ANÁLISE SOBRE A POLÍTICA DE SEGURANÇA NO TRABALHO EM REGIME HOME OFFICE OU SEMIPRESENCIAL

ANALYSIS OF THE SAFETY POLICY AT WORK IN HOME OFFICE OR SEMI-PRESENTIAL REGIME

ARTHUR MABUTI PEREIRA
FATEC - FACULDADE DE TECNOLOGIA DE BRAGANÇA PAULISTA

DERCIA ANTUNES DE SOUZA
FATEC FACULDADE DE TECNOLOGIA

CARLOS AUGUSTO GOMES
FATEC - FACULDADE DE TECNOLOGIA DE BRAGANÇA PAULISTA

DANIO LUPPI MARINHO
FATEC - FACULDADE DE TECNOLOGIA DE BRAGANÇA PAULISTA

ANÁLISE SOBRE A POLÍTICA DE SEGURANÇA NO TRABALHO EM REGIME HOME OFFICE OU SEMIPRESENCIAL

Objetivo do estudo
Analisar a segurança da informação no ambiente home office, identificar os problemas enfrentados pelas organizações nesse cenário e verificar as medidas preventivas adotadas pelas empresas.

Relevância/originalidade
A importância desse estudo está relacionada ao aumento dos ataques virtuais às organizações devido ao trabalho remoto. Será possível avaliar as estratégias de prevenção adotadas pelas empresas e os riscos reais que podem ocorrer no espaço do home office.

Metodologia/abordagem
Trata-se de uma pesquisa exploratória e descritiva. Realizou-se pesquisa bibliográfica em livros, artigos e sites. Aplicou-se questionário para trabalhadores em regime home office ou semipresencial, a fim de obter informações sobre os riscos enfrentados e a segurança da informação.

Principais resultados
A empresas estão vulneráveis a ataques cibernéticos por causa de más práticas no ambiente de trabalho, instalação de programas sem restrições, utilização de dispositivos USB em computadores corporativos, falta de promoção de reuniões sobre prevenção da exposição de informações corporativas, etc.

Contribuições teóricas/metodológicas
Verificou-se as estratégias de prevenção adotadas nas empresas e os riscos reais que ocorrem no espaço do home office A segurança da informação visa proteger as informações de valor para uma organização, incluindo dados internos, sistemas e o ambiente externo à empresa.

Contribuições sociais/para a gestão
A segurança da informação se tornou prioridade estratégica para as empresas, por isso é necessário investir em recursos tecnológicos adequados, implementar políticas de segurança abrangentes e promover a conscientização dos funcionários sobre boas práticas de segurança.

Palavras-chave: Política de Segurança , Segurança da informação, Tecnologia, Semipresencial, Home office

ANALYSIS OF THE SAFETY POLICY AT WORK IN HOME OFFICE OR SEMI-PRESENTIAL REGIME

Study purpose
Analyze information security in the home office environment, identify the problems faced by organizations in this scenario and verify the preventive measures adopted by companies.

Relevance / originality
The importance of this study is related to the increase in virtual attacks on organizations due to remote work It will be possible to assess the prevention strategies adopted by companies and the real risks that may occur in the home office.

Methodology / approach
This is an exploratory and descriptive research. Bibliographical research was carried out in books, articles and websites. A questionnaire was applied to home office or blended workers in order to obtain information about the risks faced and information security.

Main results
Companies are vulnerable to cyber attacks because of bad practices in the work environment, installation of unrestricted programs, use of USB devices on corporate computers, lack of promotion of meetings on preventing exposure of corporate information, etc.

Theoretical / methodological contributions
The prevention strategies adopted in companies and the real risks that occur in the home office space were verified. Information security aims to protect valuable information for an organization, including internal data, systems and the external environment of the company.

Social / management contributions
Information security has become a strategic priority for companies, so it is necessary to invest in adequate technological resources, implement comprehensive security policies and promote employee awareness of good security practices.

Keywords: Security Policy , Information Security, Technology , Blended classes, Home office

ANÁLISE SOBRE A POLÍTICA DE SEGURANÇA NO TRABALHO EM REGIME *HOME OFFICE* OU SEMIPRESENCIAL

1. Introdução

Com o avanço tecnológico e o aumento do trabalho em *home office*, a segurança da informação tornou-se crucial para as organizações. Durante a pandemia, muitos colaboradores passaram a trabalhar em casa, utilizando dispositivos como computadores e celulares para realizar suas atividades profissionais remotamente. A segurança da informação visa proteger os dados e garantir a integridade das informações, tanto internamente quanto em relação ao ambiente externo. É fundamental proteger essas informações contra acesso não autorizado, a fim de evitar danos à empresa e a terceiros (ORGANIZAÇÃO INTERNACIONAL DO TRABALHO, 2021).

O *home office* está se tornando cada vez mais comum nas empresas, e é importante que esse processo ocorra de maneira segura, considerando a segurança da informação como parte essencial dos negócios. O trabalho remoto está sendo implementado de forma híbrida, e pesquisas estão sendo realizadas para garantir a segurança nesse contexto, especialmente após a pandemia da Covid-19.

Este trabalho tem como objetivo analisar a segurança da informação no *ambiente home office*, identificar os problemas enfrentados pelas organizações nesse cenário e verificar as medidas preventivas adotadas pelas empresas. Este trabalho tem relevância visto que na atualidade já é conhecido diversos ataques ocorridos às organizações de forma virtual. Por conta da nova forma de trabalho, o número de ataques tem aumentado amplamente nos últimos tempos. Assim, será possível verificar a forma com que as empresas se previnem e os reais riscos que podem ocorrer no espaço *Home Office.*

A metodologia deste estudo é exploratória e descritiva. Foram levantados conteúdos relevantes sobre o tema, a fim de obter uma compreensão mais aprofundada. Foi aplicado um questionário para pessoas que trabalham em regime *home office* ou semipresencial, a fim de obter informações sobre os riscos enfrentados e a forma como a segurança da informação é abordada nesse ambiente.

2. Referencial teórico

2.1 Segurança da informação

Segundo Fontes (2006), a segurança da informação é um agrupamento regras e procedimentos que visam manter as informações de uma empresa protegidas e a permita alcançar suas metas e projetos. É o ato de proteger dados sensíveis da organização contra ameaças vindas do exterior como: *spywares*, *ransomware*, vírus e invasões; ou até do ambiente físico / interno da empresa, contra inundações ou incêndios por exemplo.

A COBIT *Security Baseline* (IT Governance *Institute*, 2007) destaca a importância de proteger as informações contra ameaças que podem resultar em perda, inacessibilidade, alteração ou divulgação indevida. Essas ameaças incluem erros, fraudes, acidentes e danos intencionais. Nesse sentido, são adotados princípios fundamentais da Segurança da Informação (PSI), como confidencialidade, integridade e disponibilidade, para evitar tais contratempos.

Com base nas ideias de Hintzbergen et al. (2018), a confidencialidade envolve restrições de acesso a arquivos empresariais, permitindo apenas indivíduos autorizados. A integridade é essencial para manter as informações intactas e legítimas. Já a disponibilidade diz respeito à capacidade da empresa em fornecer acesso seguro e fluido aos recursos conforme as necessidades dos usuários autorizados.

Para que a empresa tenha êxito no ambiente organizacional, seus colaboradores têm vital importância para manter o funcionamento da empresa. Como enfatizado por Fontes (2006), o colaborador dentro da organização tem fundamental importância com a empresa para

manter a segurança dos dados e seguir regras e normas existentes para que seja cumprida sua função.

Ainda para este mesmo autor, os regulamentos (políticas, normas e regras) de segurança da informação têm como objetivo fazer com que o uso da informação da organização aconteça de uma forma estruturada, possibilitando que o negócio não seja prejudicado por um mau uso da informação: seja por erro ou acidente.

2.2 Tipos de vulnerabilidades

Conforme Jerussalmy (2020), as vulnerabilidades são falhas, defeitos ou fraquezas que podem ser exploradas para violar a política de segurança. Ele ressalta que as medidas de proteção em ambientes de rede doméstica e o uso de computadores pessoais tornam as informações das organizações mais vulneráveis por diversos motivos, como a falta de bloqueio do dispositivo utilizado e a falta de criptografia dos dados.

Diante deste contexto, Rodrigues Jr. et al. (2020) afirma que empresas de diversos setores ao redor do mundo estão adotando o trabalho remoto como estratégia, mas é crucial garantir a segurança dessa modalidade do ponto de vista empresarial. Os autores destacam que muitas empresas estão enfrentando seus primeiros desafios nesse cenário, com modelos variados de implementação do *home office*.

A respeito dos mesmos autores, mencionam que os dados mostram a falta de experiência das empresas na criação de políticas de segurança digital para o trabalho remoto. Além disso, é importante utilizar diferentes credenciais e laptops separados para garantir a segurança das informações da organização e a divisão entre o trabalho e aspectos pessoais. Isso ajudará a prevenir invasões e vulnerabilidades em um ambiente de trabalho híbrido.

Segundo Favero e Favero (2021 apud Rodrigues (2022), os dados dos clientes são valiosos para as empresas e são protegidos com segurança. No entanto, criminosos digitais estão cada vez mais cientes do valor desses dados, resultando em vazamentos de dados, um dos cibercrimes mais prejudiciais atualmente. Desse modo, várias medidas vêm sendo tomadas, dentre elas, é a utilização de VPN (Virtual Private Network) pela qual é fundamental para as operações da empresa neste novo cenário. O fato de impactar e influenciar em questões relacionadas com a segurança e disponibilidade segura das informações (RODRIGUES JR. et al., 2020).

Segundo o *site* Owasp (2022), as vulnerabilidades estão citadas e descritas a seguir:

- Falhas Criptográficas: Pode expor dados confidenciais como senha, registros comerciais, informações de cartão de crédito, endereços de e-mail, registros de saúde ou outros dados pessoais do usuário. Para evitar isso, todos os dados devem ser armazenados com os algoritmos de *hashing* recomendados.
- Controle de acesso quebrado: Durante o desenvolvimento do aplicativo são aplicados controles de acesso que proíbem os usuários de recuperar as informações de sua permissão concedida. A falha no desempenho eficiente pode levar à divulgação não autorizada de informações, destruição de dados modificação, dentre outros.
- Configuração incorreta de segurança: Controles de segurança configurados de forma imprecisa ou insegura podem causar problemas de segurança, vulnerabilidade de configuração incorreta e colocando o sistema em risco. Recursos desnecessários instalados, software desatualizado etc. também podem causar problemas de segurança.
- Falhas de Identificação e Autenticação: Antes de acessar qualquer *site* protegido, o aplicativo deve verificar a identidade do usuário, autenticação e gerenciamento de sessão. Essas coisas são importantes para proteção contra-ataques relacionados à autenticação ou podem levar à vulnerabilidade de identificação e falhas de autenticação.

2.3 Ataques e seus objetivos

Segundo Kim e Solomon (2014 apud Rodrigues (2022), os ataques cibernéticos visam obter informações, interromper operações e causar danos às empresas. Eles podem ser classificados em ataques ativos, que modificam informações por meio de intrusão física, e ataques passivos, em que o intruso apenas observa ou intercepta a informação. Esses ataques representam uma ameaça significativa à segurança das organizações.

De acordo com Dias (2000), um ataque é um evento indesejável que pode remover, desabilitar, danificar ou destruir um recurso. O autor destaca o anonimato proporcionado pela *internet* como uma característica complicadora, dificultando a identificação dos responsáveis pelas ações executadas em rede. O advento das redes de longo alcance, especialmente a *internet*, ampliou o cenário para a ocorrência de ataques.

Segundo Mitnick (2003, p. 207), "nove entre dez grandes corporações e órgãos governamentais já foram atacados por invasores de computadores, a julgar pelos resultados de uma pesquisa realizada pelo FBI e reportada pela Associated Press em abril de 2002". A partir dessas informações, é possível compreender a importância de assegurar a preservação dos dados nas empresas, independente do contexto de trabalho físico ou *home office*.

"Evidencia-se a necessidade de investimento e planejamento na Segurança da Informação de uma organização, de forma a manter e proteger todos os seus ativos, pois organizações investem muito dinheiro em seus sistemas de software, tornando-os ativos de extrema importância para a organização" (SOMMERVILLE, 2011 apud ARAUJO, 2021, p. 11). De acordo com esta afirmação, qualquer perda de informação ou indisponibilidade dos sistemas representam um grave prejuízo para a empresa.

Segundo Valente (2022, p. 36), "os sistemas de Tecnologias da Informação (TI) devem garantir – por defeito – que nenhum comportamento indesejável é possível, e que qualquer ataque informático é devidamente mitigado", entretanto, mesmo nas empresas mais robustas, em questão de segurança, é possível extinguir todas as vulnerabilidades. Algumas das táticas mais comuns utilizadas em ataques cibernéticos estão citadas e descritas a seguir:

- Engenharia Social: É um dos métodos mais utilizados para obter informações confidenciais. Utilizando-se da ingenuidade ou confiança de um colaborador da empresa, o criminoso manipula o usuário para que ele forneça informações sensíveis como logins, senhas e outros dados, utilizando da interação humana e manipulação psicológica.
- *Ransomware*: Esse ataque consiste na obstrução de funções do computador ou criptografia de arquivos da máquina, impossibilitando sua utilização ou acesso. Tal feito tem como objetivo extorquir a vítima para a liberação dos dados e funções, configurando-se como um sequestro de dados.
- Ataque DDoS: Ataques de negação de serviço distribuído sobrecarrega a capacidade de rede ou infraestrutura de uma companhia para impossibilitar a função dos seus serviços, realizando o envio de múltiplas solicitações através de várias estações infectadas com *softwares* maliciosos controlados pelo infrator.
- *Phishing*: Nesse método, infratores utilizam *e-mails* e redes sociais para enviar mensagens com pretextos para usuários abrirem links anexos. Estes o redirecionam para *sit*es maliciosos semelhantes a legítimos. Dessa forma, o usuário é induzido a inserir suas informações pessoais como logins, senhas, números de cartão, dentre outros, que são, então, redirecionadas aos criminosos.

2.4 Home office

De acordo com Morgenstern e Santos (2016), o termo *Home Office* é sinônimo de outras expressões, como teletrabalho, trabalho em domicílio, escritório em casa, trabalho à distância,

entre outros. Isso se refere a um contexto laboral em que o colaborador realiza suas tarefas remotamente, fora do local físico da empresa, mantendo um vínculo empregatício formal com a organização.

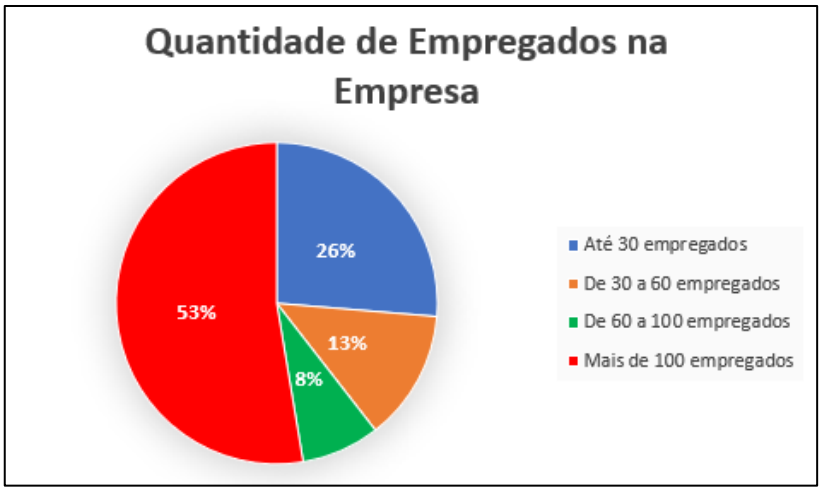
As transformações sociais, econômicas e tecnológicas trazidas pela globalização têm impactado significativamente o contexto de trabalho. A flexibilização da produção, a terceirização, o *just-in-time* e outras mudanças valorizam um modelo de trajetória profissional individualizada e do capital humano. Além disso, a abertura de mercados em países em desenvolvimento e o aumento do trabalho em *home office* impulsionam novas formas de trabalhar, que se tornam uma realidade no fenômeno trabalhista contemporâneo (RAFALSKI & ANDRADE, 2015).

O regime *home office* se tornou predominante em vários setores, como educação, empresas, comércio, clínicas, entre outros, nos últimos três anos devido à pandemia de Covid-19 e a necessidade de isolamento social. Marchand (2004 apud Mussiat 2021), explica que um dos principais desafios foi se adaptar rapidamente a um novo estilo de vida e ao trabalho remoto. Como resultado da urgência imposta pela pandemia, as empresas tiveram pouco tempo para implementar medidas adequadas de segurança da informação.

3. Análise e discussão dos resultados

O objetivo deste trabalho é analisar a segurança da informação no ambiente *home office* de forma a identificar os problemas enfrentados pela organização neste ambiente e como as empresas se previnem dentro deste contexto. Foi aplicado um questionário com 15 perguntas para profissionais que trabalham em regime *home office* ou semipresencial. Diante dos questionários enviados, 38 pessoas responderam à pesquisa.

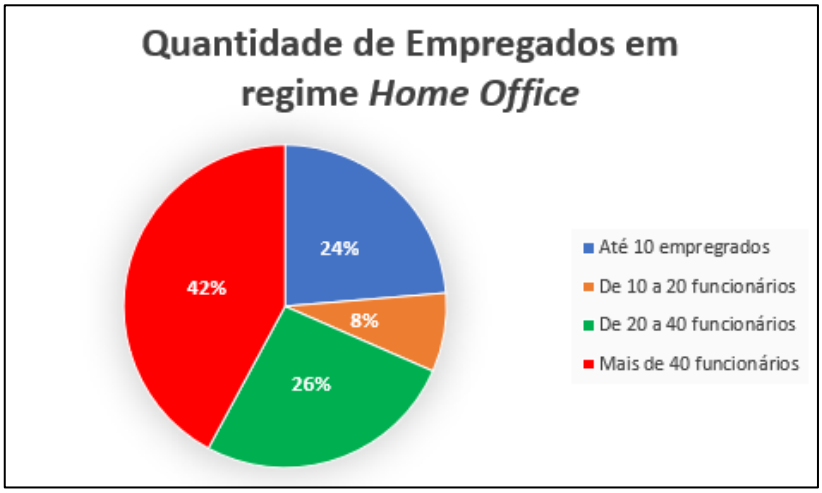
Gráfico 1 – Quantidade de empregados na empresa



Fonte: Dados da pesquisa (2023)

Em relação a quantidade de empregados nas empresas, os resultados indicam que a metade dos respondentes (20 pessoas) estão empregados em empresas com mais de 100 funcionários. Os outros 18 respondentes estão distribuídos em (até 30 funcionários, de 30 a 60 funcionários e de 60 a 100 funcionários).

Gráfico 2 – Quantidade de empregados em regime *Home Office*

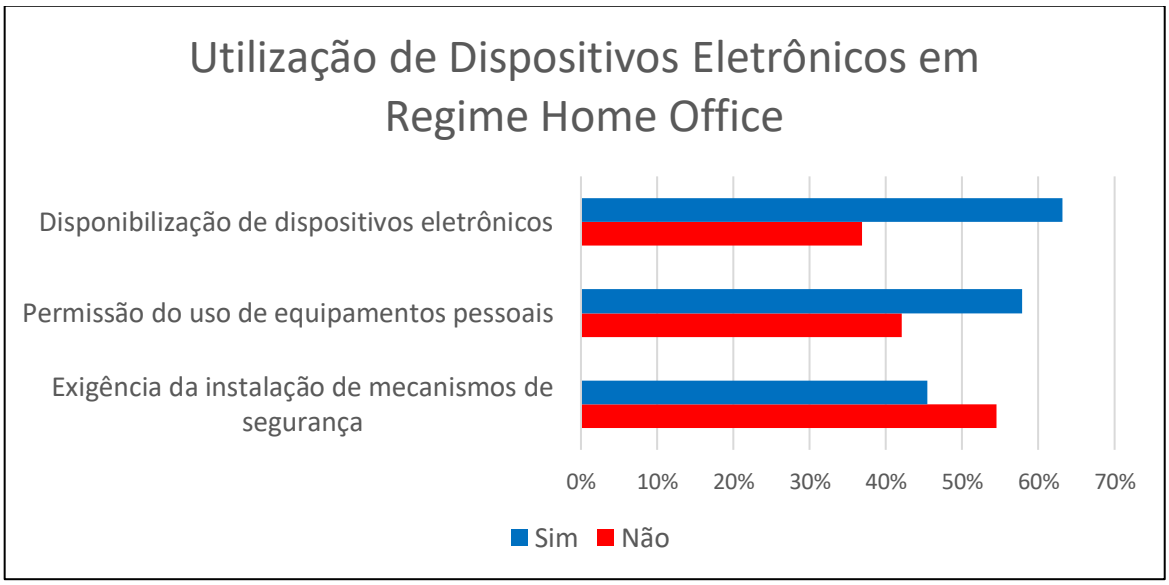


Fonte: Dados da pesquisa (2023)

Quando questionados acerca da quantidade de empregados que trabalham no regime de trabalho remoto (*home office*) / semipresencial dentro das organizações em que os respondentes trabalham, verifica-se que a maior parte dos colaboradores dessas empresas estão exercendo suas funções longe do ambiente organizacional.

Esses resultados levam à conclusão de que um número considerável de empresas estar suscetível a ataques devido à quantidade de profissionais que trabalham fora do ambiente de trabalho convencional. De acordo com Melo (2020), a segurança digital é extremamente crucial nos tempos atuais, devido ao aumento de ataques e ameaças durante a pandemia e o trabalho remoto. Os criminosos aproveitam essa situação, ressaltando a importância de investir em segurança digital, especialmente no ambiente empresarial.

Gráfico 3 – Utilização de Dispositivos Eletrônicos em Regime Home Office



Fonte: Dados da pesquisa (2023)

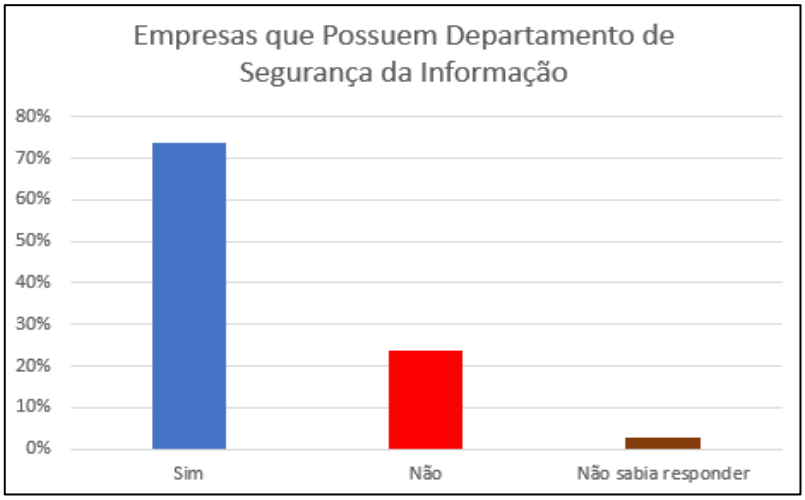
Foi perguntado para os entrevistados se a organização correspondente ao seu vínculo empregatício disponibiliza equipamentos para a exercício de suas funções laborais, como observado, 63% das respostas foram afirmativas, porém, ainda há organizações que estão suscetíveis a ataques cibernéticos pela falta da disponibilização dos equipamentos adequados.

A pandemia de Covid-19 impediu que as organizações reforçassem a segurança em dispositivos de trabalho, levando os funcionários a usar dispositivos menos seguros em casa. Isso aumenta a pressão sobre as empresas para mitigar riscos de segurança e fortalecer defesas em todos os dispositivos e aplicativos (SARGINSON, 2020). Como resultado, a adoção de dispositivos eletrônicos fornecidos pelas empresas tem aumentado devido à pressão gerada pela pandemia.

Mesmo com a alta disponibilização de recursos para mitigar os riscos de segurança para a empresa, 58% das organizações concedem permissão aos colaboradores para utilizarem seus próprios dispositivos pessoais na execução de suas atividades laborais, como demonstrado no gráfico 3. Isso abrange não somente a utilização de computadores de mesa e *laptops*, mas também o uso de dispositivos móveis para acessar *e-mails* e aplicativos de comunicação corporativa. Essa prática pode gerar brechas na segurança, tornando a organização mais vulnerável a ataques e outras ameaças, pois dispositivos pessoais, no geral, não estão em conformidade com os padrões de segurança estabelecidos pela empresa, incluindo o acesso a links questionáveis, utilização de *softwares* piratas, ausência de um antivírus e uso de sistemas operacionais desatualizados.

Em relação a pergunta “Caso a empresa permita utilizar seus equipamentos pessoais, ela exige a instalação que algum mecanismo de segurança?” para minimizar qualquer chance de risco, verifica-se que isso não ocorre, pois 55% dos entrevistados negaram a solicitação de instalar tais mecanismos. A partir disso, conclui-se que a maior parte das empresas que permitem a utilização de recursos pessoais não exigem um regulamento próprio de segurança.

Gráfico 4 – Empresas que possuem departamento de segurança da informação



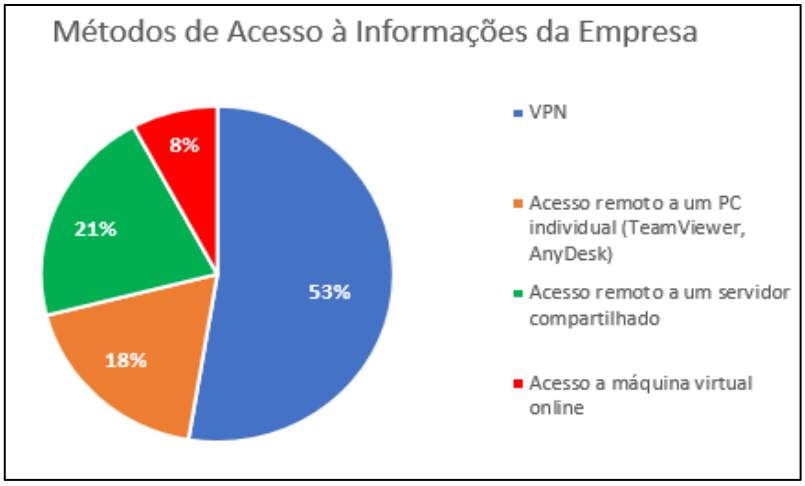
Fonte: Dados da pesquisa (2023)

Foi questionado para os entrevistados se existe nas empresas em que trabalham, um setor de Tecnologia da Informação específico para tratar assuntos de segurança da informação, e foram obtidas respostas afirmativas por 74% dos entrevistados. Assim sendo, é notável que a maioria das empresas se encontra de fato preocupadas com as questões de segurança e está empenhada em combater as vulnerabilidades geradas pelo trabalho remoto.

Rodrigues Jr. et al. (2020) aponta que a existência de um departamento de TI é vital para o funcionamento adequado da empresa e a manutenção de seus sistemas. O setor de Segurança da Informação desempenha um papel crucial, contando com uma equipe especializada capaz de identificar e corrigir vulnerabilidades de forma rápida e eficiente, garantindo prazos adequados para a solução dos problemas.

As medidas de segurança que uma empresa pode propor para seus colaboradores não se limitam apenas a disponibilizar equipamentos e impedir acesso a *site*s maliciosos, mas, também, é necessário que haja um método para que seus funcionários acessem suas redes e seus dados de forma segura e que haja rastreabilidade do que foi realizado. Isto se dá pelo fato que outro indivíduo ou até mesmo o próprio colaborador possa agir contra a empresa e extrair ou excluir dados importantes sem que eles tomem conhecimento.

Gráfico 5 – Métodos de Acesso a Informações da Empresa



Fonte: Dados da pesquisa (2023)

De acordo com Melo (2020), a mudança para o *home office* resultou no acesso remoto a dispositivos e ferramentas empresariais em redes domésticas, que geralmente não possuem políticas de segurança adequadas. Diante da falta de políticas de proteção, foram feitas perguntas aos entrevistados sobre como eles acessam a infraestrutura tecnológica das empresas, o que levanta alguns pontos a serem analisados.

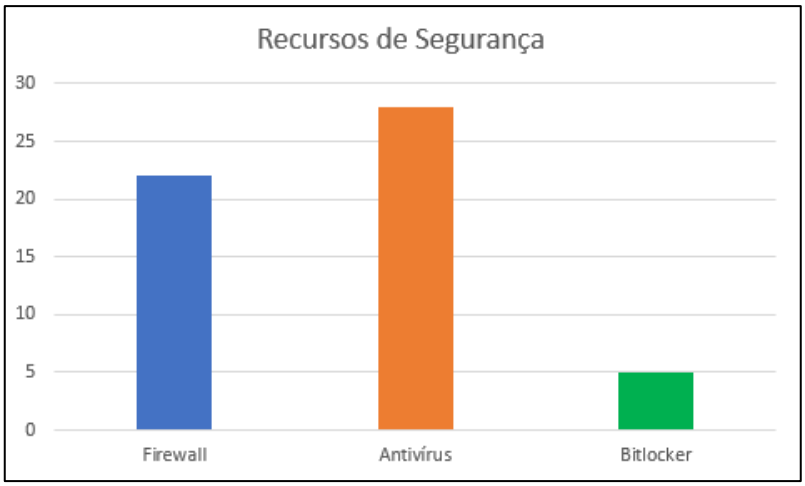
Segundo a Kaspersky (2023), a VPN e o acesso a máquina virtual são métodos seguros de acesso devido ao uso de senhas individuais e rastreabilidade. As VPNs oferecem uma conexão protegida e criptografada, ocultando a identidade do usuário e dificultando o roubo de dados. Esses métodos garantem a segurança das atividades *online* dos colaboradores, conforme mencionado na matéria, e é utilizado por 61% dos respondentes.

Segundo a N&DC (2020), o trabalho remoto traz desafios para as equipes de segurança, que enfrentam dificuldades em monitorar uma ampla gama de dispositivos e identificar ameaças avançadas. A falta de visibilidade das atividades dos usuários remotos e do tráfego de rede aumenta o risco de invasões. Além disso, a gestão de ferramentas de detecção de ameaças é mais complicada com os analistas de segurança trabalhando em casa. Essa situação facilita a ação dos *hackers*, permitindo ciberataques despercebidos.

Os acessos remotos representam um impasse, em específico, utilizando programas como *TeamViewer e AnyDesk* que qualquer pessoa com o id e senha do computador que é realizado o acesso pode entrar na máquina e realizar as alterações que desejar, sem que a empresa consiga identificar o autor do acesso.

O acesso de servidor compartilhado possui duas situações distintas. Se a empresa fornece um login e senha corporativo para cada usuário, não há problemas. No entanto, é comum utilizar o login de administrador, permitindo que qualquer pessoa com esse acesso faça alterações no servidor. Isso poderia ser evitado com o uso de logins e senhas individuais, que permitem a atribuição de permissões específicas para cada usuário no ambiente.

Gráfico 6 – Recursos de Segurança



Fonte: Dados da pesquisa (2023)

Foi perguntado para os entrevistados quais recursos de segurança mais comuns são instalados no computador pessoal ou empresarial que utilizam em sua rotina de trabalho. Dentre os respondentes, apenas 30 conseguiram identificar os recursos e informar quais eram.

As solicitações mais comuns das empresas são o antivírus (28 pessoas) e o firewall (22 pessoas), sendo o *Bitlocker* o menos utilizado (5 pessoas). O antivírus auxilia na prevenção de download de arquivos maliciosos e verificação constante do sistema. O Firewall funciona como um agente que irá verificar as permissões de recebimento e liberação ao acesso de informações do computador, assim, protegendo o funcionamento de *spywares*, por exemplo.

O *Bitlocker*, mesmo não sendo muito utilizado, tem sua importância por proteger as informações físicas registradas no computador, em específico, em seu HD. Caso o computador seja furtado, será necessário a inserção de uma senha para o acesso as informações. Caso não a possua, é impossível verificar o HD, por causa da criptografia de seus dados pela ferramenta.

Gráfico 7 – Sistema Operacional Atualizado

Fonte: Dados da pesquisa (2023)

Foi questionado para as pessoas que trabalham remotamente se o sistema operacional de suas máquinas é atualizado constantemente e podemos verificar 34 respostas afirmativas, conforme o gráfico 7.

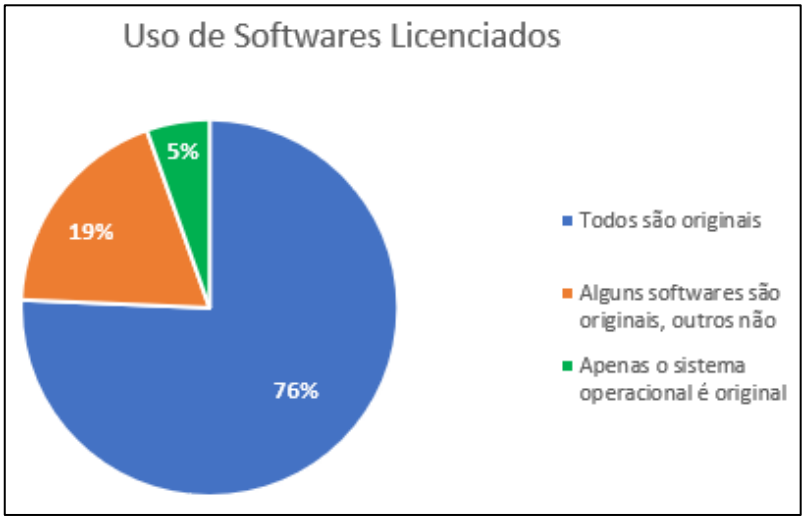
Um sistema operacional desatualizado ou descontinuado é uma porta de entrada perfeita para criminosos cibernéticos. Segundo Mota (2017) em uma reportagem da BBC, ocorreu um grande ciberataque à Equifax, empresa de gestão de crédito, resultando no vazamento de informações de 143 milhões de americanos. Os *hackers* aproveitaram uma vulnerabilidade em um software desatualizado para realizar o ataque. Esse incidente destaca a importância das atualizações de aplicativos, *softwares* e sistemas operacionais, não apenas para melhorias de usabilidade, mas também para corrigir falhas de segurança.

No geral, quando estas ferramentas são atualizadas de modo constante, bugs e outras falhas são corrigidos e os dados de seus usuários, protegidos. Porém, quando o sistema se encontra desatualizado, essas disfunções continuam lá por um período indefinido, permitindo que os criminosos utilizem essas brechas para acessar as máquinas com o software desatualizado.

Além disso, mesmo que seja tomado os devidos cuidados na configuração da máquina, os programas instalados nela também podem servir como porta de entrada para ataques. Caso seja instalado um programa pirata / crackeado, é possível que um *spyware*, ou outro software malicioso, seja instalado em conjunto e possa ameaçar a segurança dos dados.

Segundo a UFRJ (2022), *softwares* piratas são programas não pagos ou autorizados pelo fabricante, podendo comprometer a segurança e o funcionamento dos arquivos das organizações. O uso desses programas traz diversos problemas, como vulnerabilidade dos dados, exposição de informações confidenciais e risco de vírus e malware. É importante evitar o uso de *softwares* piratas para garantir a segurança das informações.

Gráfico 8 – Uso de *Softwares* Licenciados

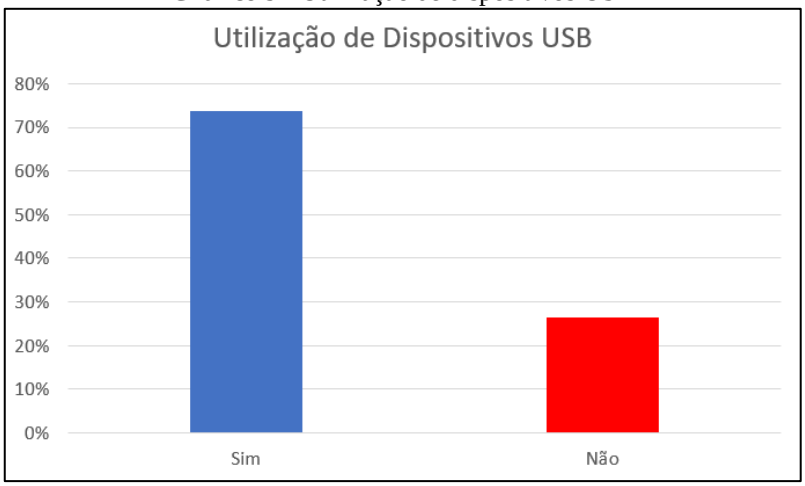


Fonte: Dados da pesquisa (2023)

Diante do exposto, foi questionado aos colabores que trabalham em regime *home office* ou semipresencial se todos os *softwares* utilizados nas máquinas laborais são devidamente licenciados ou não. E pode-se ver que a maioria, 76% dos respondentes, afirma que todos os *softwares* são originais.

Para proteger o ambiente de trabalho é recomendado evitar o uso de dispositivos removíveis, como *pendrives* e HDs externos, de acordo com Alves (2020). Essa medida é semelhante à adotada pelas empresas, pois esses dispositivos podem facilitar a entrada de infecções e ataques. Ter um antivírus com monitoramento contínuo pode ajudar a bloquear possíveis ameaças, mas evitar o uso desses dispositivos é uma medida mais apropriada para garantir a segurança (ALVES, 2020).

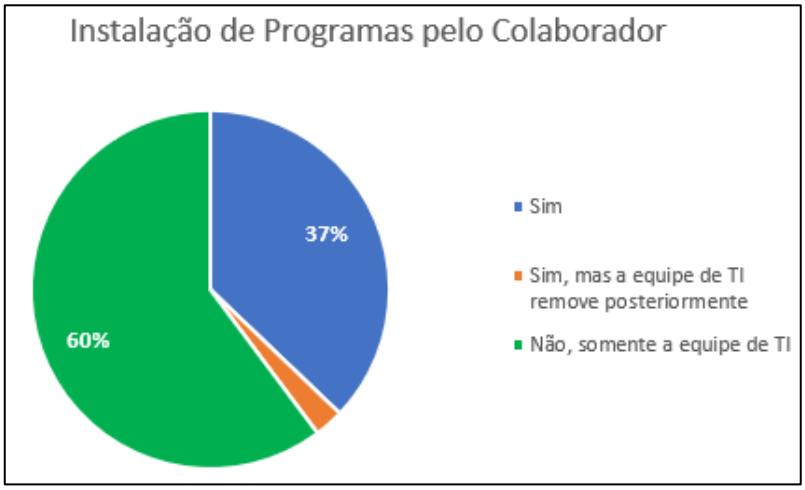
Gráfico 9 - Utilização de dispositivos USB



Fonte: Dados da pesquisa (2023)

Tendo em vista o argumento supracitado de Alves, foi questionado a respeito se há permissão do uso de dispositivos USB nas empresas dos entrevistados e foi obtido 74% de respostas afirmativas quanto a pergunta, o que é um número preocupante, visto que aumenta, de forma significativa, a chance de abertura de ataques à empresa.

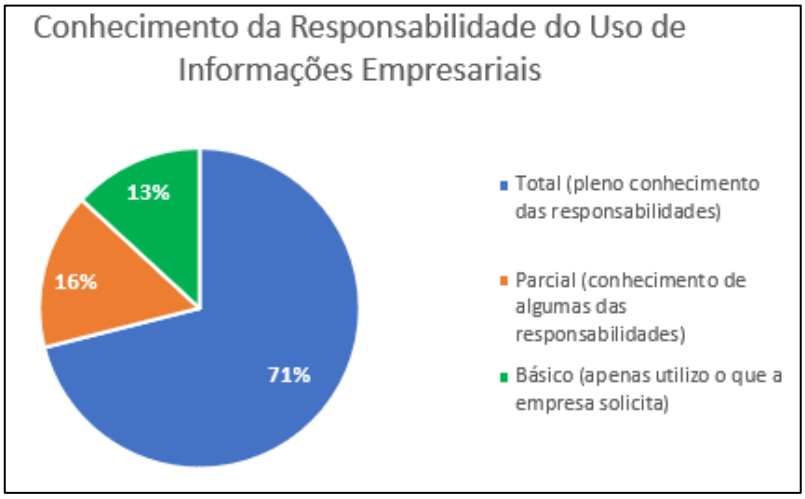
Gráfico 10 – Instalação de Programas pelo Colaborador



Fonte: Dados da pesquisa (2023)

Não é indicado permitir que os colaboradores das empresas instalem *softwares* nos computadores sem verificação da equipe de TI, dado a possibilidade de serem instalados programas com malwares, ou utilização de programas de acesso remoto e não licenciados, assim colocando em risco à organização. Levando em consideração esses dados, foi constatado 63% de respostas que os próprios colaboradores podem instalar programas diversos.

Gráfico 11 – Conhecimento da responsabilidade do uso de informações empresariais

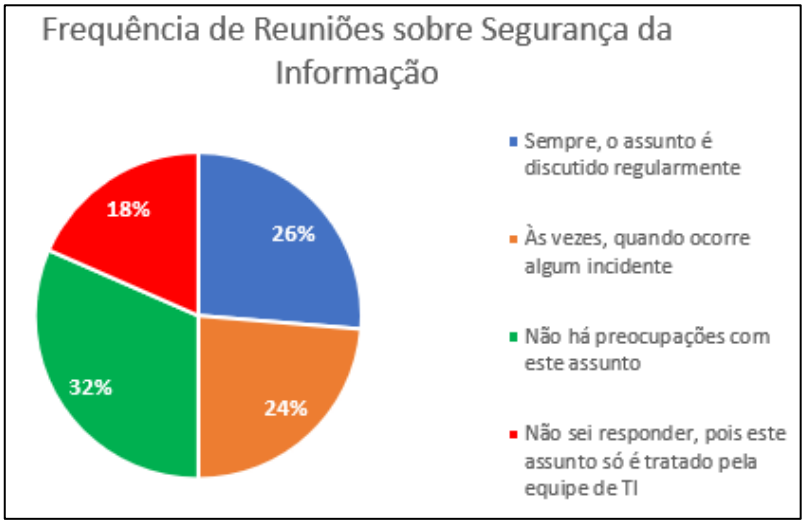


Fonte: Dados da pesquisa (2023)

Com base neste pressuposto, foi coletado dados acerca do conhecimento da responsabilidade do uso das informações empresariais e os resultados confirmam que a maioria dos indivíduos entrevistados (71% dos respondentes) possuem pleno conhecimento de suas responsabilidades para com as informações da organização.

É importante que os colaboradores tenham pleno conhecimento do uso das informações da empresa, em razão de que são os ativos mais valiosos e estratégicos da mesma, valorizando a organização. Por conseguinte, é essencial que os usuários protejam as informações contra riscos e ameaças, realizem o uso ético e legal delas e as compartilhe de forma criteriosa para pessoas autorizadas e que mantenham boas práticas de segurança conforme os seguimentos das normas empresariais.

Gráfico 12 – Frequência de reuniões sobre segurança da informação

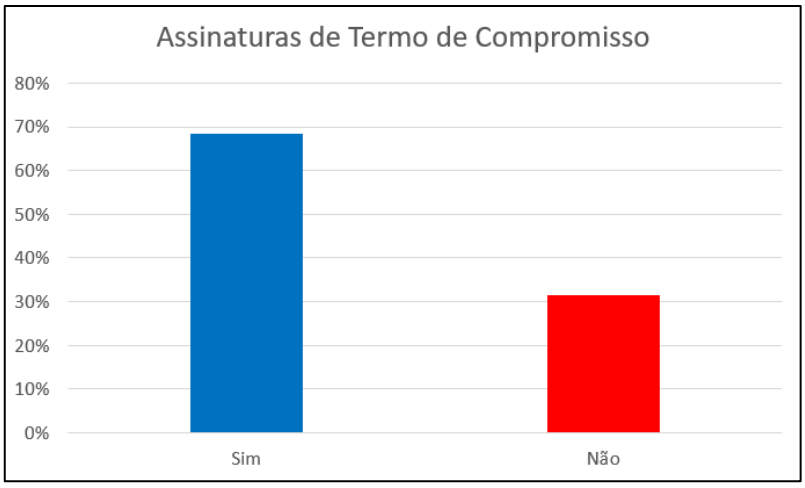


Fonte: Dados da pesquisa (2023)

De acordo com os resultados sobre "frequência de reuniões sobre segurança da informação", verifica-se um cenário preocupante por parte das empresas: (24% dos casos) tem reunião quando ocorre um incidente, (32% dos casos) não há preocupação sobre o assunto e (18% dos casos) é conversado apenas entre a TI.

Mitnick (2003) defende a importância de um programa de conscientização sobre a segurança das informações para evitar os ataques da engenharia social. Ele sugere que seja assegurado por parte da função dos funcionários e que seja desenvolvido em conjunto com o Departamento de Recursos Humanos métodos criativos e variados para comunicar as mensagens de segurança, gerando mais engajamento pelos colaboradores.

Gráfico 13 – Assinaturas de Termo de Compromisso



Fonte: Dados da pesquisa (2023)

O termo de compromisso protege as informações da empresa, estabelecendo obrigações e responsabilidades dos colaboradores. Busca prevenir violações, define sanções, boas práticas de segurança da informação e estabelece normas de segurança. No entanto, 32% dos respondentes não têm um acordo de confidencialidade, apesar de sua importância.

4. Conclusão

A análise aborda a segurança da informação no ambiente *home office*, considerando os desafios enfrentados pelas organizações nesse contexto e as medidas preventivas adotadas. Com o avanço tecnológico e a pandemia atual, o trabalho remoto se tornou mais comum, exigindo o uso da tecnologia da informação para atividades profissionais à distância. No contexto do trabalho remoto e semipresencial, a segurança da informação se tornou um desafio ainda maior. O aumento do número de profissionais trabalhando fora do ambiente de trabalho convencional tornou as empresas mais suscetíveis a ataques cibernéticos e outras ameaças.

A segurança da informação visa proteger as informações de valor para uma organização, incluindo dados internos, sistemas e o ambiente externo à empresa. É fundamental proteger essas informações contra acessos indevidos que possam causar prejuízos. Foi observado que muitas organizações não possuem recursos tecnológicos adequados para garantir a autenticidade, integridade, disponibilidade e confidencialidade dos dados. A falta de equipamentos adequados e a permissão para uso de dispositivos pessoais pelos colaboradores contribuem para a vulnerabilidade das empresas. Além disso, a ausência de regulamentos de segurança específicos para esses dispositivos aumenta os riscos.

Embora a maioria das empresas tenha um setor de Tecnologia da Informação (TI) para tratar de questões de segurança, ainda existem desafios a serem enfrentados. A rápida transição para o trabalho remoto durante a pandemia deixou algumas organizações sem tempo ou recursos para reforçar a segurança em dispositivos de trabalho, resultando em muitos funcionários usando dispositivos e redes menos seguros em casa.

A falta de políticas de segurança adequadas e a utilização de métodos de acesso remoto menos seguros aumentam a probabilidade de ataques e o acesso não autorizado aos sistemas corporativos. Para garantir uma segurança abrangente, as empresas devem adotar medidas como o uso de VPNs, acesso a máquinas virtuais, instalação de recursos de segurança (antivírus e *firewalls*) e atualização constante dos sistemas operacionais e *softwares* instalados nas máquinas. A utilização de *softwares* piratas ou desatualizados compromete a segurança dos dados.

Em resumo, a segurança da informação é uma prioridade estratégica para as empresas modernas, especialmente no contexto do trabalho remoto. É necessário investir em recursos tecnológicos adequados, implementar políticas de segurança abrangentes e promover a conscientização dos funcionários sobre boas práticas de segurança para preservar a integridade dos dados, proteger os ativos e manter a confiança dos clientes e parceiros comerciais.

Referências

ALVES, P. (2020). **Dicas para trabalhar em *home office*: saiba proteger informações importantes**. Tech Tudo. 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 junho de 2023.

ARAUJO, I. (2021). Proposta de política de segurança da informação para ambiente de trabalho *Home Office*. **Trabalho de conclusão de curso da Universidade Evangélica de Goiás**, Anápolis – GO. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/19640/1/TCC1%20NaIvan%20Final.pdf. Acesso em: 12 de abri. 2023.

COBIT SECURITY BASELINE: ***An Information Survival Kit***. (2007). 2ª Edição. IT Governance Institute. Disponível em: https://nanopdf.com/download/cobit-security-baseline_pdf. Acesso em: 17 de mai. 2023.

FONTES, E. (2006). **Segurança da informação: o usuário faz a diferença**. 1ª Edição. São Paulo: Saraiva.

DIAS, C. (2000). **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books.

HINTZBERGEN, J. et al. (2018). **Fundamentos de Segurança da Informação**: Com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Ed. BRASPORT.

JERUSSALMY, E. (2020). **Confira cuidados no *home office* com a segurança da informação**. Revista Brasil. Disponível em: https://radios.ebc.com.br/revista-brasil/2020/03/confira-cuidados-no-home-office-com-seguranca-da-informacao. Acesso em: 31 de mai. de 2023.

KASPERSKY LAB. (2023). **O que é uma VPN e como funciona?** Kaspersky. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn. Acesso em: 01 de jun. de 2023.

MELO, U. (2020). **Cibersegurança aplicada à segurança física**. Ciso Adviser. Disponível em: https://www.cisoadvisor.com.br/security-room-posts/ciberseguranca-aplicada-a-seguranca-fisica/. Acesso em: 25 mai. 2023.

MITNICK, K. D. (2003). **A Arte de Enganar: Ataques de Hackers**: Controlando o Fator Humano na Segurança da Informação. São Paulo: Ed. Pearson Education.

MORGENSTERN, E.; SANTOS, D. (2016). **A imposição do *Home Office* e suas consequências trabalhistas**. In: PONCHIROLLI, Osmar. **Memorial TCC: Caderno da Graduação**. Curitiba – PR: FAE Centro Universitário. Disponível em: https://memorialtcccadernograduacao.fae.edu/cadernotcc/issue/view/2. Acesso em: 23 mai. 2023.

MOTA, C. (2017). **Por que atualizar computador é mais importante até que antivírus para evitar ciberataques**. BBC News Brasil. Disponível em: https://www.bbc.com/portuguese/geral-42318064. Acesso em: 22 de maio de 2023.

MUSSIAT, A. (2021). **O impacto do *Home Office* nas startups de Curitiba durante a pandemia do covid-19**. In: PONCHIROLLI, Osmar. **Memorial TCC: Caderno da Graduação**. Curitiba – PR: FAE Centro Universitário. Disponível em: https://memorialtcccadernograduacao.fae.edu/cadernotcc/issue/view/8. Acesso em 23 mai. 2023.

N&DC SYSTEMS INTEGRATOR. (2020). **Segurança do acesso remoto: conheça 4 riscos e como solucioná-los**. N&DC. Disponível em: https://ndc.com.br/seguranca-do-acesso-remoto-conheca-4-riscos-e-como-soluciona-los/#:~:text=Falta%20de%20visibilidade%20da%20atividade%20do%20usu%C3%A1rio&text=Essa%20combina%C3%A7%C3%A3o%20de%20problemas%20facilita,e%2C%20consequentemente%2C%20realizarem%20ciberataques.&text=Ao%20contr%C3%A1rio%20de%20investir%20em,maximizam%20a%20integra%C3%A7%C3%A3o%20entre%20sistemas. Acesso em: 01 jun. 2023.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO - OIT. (2021). **Teletrabalho durante e após a pandemia da COVID-19**. Disponível em: https://www.ilo.org/brasilia/publicacoes/WCMS_772593/lang--pt/index.htm. Acesso em: 29 mar. 2023.

OWASP. **OWASP Top Ten Project**. Owasp. (2021). Disponível em: https://owasp.org/www-project-top-ten/#. Acesso em: 22 maio 2023.

RAFALSKI, J. C; ANDRADE, A. L. (2015). **Home-Office: Aspectos Exploratórios do Trabalho a partir de Casa**. Temas em Psicologia, Ribeirão Preto, Brasil, vol. 23, núm. 2, pp. 431-441. Disponível em: https://www.redalyc.org/pdf/5137/513751491013.pdf. Acesso em: 22 mai. 2023.

RODRIGUES, B. (2022). **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, Itacoatiara – AM. Disponível em: https://www.riu.ufam.edu.br/handle/prefix/6170. Acesso em: 12 abri. 2023.

RODRIGUES Jr. et. al. (2020). *Home office* e a segurança da informação em tempos de pandemia. **Revista Eletrônica da Faculdade Invest de Ciências e Tecnologia**, Cuiabá - MT, v.3, n.1. Disponível em: http://revista.institutoinvest.edu.br/index.php/revistainvest/article/view/27/22. Acesso em: 12 abr. 2023.

SARGINSON, N. (2020). **Securing Your Remote Workforce Against New Phishing Attacks**. Computer Fraud & Security. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7508515/pdf/main.pdf. Acesso em: 29 mai. 2023.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ). (2022). Riscos da pirataria. **Segurança da Informação UFRJ**. Disponível em: https://www.security.ufrj.br/dicas/riscosdapirataria/. Acesso em: 02 jun. 2023.

VALENTE, S. (2022). **A cibersegurança no contexto das pequenas e médias empresas portuguesas: um estudo sobre a consciencialização e investimento na mitigação do cibercrime.** Dissertação (Mestrado) – Mestrado em Engenharia Informática, Universidade de Évora – Escola de Ciências e Tecnologia, Évora, 2022. Disponível em: https://dspace.uevora.pt/rdpc/bitstream/10174/33107/1/Mestrado-Engenharia_Informatica-Sergio_Valente.pdf. Acesso em: 17 mai. 2023.