação de informações sensíveis sem ferir a privacidade do mesmo • A aplicação de procedimentos administrativos apropriados, como complexidade e duração da senha para previr acesso não autorizados de terceiros • Uso de VPN, antivírus e *antimalware* nos dispositivos • Ter um plano de emergência para a interrupção no fornecimento de energia
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão da Bibliográfica

IDENTIFICADOR	A09
A. DADOS DA PUBLICAÇÃO:	
Título:	Security Risks in Teleworking: A Review and Analysi
Autor(es):	Yang, H.; Zheng, C.; Zhu, L.; Chen, F.; Zhao, Y. & Valluri, M.
Fonte de Publicação:	Google Acadêmico
Ano de Publicação:	2013
Resumo:	O teletrabalho como uma prática de trabalho inovadora atrai as organizações a aplicá-lo em organizações inteiras, proporcionando muitos benefícios. No entanto, os riscos relacionados à segurança da informação gerados no teletrabalho ameaçam as organizações para implementá-lo.
B. DADOS DERIVADOS DO OBJETO:	
Ameaça à segurança da informação	• Cópia impressa de informações confidenciais é extraviada ou roubada • Interceptação de dados durante a transmissão se utilizando canais de comunicação • Furto/roubo do computador pessoal contendo informações confidenciais ou chave de segurança
Vulnerabilidades nas organizações/funcionários	• Divulgação não autorizada de dados • Risco de vazamento de informações para os indivíduos errados será aumentado no home office • Impressão de informações confidenciais • Rede de acesso insegura • Instalação de programas duvidosos • Desastre natural (terremoto, incêndio, inundação). • Burlar o sistema de segurança da organização para acessar sites restritos/não confiáveis • Computador pessoal não apropriado para acesso seguro ao servidor da organização • Modificação de dados acidentalmente no ambiente home office • Segurança/Política da empresa incapaz de monitorar o tráfego de dados • Interrupções abruptas na comunicação entre funcionários e o servidor da organização podem ocasionar enormes prejuízos para o funcionário e para a organizações • Mudanças na tecnologia adotada
Práticas adotadas para a segurança da informação	• Treinamento em segurança da informação • Criptografia de dados • Ter o próprio canal de comunicação para transmissão de dados confidenciais • Desenvolver programas de treinamento para funcionários trabalharem de maneira segura no home office • Fazer backup de dados • Proteger os dispositivos de acesso
C. DADOS ADICIONAIS:	
Metodologia adotada:	Revisão da Bibliográfica

Apêndice B - Questionário com os Profissionais

Caracterização dos Participantes

Qual sua faixa etária de idade?
( ) Até 21 anos
( ) de 22 a 26 anos
( ) de 27 a 30 anos
( ) de 31 a 35 anos
( ) Acima de 36 anos

Organização que atua?
( ) Privada
( ) Pública

Formação?
( ) Administração
( ) Recursos Humanos
( ) Engenharia
( ) Tecnologia da Informação
( ) Direito

Área de atuação na organização?
( ) Administração
( ) Contratação de pessoas
( ) Análise jurídica
( ) Planejamento
( ) Controle
( ) Tecnologia da Informação

Quanto tempo de trabalho possui na organização?
( ) menos de 6 meses
( ) de 6 meses a 1 ano
( ) mais de 1 ano a 2 anos
( ) mais de 2 anos

Seleção das práticas adotadas na segurança da informação

Exerceu trabalho em home office?
( ) sim
( ) não

Dentre as opções abaixo, marque somente 3 que acha ser importante para a segurança da informação em ambiente home office?

- Medidas de autenticação
- Ferramentas de monitoramento de acesso
- Adoção de políticas de segurança
- Medida de proteção do ambiente
- Uso de programa de *antimalware*
- Evitar clicar em links desconhecidos
- Uso seguro das senhas
- Treinamento com os funcionários

Identificação do Nível de Relevância de acordo com as Práticas de Segurança da Informação

Marque o quão relevante você considera as práticas a seguir para a segurança da informação em ambiente home office.

ID	Questão	Sem Relevância	Baixa Relevância	Média Relevância	Alta Relevância	Altíssima Relevância.
Q1	Evitar usar dispositivo pessoal para o trabalho					
Q2	Não acessar sites inseguros					
Q3	Comunicação com a empresa					
Q4	Treinamento para o trabalho em home office					
Q5	Comprometimento organizacional					
Q6	Descarte seguro de dados confidenciais empresarial					
Q7	Usar rede privada virtual (VPN)					
Q8	Usar antivírus					
Q9	Uso seguro de senhas					
Q10	Política de segurança organizacional					
Q11	Medidas de autenticação					
Q12	Proteção do ambiente de trabalho em casa					
Q13	Ferramenta de monitoramento de *logging*					