POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO HOME OFFICE: ESTRATÉGIAS PARA PROTEGER DADOS EM AMBIENTES REMOTOS

INFORMATION SECURITY POLICIES IN THE HOME OFFICE: STRATEGIES FOR PROTECTING DATA IN REMOTE ENVIRONMENTS

Juliana Aparecida Mistron
Fatec Araraquara – Prof. José Arana Varela
juliana.mistron@fatec.sp.gov.br

Isaías da Silva Moura
Fatec Araraquara – Prof. José Arana Varela
isaias.moura@fatec.sp.gov.br

Wdson de Oliveira
Fatec Araraquara - Prof. José Arana Varela
Wdson.oliveira01@fatec.sp.gov.br

Resumo

Este artigo analisa os desafios e as melhores práticas para a implementação de políticas de segurança da informação em home office. Foi realizada uma revisão bibliográfica e uma pesquisa quantitativa, que envolveu 53 participantes, revelando que a maioria das empresas já possui políticas de segurança, mas há lacunas em sua implementação e no conhecimento dos colaboradores. Os principais desafios estão relacionados à complexidade das políticas, à falta de equipamentos adequados e ao baixo nível de conhecimento sobre segurança. A pesquisa destaca a importância da conscientização dos colaboradores, da adoção de tecnologias como VPNs e da revisão periódica das políticas para garantir a proteção dos dados. Os resultados sugerem que, embora as políticas de segurança sejam vistas como importantes, ainda precisam ser aprimoradas para garantir a segurança da informação em ambientes de trabalho remoto.

Palavras-chave: Segurança da Informação, Home Office, Vulnerabilidades, Políticas de Segurança.

Abstract

This article analyzes the challenges and best practices for implementing information security policies in remote work environments. A bibliographic review and a quantitative study were conducted, involving 53 participants, revealing that most companies already have security policies in place, but there are gaps in their implementation and in employees' knowledge. The main challenges are related to the complexity of the policies, the lack of adequate equipment,

and the low level of security knowledge. The study highlights the importance of employee awareness, the adoption of technologies like VPNs, and the periodic review of policies to ensure data protection. The results suggest that, although security policies are seen as important, they still need to be improved to ensure information security in remote work environments.

***Keywords**: Information Security, Home Office, Vulnerabilities, Security Policies.*

1. Introdução

A crescente adoção do trabalho remoto transformou a maneira como as empresas gerenciam suas operações e, consequentemente, aumentou os desafios relacionados à segurança da informação. Com funcionários trabalhando em ambientes fora do controle direto da organização, surgem novas vulnerabilidades que exigem a implementação de políticas robustas de segurança para proteger dados sensíveis. A migração acelerada para o *home office*, impulsionada pela pandemia de COVID-19, destacou a necessidade de estratégias específicas que atendam às demandas desse modelo de trabalho, onde dispositivos pessoais e redes domésticas são frequentemente utilizados (NASCIMENTO et al, 2023).

Nesse contexto, o objetivo deste artigo é responder à seguinte questão de pesquisa: Quais são os principais desafios e as melhores práticas para a implementação de políticas de segurança da informação no *home office*, de forma a proteger dados sensíveis e mitigar riscos cibernéticos? A pesquisa busca entender como as empresas podem adotar uma abordagem integrada, que envolva a conscientização dos colaboradores, o uso de ferramentas de segurança adequadas e a aplicação de protocolos de resposta a incidentes. A proteção dos dados não se limita ao uso de senhas fortes ou *softwares* antivírus; é essencial garantir que as práticas de segurança sejam seguidas consistentemente, e que os colaboradores entendam a importância de sua adesão às normas estabelecidas. Para isso, a educação contínua sobre ameaças cibernéticas e treinamentos regulares são partes indispensáveis de qualquer política eficaz (FERRO, 2024).

Além disso, as políticas de segurança precisam se adaptar à flexibilidade do *home office*, estabelecendo diretrizes claras sobre o uso de dispositivos pessoais e a separação de dados corporativos e pessoais. O uso de redes privadas virtuais (VPNs), a criptografia de dados e a autenticação multifator são exemplos de medidas técnicas que podem ser incorporadas às políticas para reforçar a segurança. Essas soluções técnicas, quando combinadas com a

conscientização dos funcionários, criam um ambiente mais seguro, mitigando riscos como o roubo de dados e o acesso não autorizado (SILVA, 2023).

Outro ponto crucial para o sucesso das políticas de segurança em *home office* é o monitoramento constante e a atualização das medidas adotadas. O ambiente de ameaças cibernéticas está em constante evolução, e as empresas precisam revisar suas políticas regularmente para acompanhar as novas técnicas de invasão. A implementação de controles periódicos e auditorias de segurança pode ajudar a identificar falhas e promover ajustes que mantenham a proteção sempre atualizada (KLEINJOHANN et al, 2021).

O desenvolvimento de políticas de segurança da informação voltadas para o trabalho remoto deve ser uma prioridade estratégica para qualquer empresa que adote o *home office*. Essas políticas são essenciais para garantir a proteção de dados em todos os níveis, desde dispositivos individuais até servidores corporativos. Além de mitigar riscos como perdas financeiras e danos à reputação, a implementação de medidas de segurança robustas promove um ambiente de trabalho mais confiável e produtivo para os colaboradores (COSTA, 2024).

2. Referencial Teórico

O presente capítulo tem como objetivo embasar teoricamente o desenvolvimento de políticas de segurança da informação aplicadas ao contexto do trabalho remoto, com ênfase na proteção de dados em ambientes de *home office*. Para isso, serão incluídos os principais conceitos e teorias que envolvem a segurança da informação, bem como as normativas e boas práticas que orientam a criação de diretrizes eficazes para a proteção das informações.

2.1 Segurança da Informação no Contexto Atual

Atualmente, a segurança da informação tornou-se um dos pilares essenciais para a sustentabilidade das operações empresariais, governamentais e até pessoais. A digitalização crescente das atividades, impulsionada por inovações tecnológicas e pelo aumento do uso da internet, trouxe novos desafios e ameaças à integridade dos dados. Ataques cibernéticos, como o *ransomware* e o *phishing*, estão se tornando cada vez mais sofisticados, afetando empresas de todos os setores e tamanhos. A necessidade de proteger informações sensíveis, sejam elas

financeiras, pessoais ou operacionais, é um imperativo para garantir a continuidade dos negócios e a confiança dos *stakeholders* (WARZEL; PETERSEN, 2022).

As empresas, especialmente aquelas que operam com dados críticos, enfrentam a pressão de adequar suas práticas de segurança à realidade digital. A legislação, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na Europa, forçou organizações a adotar medidas mais rigorosas de proteção e privacidade de dados. Não se trata apenas de evitar ataques cibernéticos, mas também de garantir que os dados sejam manipulados de forma ética e legal. A implementação dessas leis trouxe à tona a necessidade de uma cultura de segurança da informação, que permeia desde a alta gestão até os colaboradores operacionais (FANSTONE; CARVALHO; TRISTÃO, 2021).

Além disso, a popularização do trabalho remoto e a adoção de tecnologias como a nuvem ampliaram a superfície de ataque das organizações. O uso de dispositivos pessoais para acessar redes corporativas e a dependência de serviços de terceiros para armazenamento de dados requerem políticas de segurança mais abrangentes. As soluções convencionais de segurança, baseadas apenas em *firewalls* e antivírus já não são suficientes para conter a diversidade e complexidade dos ataques atuais. Assim, tecnologias avançadas como a inteligência artificial e a análise de comportamento estão sendo empregadas para detectar e mitigar ameaças em tempo real (ROCKENBACH, 2021).

Outro aspecto importante da segurança da informação no contexto atual é a conscientização dos usuários. Muitos ataques são bem-sucedidos devido à falha humana, seja por negligência ou desconhecimento das melhores práticas de segurança. Programas de educação e treinamento contínuo sobre ameaças cibernéticas e medidas preventivas são cruciais para minimizar esses riscos. Ao investir em conscientização, as organizações não apenas fortalecem suas defesas tecnológicas, mas também criam uma linha de defesa humana capaz de identificar e evitar potenciais vulnerabilidades (LOPES; DE CASTRO, 2022).

Portanto, a segurança da informação no cenário contemporâneo não pode ser vista como uma responsabilidade exclusiva do departamento de TI, mas sim como uma prioridade estratégica para toda a organização. Com a crescente complexidade das ameaças e a regulamentação cada vez mais rigorosa, as empresas precisam adotar uma abordagem proativa

e integrada, que combine tecnologia de ponta, políticas robustas e uma forte cultura de segurança entre seus colaboradores. Somente assim será possível proteger os dados, manter a confiança e assegurar a continuidade das operações no ambiente digital (SANTOS, 2021).

2.2 Riscos e Ameaças no *Home Office*

Com a expansão do trabalho remoto, surgiram novos riscos e ameaças à segurança da informação que exigem atenção especial por parte das empresas e colaboradores. O *home office*, embora traga benefícios como flexibilidade e redução de custos, também aumenta a vulnerabilidade das redes e dispositivos utilizados fora do ambiente corporativo. Um dos principais riscos é o uso de redes domésticas, muitas vezes mal protegidas, que podem ser alvo de invasores. Redes sem criptografia ou com senhas fracas facilitam o acesso não autorizado a informações sensíveis, tornando as organizações mais suscetíveis a ataques cibernéticos (BRANDÃO; PERUCCHI; FREIRE, 2023)

Outro risco significativo está relacionado ao uso de dispositivos pessoais para acessar sistemas corporativos. Muitos colaboradores utilizam computadores e *smartphones* que não possuem os mesmos níveis de segurança que os dispositivos fornecidos pelas empresas, como antivírus atualizados ou *firewalls* adequados. Isso abre portas para *malwares*, *spywares* e outras formas de *software* malicioso que podem se infiltrar na rede da empresa através de conexões inseguras ou comportamentos descuidados dos usuários, como clicar em *links* suspeitos ou baixar arquivos infectados (MORO et al, 2023).

A falta de controle direto sobre os colaboradores no ambiente doméstico também contribui para o aumento das ameaças. No *home office*, é mais difícil monitorar a adesão dos funcionários às políticas de segurança, o que pode resultar em falhas de *compliance*, como o armazenamento inadequado de dados ou o compartilhamento de informações confidenciais em plataformas não autorizadas. O uso de ferramentas de colaboração online, se não devidamente controladas, pode gerar vulnerabilidades de segurança, especialmente quando os dados trafegam por serviços de terceiros que não possuem os mesmos padrões de proteção da empresa (COSTA, 2022).

O *Phishing* também é uma ameaça que cresce no ambiente de *home office*. Os cibercriminosos aproveitam a dispersão dos colaboradores para realizar ataques direcionados, enviando e-mails fraudulentos que parecem vir de fontes confiáveis, como a própria empresa ou parceiros comerciais. A falta de interação presencial pode reduzir a capacidade dos colaboradores de identificar essas tentativas de golpe, levando a vazamentos de credenciais e comprometimento de dados. Além disso, a ausência de supervisão imediata no *home office* torna mais difícil detectar rapidamente quando uma credencial é comprometida (NEVES; PEREIRA; DA SILVA, 2021).

Portanto, mitigar os riscos e ameaças no *home office* exige um esforço coordenado entre tecnologia, políticas de segurança robustas e a educação contínua dos colaboradores. Implementar medidas como o uso de redes privadas virtuais (VPNs), autenticação multifator e a criptografia de dados são essenciais para minimizar vulnerabilidades. Além disso, promover treinamentos regulares e conscientização sobre as boas práticas de segurança é vital para garantir que todos os membros da organização estejam alinhados às diretrizes de proteção da informação (COELHO et al, 2022).

2.3 Políticas de Segurança da Informação

As políticas de segurança da informação são um conjunto de diretrizes e práticas estabelecidas por uma organização para proteger seus ativos digitais, incluindo dados, sistemas e redes, contra ameaças internas e externas. Elas servem como um manual para garantir que os colaboradores e todos os envolvidos no ambiente corporativo sigam padrões de segurança que minimizem os riscos de incidentes cibernéticos. Essas políticas abrangem desde o controle de acesso a sistemas, até a proteção de dados sensíveis, gestão de senhas, uso de dispositivos e resposta a incidentes de segurança (JOTA, 2023).

Em ambientes físicos, muitas empresas já adotam políticas rigorosas para proteger suas informações. Exemplos comuns incluem o uso de crachás e autenticação biométrica para acessar áreas restritas, bloqueio de estações de trabalho quando não estão em uso, a implementação de *firewalls* e antivírus, e a criptografia de dados armazenados em servidores internos. Há também controles rígidos sobre a entrada de dispositivos pessoais, como USBs,

e o monitoramento de redes locais por meio de sistemas de detecção de intrusões (IDS). Essas práticas ajudam a criar uma barreira para proteger os dados e o patrimônio digital da empresa de ataques externos e de ameaças internas (STAUBITZ, 2021).

No entanto, com a migração para o trabalho remoto, essas políticas precisam ser adaptadas para garantir a proteção de informações sensíveis fora do ambiente corporativo. Uma política de segurança adaptada para o *home office* pode incluir o uso obrigatório de redes privadas virtuais (VPNs) para acessar sistemas corporativos, o que garante a criptografia das conexões entre o dispositivo do colaborador e os servidores da empresa (OLIVEIRA, 2021). Além disso, é comum implementar a autenticação multifator (MFA) como uma camada adicional de proteção ao login de sistemas críticos. A política também deve abranger diretrizes claras sobre o uso de dispositivos pessoais, como *notebooks* e *smartphones*, exigindo que esses dispositivos estejam protegidos com senhas, criptografia e *software* de segurança atualizado (SOUZA; COSTA, 2024).

Outro exemplo de adaptação de políticas de segurança para o trabalho remoto é a conscientização e treinamento contínuo dos colaboradores sobre boas práticas de segurança, como a identificação de e-mails de *phishing* e a importância de não compartilhar credenciais. Ferramentas de monitoramento remoto também podem ser incluídas para rastrear o acesso e as atividades realizadas em sistemas corporativos, além da aplicação de políticas de *backup* remoto para assegurar a recuperação de dados em caso de incidentes (MENDES, 2022).

Essas adaptações, somadas à implementação de controles tecnológicos, como a criptografia e o uso de soluções de gestão de identidade, garantem que as informações da empresa estejam seguras mesmo fora dos limites físicos do escritório. Com essas medidas, as políticas de segurança da informação podem oferecer um nível de proteção adequado para o ambiente remoto, evitando vulnerabilidades de segurança e garantindo a conformidade com regulamentos de proteção de dados (RODRIGUES, 2022).

2.4 Políticas de Segurança da Informação

As normas e padrões de segurança da informação fornecem a base essencial para garantir a proteção de dados e a conformidade regulatória nas organizações, especialmente em

ambientes de trabalho remoto. Esses padrões funcionam como guias que as empresas podem seguir para proteger suas informações e se alinhar às exigências legais e de mercado. Entre as normas mais relevantes estão a ISO/IEC 27001 e a Lei Geral de Proteção de Dados (LGPD), ambas essenciais para o desenvolvimento de políticas robustas de segurança, além de outras regulamentações globais que contribuem para a criação de um ambiente seguro para o *home office* (PEREIRA; NEVES, 2021).

A ISO/IEC 27001 é um padrão internacional amplamente reconhecido para a gestão da segurança da informação. Ela define os requisitos para a criação, implementação, manutenção e melhoria contínua de um sistema de gestão de segurança da informação (SGSI). Este padrão oferece uma abordagem sistemática para proteger dados confidenciais, abrange controles de segurança que mitigam riscos cibernéticos e busca a confidencialidade, integridade e disponibilidade das informações (RODRIGUES; ARAÚJO; TORQUATO, 2023). No contexto do *home office*, a ISO/IEC 27001 é especialmente útil para empresas que precisam garantir a segurança das informações fora do ambiente físico controlado, fornecendo diretrizes para práticas como o controle de acesso remoto, gestão de riscos e políticas de segurança adaptadas ao trabalho à distância (FRANCISCO; MPANDA, 2023).

Já a Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde 2020, regula a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, tanto por entidades públicas quanto privadas. Ela é crucial para proteger os direitos de privacidade dos indivíduos e garantir a transparência no uso dos dados. No ambiente de *home office*, as empresas devem estar atentas ao cumprimento da LGPD, principalmente no que diz respeito ao uso de dados pessoais por parte dos colaboradores fora do ambiente corporativo (CHAGAS, 2023). A conformidade com a LGPD exige que as organizações adotem medidas como criptografia de dados sensíveis, consentimento para o tratamento de informações pessoais e a implementação de controles rigorosos para evitar o vazamento de dados. O não cumprimento dessa legislação pode resultar em multas significativas e danos à reputação da empresa (BERWALDT, 2022).

Além da ISO/IEC 27001 e da LGPD, outras normas e regulamentações também desempenham um papel importante na segurança da informação no *home office*. A ISO/IEC 27002, por exemplo, complementa a ISO/IEC 27001, oferecendo um conjunto detalhado de

práticas recomendadas para controles de segurança. A General Data Protection Regulation (GDPR), da União Europeia, é outra regulamentação relevante, especialmente para empresas que lidam com dados de cidadãos europeus. Assim como a LGPD, a GDPR impõe regras rígidas sobre como os dados pessoais devem ser tratados, incluindo o direito de os titulares dos dados solicitarem a exclusão ou correção de suas informações. A NIST SP 800-53, do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos, também é amplamente adotada por organizações que buscam melhorar a sua postura de segurança, fornecendo diretrizes sobre como gerenciar e monitorar riscos cibernéticos (SILVA; DE SOUZA, 2020).

A conformidade com esses padrões e regulamentações é fundamental para garantir a segurança da informação, especialmente em um cenário de trabalho remoto. Com uma base sólida de normas e uma estrutura de controle eficiente, as empresas podem assegurar a proteção de dados e evitar penalidades legais. Implementar essas práticas no *home office* é um desafio que exige a conscientização dos colaboradores, políticas adaptadas e o uso de tecnologias apropriadas para garantir que os dados permaneçam seguros, independentemente de onde estejam sendo acessados (OLIVEIRA; ARMOND, 2022).

3. Metodologia

A fim de atingir os objetivos propostos neste trabalho, foi realizado um levantamento bibliográfico que serviu como base conceitual para o desenvolvimento do artigo. A pesquisa envolveu a consulta a livros, revistas especializadas e artigos disponíveis na internet.

Além da pesquisa bibliográfica, foi conduzida uma pesquisa quantitativa com o objetivo de analisar dados objetivos e mensurar a percepção sobre a segurança e a eficácia das políticas de segurança da informação em ambientes de trabalho remoto.

A coleta de dados foi realizada por meio de um questionário online, desenvolvido com a ferramenta Google Forms. O questionário foi estruturado com perguntas objetivas e fechadas, organizadas em seções para abordar diferentes aspectos da segurança da informação em home office. As questões foram elaboradas para avaliar práticas de segurança, percepção dos

colaboradores sobre a eficácia das políticas, desafios enfrentados e o nível de conscientização sobre ameaças cibernéticas.

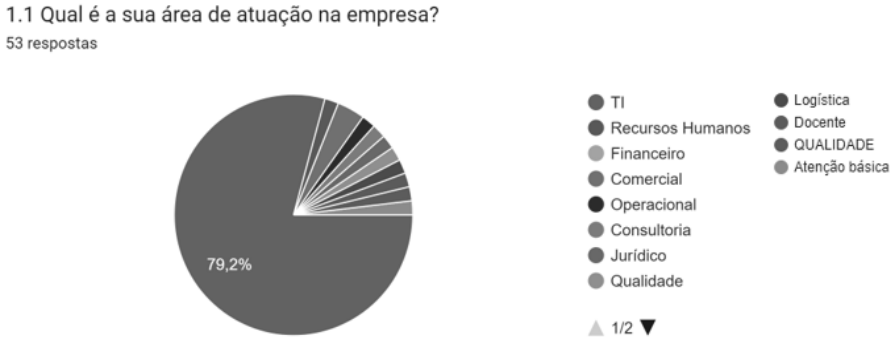
A amostra foi composta por colaboradores de empresas localizadas na região de Araraquara que adotaram o modelo de *home office*. Os participantes foram selecionados com base em critérios específicos, como: estarem empregados em empresas que implementaram o trabalho remoto, estarem envolvidos diretamente com o cumprimento das políticas de segurança da informação e aceitarem participar voluntariamente da pesquisa. A coleta de dados ocorreu nos dias 5 e 6 de novembro de 2024, com um total de 53 respondentes.

O objetivo da pesquisa foi identificar as práticas, percepções e desafios enfrentados na implementação e no cumprimento das políticas de segurança da informação no contexto do *home office*, fornecendo resultados sobre a eficácia das estratégias adotadas.

4. Resultados e Discussões

A Figura 1 mostra a distribuição dos participantes da pesquisa conforme sua área de atuação nas empresas. A maioria é da área de Tecnologia da Informação (TI), com 79,2%. A área Comercial tem 3,8%, seguida por Recursos Humanos (1,9%), Operacional (1,9%), Consultoria (1,9%), Jurídico (1,9%), Qualidade (1,9%), Logística (1,9%), Docente (1,9%) e Atenção Básica (1,9%). A área financeira não teve nenhum respondente.

Figura 1 - Área de atuação dos participantes



Fonte: Elaborado pelos autores

A Figura 2 revela a distribuição hierárquica dos respondentes. O nível Operacional representa a maioria, com 62,3% das respostas. Outros níveis, como Supervisão (9,4%), Gerência (11,3%), Diretoria (9,4%), e Consultor ou Autônomo (7,5%), têm presença menor.

Figura 2 - Nível hierárquico dos participantes

Fonte: Elaborado pelos autores

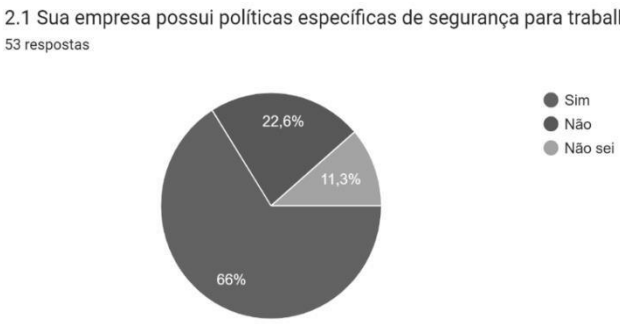
A Figura 3 aponta que a maioria dos colaboradores (42,3%) iniciou o trabalho remoto há menos de um ano, indicando uma adoção recente dessa modalidade na empresa. Outros 17,3% trabalham em regime home office há 1 a 2 anos, enquanto 28,8% possuem entre 3 e 4 anos de experiência, sugerindo um processo de adaptação em curso. No entanto, apenas 11,5% dos colaboradores têm mais de cinco anos de experiência em *home office*, o que indica que a adoção do trabalho remoto tem se intensificado ao longo do tempo.

Figura 3 - Tempo de trabalho em regime de home office

Fonte: Elaborado pelos autores

A Figura 4 mostra que, embora a maioria das empresas (66%) já tenha implementado políticas de segurança para o trabalho remoto, uma parcela significativa (22,6%) ainda não o fez, o que as expõe a riscos cibernéticos. Além disso, a falta de conhecimento sobre essas políticas por parte de 11,3% dos colaboradores destaca a necessidade de aprimorar a comunicação interna e garantir o acesso claro às medidas de segurança.

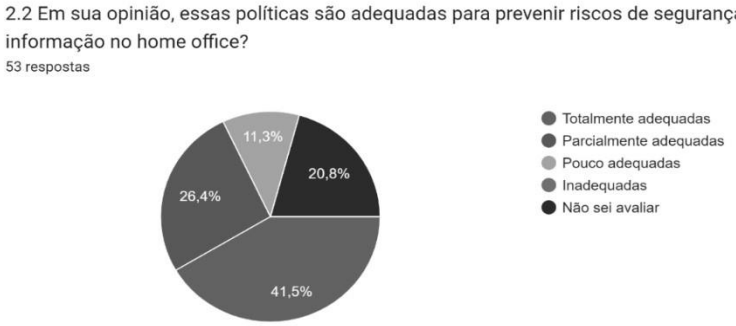
Figura 4 - Políticas de segurança



Fonte: Elaborado pelos autores

A Figura 5 demonstra uma divisão de opiniões sobre a eficácia das políticas de segurança da informação no contexto do trabalho remoto. Enquanto 41,5% dos entrevistados consideram as políticas totalmente adequadas, 26,4% as avaliam como parcialmente adequadas, 11,3% as avaliam como pouco adequadas e 20,8% não souberam avaliar.

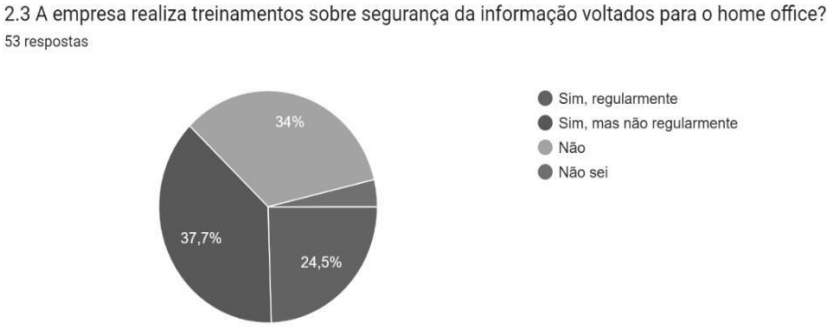
Figura 5 - Políticas de segurança adequadas



Fonte: Elaborado pelos autores

A Figura 6 ilustra que 24,5% das empresas oferecem treinamentos regulares sobre segurança da informação para colaboradores em regime de *home office*, enquanto 37,7% não realizam essa prática de forma regular. Além disso, 34% afirmaram não receber treinamentos sobre segurança da informação e 3,8% dos respondentes não souberam responder.

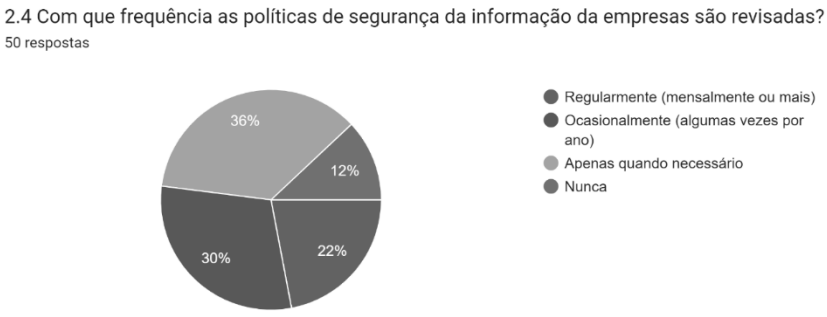
Figura 6 - Treinamentos sobre segurança da informação



Fonte: Elaborado pelos autores

A Figura 7 aponta que 22% das empresas revisam suas políticas de segurança da informação de forma regular, 30% o fazem ocasionalmente e 36% apenas quando considerado necessário. No entanto, 12% nunca realizam essa revisão, o que as torna vulneráveis a riscos e dificulta a adaptação às mudanças nas ameaças cibernéticas.

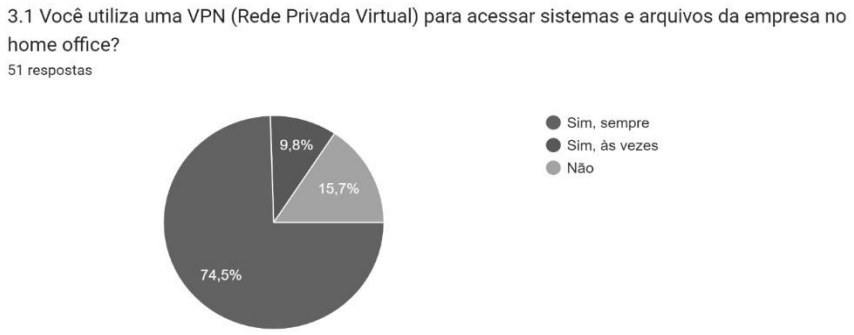
Figura 7 - Frequência de revisão das políticas de segurança



Fonte: Elaborado pelos autores

A Figura 8 indica que 74,5% dos colaboradores utilizam VPN de forma regular no trabalho remoto, 9,8% utilizam ocasionalmente e 15,7% não fazem uso da ferramenta.

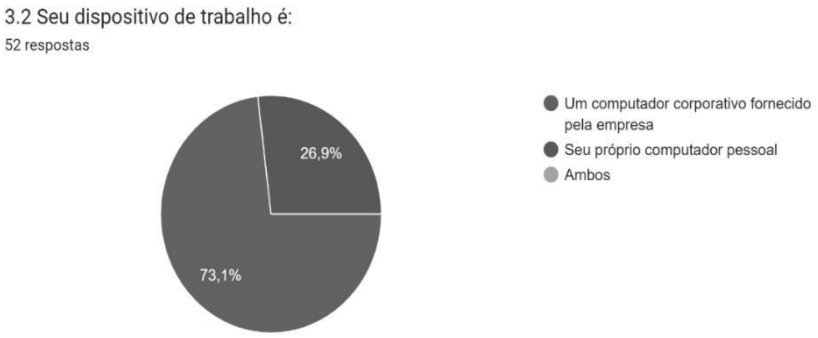
Figura 8 - Utilização de VPN



Fonte: Elaborado pelos autores

A Figura 9 destaca que 73,1% dos colaboradores utilizam computadores corporativos para o *home office*, enquanto 26,9% utilizam seus dispositivos pessoais.

Figura 9 - Dispositivo de trabalho

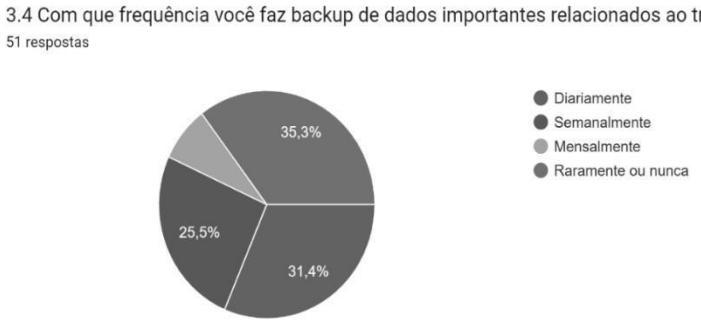


Fonte: Elaborado pelos autores

A Figura 10 revela que 31,4% dos entrevistados realizam *backups* diariamente, 25,5% realizam semanalmente, 7,8% realizam mensalmente e a maioria 35,3% realizam raramente ou

nunca, indicando uma falha importante, já que a falta de uma rotina de *backups* pode representar um risco significativo para a integridade dos dados.

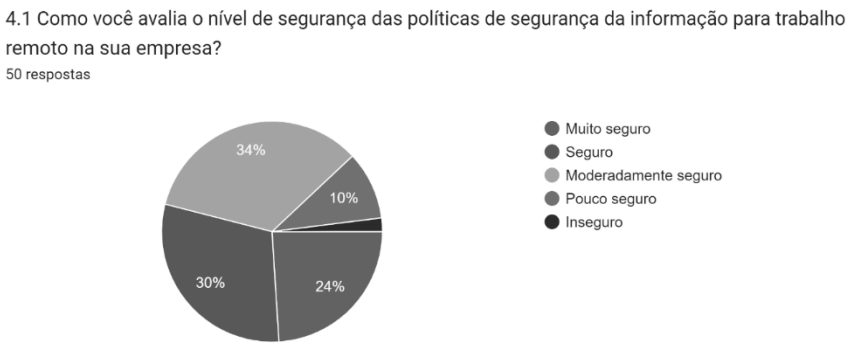
Figura 10 - Ferramentas de segurança



Fonte: Elaborado pelos autores

A Figura 11 mostra que 24% dos colaboradores consideram as políticas de segurança da informação como muito seguras, 30% as avaliam como seguras, 34% as classificam como moderadamente seguras, 10% as consideram pouco seguras e 2% avaliam como inseguras.

Figura 11 - Nível de segurança das políticas de segurança da informação

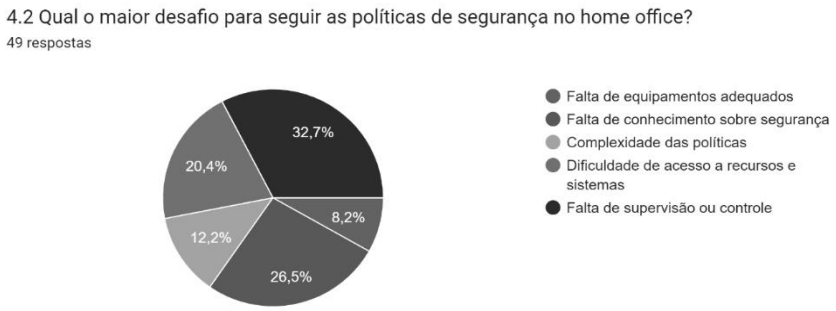


Fonte: Elaborado pelo autor

A Figura 12 evidencia os principais desafios enfrentados pelos colaboradores em relação às políticas de segurança no trabalho remoto: a falta de supervisão ou controle (32,7%), a falta de conhecimento sobre segurança (26,5%) e a dificuldade de acesso a recursos e sistemas (20,4%). Outros desafios incluem complexidade das políticas (12,2%) e a falta de equipamentos

adequados (8,2%). Esses dados indicam a necessidade urgente de aprimorar os recursos disponíveis, oferecer treinamentos mais eficazes, simplificar as políticas e garantir um acompanhamento mais próximo dos colaboradores.

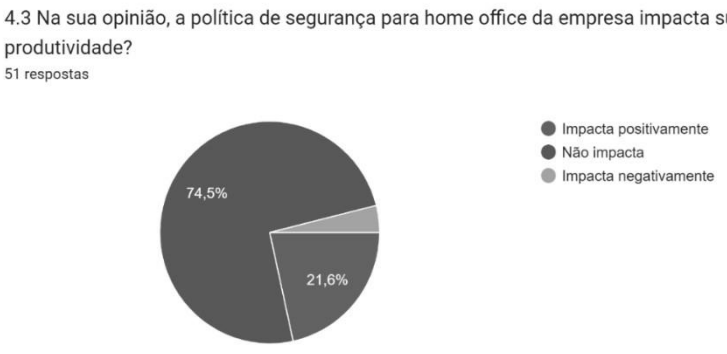
Figura 12 - Desafios para seguir as políticas de segurança



Fonte: Elaborado pelo autor

A Figura 13 destaca que 74,5% dos colaboradores acreditam que as políticas de segurança da informação não afetam a produtividade no trabalho remoto, enquanto 21,6% percebem um impacto positivo e 3,9% percebem um impacto negativo. Esses resultados indicam que as políticas são vistas como benéficas tanto para a segurança quanto para o desempenho.

Figura 13 - Impacto na produtividade



Fonte: Elaborado pelos autores

5. Considerações Finais

A crescente adoção do *home office* tem impulsionado a necessidade de repensar as estratégias de segurança da informação nas organizações. A literatura revela que os principais desafios nesse cenário incluem a fragmentação das redes, com o uso de conexões domésticas menos seguras, o que aumenta a vulnerabilidade a ataques cibernéticos. Além disso, o uso de dispositivos pessoais para acessar dados corporativos sem as devidas proteções, a dificuldade em monitorar a atividade dos colaboradores em ambientes remotos e a falta de conscientização sobre as melhores práticas de segurança podem resultar em erros que comprometem a integridade da informação.

Embora o trabalho remoto traga desafios, ele também impulsiona a inovação em soluções de segurança da informação. A necessidade de proteger dados em ambientes descentralizados fomenta o desenvolvimento de novas tecnologias, como VPNs, autenticação multifatorial e ferramentas de segurança em nuvem. A colaboração segura em ambientes remotos exige a adoção de ferramentas mais eficientes e seguras, o que pode fortalecer a cultura de segurança da informação nas organizações. Isso é impulsionado pela implementação de políticas robustas e programas de treinamentos regulares para os colaboradores.

Para garantir a segurança da informação em ambientes de trabalho remoto, é essencial adotar soluções robustas, como VPNs, autenticação multifatorial e criptografia de dados. Além disso, promover a conscientização contínua por meio de treinamentos regulares sobre as melhores práticas de segurança é fundamental. O monitoramento constante das ameaças, bem como a revisão periódica das políticas de segurança também são cruciais. Ao cultivar uma cultura de segurança, onde todos se sintam responsáveis pela proteção dos dados, as empresas podem reduzir significativamente os riscos associados ao trabalho remoto e proteger seus ativos mais valiosos.

Para avançar nas pesquisas nessa área, sugere-se uma análise mais aprofundada dos dados coletados, utilizando técnicas estatísticas para identificar correlações e padrões significativos. Seria relevante comparar os resultados com estudos semelhantes realizados em outras organizações, a fim de identificar melhores práticas e tendências. O desenvolvimento de um modelo para avaliar a maturidade em segurança da informação das empresas que adotam o

trabalho remoto poderia enriquecer o conhecimento sobre o tema. Além disso, investigar o impacto da pandemia de COVID-19 nas políticas de segurança da informação poderia revelar novos desafios e perspectivas a serem enfrentados.

Em conclusão, a segurança da informação em ambientes de *home office* exige uma abordagem integrada que envolva tecnologia, políticas e conscientização dos colaboradores. As empresas devem investir em soluções de segurança robustas e adaptar suas políticas ao novo contexto de trabalho remoto. A conscientização contínua dos colaboradores é essencial para o sucesso das estratégias de segurança implementadas. Além disso, a adoção de um Sistema de Gestão de Segurança da Informação (SGSI), alinhado a normas como a ISO/IEC 27001, pode auxiliar as organizações a garantir a conformidade e a eficácia de suas políticas, fornecendo uma estrutura sólida para a proteção dos dados corporativos.

Referências

BERWALDT, R. M. Home office: desafios em tempos de pandemia. 2022.Disponível em <https://rd.uffs.edu.br/handle/prefix/5896>. Acesso em: 25 ago. 2024.

BRANDÃO, J. L. A.; PERUCCHI, V.; FREIRE, G. H. de A. Inovação, trabalho remoto e bibliotecas educativas públicas: caminhos para a transformação digital no mundo do trabalho pós-pandemia. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 21, p. e023001, 2023. Disponível em <https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8670044>. Acesso em: 25 ago. 2024.

CHAGAS, A. P. M. A. Gestão de segurança dos sistemas de informação eletrônica: interface usuário, tecnologia e sistema. 2023. Disponível em <https://ri.ufs.br/jspui/handle/riufs/18741>. Acesso em: 24 ago. 2024.

COELHO, L. G.; OLIVEIRA, W. A.; SILVA, A. G. F.; BARRETO, L. K. S.; PEREIRA, T. M. F. Percepções sobre o trabalho remoto durante o período pandêmico: um estudo de caso no Instituto Federal do Ceará. **Revista Brasileira de Planejamento e Desenvolvimento**. Curitiba, v. 11, n. 02, p. 476-492, mai./ago. 2022. Disponível em: <https://periodicos.utfpr.edu.br/rbpd/article/view/14554/8855>. Acesso em: 24 ago. 2024.

COSTA, G. G. da S. Percepções dos funcionários sobre treinamento e desenvolvimento em um ambiente de home office: um estudo de caso em uma empresa de telemarketing. 2024. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Norte. Disponível em <https://repositorio.ufrn.br/handle/123456789/58836>. Acesso em: 25 ago. 2024.

COSTA, T. S. Estratégias de segurança da informação diante das mudanças causadas pela pandemia, 2022. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas) - Faculdade de Tecnologia de São Paulo, São Paulo, 2022.Disponível em <http://ric.cps.sp.gov.br/handle/123456789/10548>. Acesso em: 24 ago. 2024.

LOPES, M. A. D. e S.; CASTRO, J. L. de. Vivências e contribuições de estágio de saúde coletiva em tempos de pandemia: um relato de experiência. **Revista Extensão & Sociedade**, [S. l.], v. 14, n. 2, 2022. DOI: 10.21680/2178-6054.2022v14n2ID28665. Disponível em <https://periodicos.ufrn.br/extensaoesociedade/article/view/28665>. Acesso em: 24 ago. 2024.

FANSTONE, P. dos R. P.; CARVALHO, B. D. L.; TRISTÃO, M. C. Aplicação das técnicas de Lean Inception e MVP no processo de uma Fábrica de Software Acadêmica. 2021. Trabalho de Conclusão de Curso (Engenharia de Software). Disponível em <http://repositorio.aee.edu.br/jspui/handle/aee/19664>. Acesso em: 31 ago. 2024.

FERRO, P. R. Normas trabalhistas no período da pandemia O abuso de contratos intermitentes. 2024. Disponível em <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7460>. Acesso em: 31 ago. 2024.

FRANCISCO, D. M. M.; MPANDA, V. J. S. Processo de recrutamento em home office para o trabalho remoto. **NJINGA e SEPÉ: Revista Internacional de Culturas, Línguas Africanas e Brasileiras**, v. 3, n. 2, p. 476-490, 2023. Disponível em <https://revistas.unilab.edu.br/index.php/njingaesape/article/view/1089>. Acesso em: 31 ago. 2024.

JOTA, J. D. do N. Home office: a vulnerabilidade dos trabalhadores em relação às doenças psicossociais associadas ao trabalho remoto. 2023. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Norte. Disponível em <https://repositorio.ufrn.br/handle/123456789/56791>. Acesso em: 25 ago. 2024.

KLEINJOHANN, D. S. A importância da segurança de dados e informação na função do secretário executivo: breve balanço. 2021. Disponível em <https://repositorio.ufsc.br/handle/123456789/224030>. Acesso em: 31 ago. 2024.

MENDES, J. de A. Uma abordagem sobre a segurança da informação no mundo atual. 2022. Disponível em <https://bdm.ufpa.br/jspui/handle/prefix/4401>. Acesso em: 24 ago. 2024.

MORO, E. M.; SOARES. I. N.; SANTOS. K. S. S.; SILVA, L. A.; OLIVEIRA, M. E. D.; ARAÚJO, V. A. M. de. A exclusão de colaboradores na política de bem-estar do trabalho remoto. Trabalho de conclusão de curso (Curso Técnico em Administração) - Escola Técnica Estadual ETEC de Sapopemba (Fazenda da Juta - São Paulo), São Paulo, 2023. Disponível em <https://ric.cps.sp.gov.br/handle/123456789/16900>. Acesso em: 31 ago. 2024.

NASCIMENTO, A. S. do; SILVA, C. I. M. da; LANDIM, F. F. P.; NOGUEIRA, J. dos S.; COSTA, M. G. C. De O.; CONCEIÇÃO, P. S. da; SANTOS, Y. dos. Qualidade de vida no

trabalho: modalidade home office, 2023. Trabalho de conclusão de curso (Curso Técnico em Recursos Humanos) - Escola Técnica Estadual ETEC de Sapopemba (Fazenda da Juta - São Paulo), São Paulo, 2023. Disponível em <https://ric.cps.sp.gov.br/handle/123456789/14785>. Acesso em: 31 ago. 2024.

NEVES, L. M.; PEREIRA, N. de L. B.; SILVA, M. V. da. Ransomware e phishing durante a pandemia covid-19 (Coronavírus). **FatecSeg-Congresso de Segurança da Informação**. 2021. Disponível em <https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/39>. Acesso em: 25 ago. 2024.

OLIVEIRA, G. P. S.; ARMOND, L. F. M. Home office em tempo de pandemia: saúde mental do trabalhador. 2022. 32 f. Trabalho de Conclusão de Curso (Graduação em Fisioterapia) - Universidade Federal de Uberlândia, Uberlândia, 2023. Disponível em <https://repositorio.ufu.br/handle/123456789/37001>. Acesso em: 25 ago. 2024.

OLIVEIRA, V. R. de Home Office e os Ambientes Comunicacionais: Tensões entre a Comunicação Presencial e Não-Presencial no Mundo do Trabalho. **Associação Brasileira de Pesquisadores de Comunicação Organizacional e de Relações Públicas**. São Paulo/SP, 2021. Disponível em <https://portal.abrapcorp2.org.br/wp-content/uploads/2021/07/sff-115.pdf>. Acesso em: 25 ago. 2024.

PEREIRA, N. de L. B.; NEVES, L. M. Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus). **Revista Tecnológica da Fatec Americana**, v. 9, n. 01, p. 68-83, 2021. Disponível em <https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/256>. Acesso em: 25 ago. 2024.

ROCKENBACH, R. Viabilidade de implementação de Política de Segurança da Informação em Micro e Pequenas Empresas. 2021. Disponível em <https://repositorio.ufsc.br/handle/123456789/229554>. Acesso em: 31 ago. 2024.

RODRIGUES, C. L.; ARAÚJO, V. S.; TORQUATO, L. J. F. Trabalho remoto na perspectiva do objetivo de desenvolvimento sustentáv4l Nº 8 da ONU. **UnBRevista de Direito da Universidade de Brasília**, v. 7, n. 2, p. 75-97, 2023. Disponível em <https://periodicos.unb.br/index.php/revistadedireitounb/article/view/47458>. Acesso em: 31 ago. 2024.

RODRIGUES, T. dos S. Influência do trabalho remoto no intraempreendedorismo em startups de tecnologia. 2022. Disponível em <http://repositorio.ufc.br/handle/riufc/77556>. Acesso em: 24 ago. 2024.

SANTOS, S. Q. S. As consequências da lei geral de proteção de dados (LGPD) na relação de trabalho home office. 2021. Disponível em <http://repositorio.anhanguera.edu.br:8080/jspui/handle/123456789/482>. Acesso em: 25 ago. 2024.

SILVA, F. A. da. Avaliação do departamento de recursos humanos de uma empresa de tecnologia da cidade de Piracicaba/SP em relação à segurança da informação com base em alguns controles da NBR ISO/IEC 27001/2013. 2023. Disponível em <https://ric.cps.sp.gov.br/handle/123456789/14662>. Acesso em: 24 ago. 2024.

SILVA, L. G.; SOUZA, R. B. de. A gestão de documentos e tramitação de processos na administração pública, com a utilização do Sistema Eletrônico de Informações– SEI: um estudo de caso na Universidade Federal de Viçosa. **Múltiplos Olhares em Ciência da Informação**, v. 10, 2020. Disponível em <https://periodicos.ufmg.br/index.php/moci/article/view/25838>. Acesso em: 31 ago. 2024.

SOUZA, J. A. de; COSTA, P. V. O modelo de trabalho híbrido para melhoria da qualidade de vida do colaborador. 2024. Disponível em <https://ric.cps.sp.gov.br/handle/123456789/21494>. Acesso em: 31 ago. 2024.

STAUBITZ, M. G. O impacto do home office nas relações trabalhistas e o futuro do trabalho: uma visão organizacional sobre os impactos da crescente modalidade de trabalho remoto. FGV Revista de Iniciação Científica, 2021. Disponível em <https://periodicos.fgv.br/ric/article/view/86072/81099>. Acesso em: 31 ago. 2024.

WARZEL, C.; PETERSEN, A. H. Trabalho remoto: As vantagens e desvantagens do home office. Best Business, 2022.