A IDENTIFICAÇÃO DAS VULNERABILIDADES DAS EQUIPES VIRTUAIS LOCAIS E GLOBAIS

IDENTIFYING VULNERABILITIES OF LOCAL AND GLOBAL VIRTUAL TEAMS

Marinês Ribeiro dos Santos
Faculdade de Tecnologia de Santana de Parnaíba
marines.santos@fatec.sp.gov.br

Anderson de Lima Vieira
Faculdade de Tecnologia de Santana de Parnaíba
anderson.vieira10@fatec.sp.gov.br

Mateus Francisco da Silva Santos
Faculdade de Tecnologia de Santana de Parnaíba
mateus.santos81@fatec.sp.gov.br

Irapuan Glória Júnior
Faculdade de Tecnologia de Santana de Parnaíba
ijunior@ndsgn.com.br

Resumo

O objetivo do estudo é analisar os desafios enfrentados por equipes virtuais e as estratégias que podem ser adotadas para promover uma colaboração eficaz em contextos de trabalho remoto, pois a crescente adoção de tecnologias de comunicação e a globalização dos negócios têm levado as organizações a criarem equipes compostas por membros geograficamente dispersos, além de analisar os riscos das vulnerabilidades técnicas e humana na manipulação e tratamento das informações. A pesquisa utilizou a metodologia de pesquisa bibliográfica. Após análise identificou-se que com a criação das equipes virtuais, alguns desafios surgiram em relação ao distanciamento a cultura, ao horário, valores e a segurança da informação. A utilização de aplicativos de comunicação como *Teams*, dentre outros, ficou em evidência com muitas empresas e usuários inscritos, de modo que a segurança cibernética foi afetada. As contribuições para prática são a compreensão mais aprofundada das vulnerabilidades enfrentadas por projetos que adotam equipes virtuais e as contribuições para teoria incluem pesquisas futuras relacionadas a LGPD, quais as dificuldades as empresas enfrentaram para se adequar a LGPD durante e pós pandemia.

Palavras-chave: Equipes Virtuais, Trabalho Remoto, Comunicação Virtual, Coordenação, LGPD, Estratégias de Colaboração.

Abstract

The objective of the study is to analyze the challenges faced by virtual teams and the strategies that can be adopted to promote effective collaboration in remote work contexts, as the increasing adoption of communication technologies and the globalization of business have led organizations to create teams composed of geographically dispersed members, in addition to analyzing the risks of technical and human vulnerabilities in the manipulation and processing of information. The research used a bibliographic research methodology. After analysis, it was identified that with the creation of virtual teams, some challenges arose in relation to distancing, culture, schedule, values and information security. The use of communication applications such as Teams, among others, was highlighted by many companies and registered users, so that cybersecurity was affected. The contributions to practice are a deeper understanding of the vulnerabilities faced by projects that adopt virtual teams and the contributions to theory include future research related to LGPD, what difficulties companies faced in adapting to LGPD during and after the pandemic.

Keywords*: Virtual Teams, Remote Work, Virtual Communication, Coordination, LGPD, Collaboration Strategies.*

1. Introdução

O Caos gerado pela pandemia da COVID-19 em 2020, afetou diversas empresas, sendo necessário buscar soluções e usar a criatividade para superar os problemas consequentes do coronavírus. A criação de equipes Virtuais e o trabalho remoto foram umas das soluções encontradas pelos gerentes de projetos de TI, além de outras mudanças, como a do convívio social e relações de trabalho, isolamento social e restrições à mobilidade das pessoas, resultando em uma mudança de comportamento humano em relação às questões ambientais. Nesse sentido o cenário de trabalho passou a ser o doméstico como um laboratório para o desenvolvimento das atividades e práticas sustentáveis com o objetivo de manter o equilíbrio emocional, social e ambiental (STEFFEN NETO; GLÓRIA JÚNIOR, 2021).

Com a criação das equipes virtuais e o trabalho, remoto a Lei Geral de Proteção de Dados (LGPD), com vigor desde 2020, regulamenta o uso e manipulação de dados no país, criando um ambiente seguro para empresas e usuários e, caso seja infringida, poderá causar enorme prejuízo financeiro e macular a imagem das empresas (BOTELHO; CAMARGO, 2021).

A conformidade legal com a LGPD vai além, evitar dispêndio financeiro e desgaste da imagem da organização, implica na reorganização da área de TI sobre como manipular, anonimizar, excluir os dados e como os profissionais envolvidos devem pautar suas atividades (BAX; BARBOSA, 2020).

A gestão de equipes nos projetos foi modificada com o surgimento da pandemia, com o fechamento de empresas em todo o mundo com desafio para os gestores estabelecerem novas formas de trabalho e o uso de novos softwares para o controle das atividades (STEFFEN NETO; GLÓRIA JÚNIOR, 2021)

Diante deste contexto, o artigo possui como questão de pesquisa: "Quais as vulnerabilidades inerentes a projetos que utilizam Equipes Virtuais e Globais". Os objetivos do trabalho são: (1) Identificar as diferenciações entre equipes virtuais Locais e Globais; (2) Propostas e sugestões de melhorias de segurança.

A análise comparativa entre equipes virtuais locais e globais fornece *insights* valiosos sobre como os desafios podem variar em diferentes contextos, permitindo a adoção de abordagens mais direcionadas para enfrentar esses desafios e promover o sucesso de projetos colaborativos virtuais.

2. Referencial Teórico

2.1. Gerenciamento de Projetos

Um projeto consiste em uma soma de atividades, delimitadas por um início e fim previamente definidos pelo escopo, são realizadas em grupo, objetivando construir um produto, serviço ou resultados únicos (PMI, 2021).

O gerenciamento de projetos é uma técnica relativamente nova, em sua utilização para gerir atividades corporativas. É determinado por técnicas de gestão e administração, adaptadas para obter um controle e utilização dos recursos existentes de maneira mais eficiente (KERZNER, 2021).

O *Project Management Body of Knowledge Guide do Project Management Institute* (PMBoK) se trata de um modelo, ou *framework*, que se encontra disponível no mercado com enfoque em ser um guia para o gerenciamento de projetos. Composto por 10

áreas do conhecimento, tendo como principais o Escopo, Riscos, Custo e Tempo, recomenda maneiras de realizar o gerenciamento de qualquer tipo de projeto (PMI, 2017).

O gerenciamento de projeto é a aplicação do conhecimento, habilidades e ferramentas técnicas para cumprir o projeto e entregar os resultados pretendidos, havendo um pessoas designada pela organização para executar e liderar a equipe do projeto, responsável por alcançar os objetivos do projeto, desempenhado uma variedades de funções facilitando o trabalho da equipe do projeto para alcançar os resultados e gerenciar os processos para entregar os resultados, dentre essas funções está fornecer supervisão coordenação, objetivos e feedbacks, facilitar e apoiar, realizar o trabalho e contribuir com insights, aplicar a especialização, fornecer o orientação e insight comerciais, fornece recursos e orientações, manter a governança (PMI, 2021)

2.2. Equipes Virtuais

A partir da pandemia da COVID-19 muitas mudanças foram adotadas, desde formas de convívio social e até mesmo nas relações de trabalho. Foi decretada, por muitas nações, isolamento social, restrições na mobilidade das pessoas, distanciamento e testagem (OLIVEIRA; LUCAS; IQUIAPAZA, 2020).

Um desdobramento imediato foi a criação repentina de equipes virtuais locais, em que os membros da equipe estão no mesmo país, mas em locais geograficamente distantes (HANEBUTH, 2015; PAINTER et al., 2016). Nos casos em que os integrantes estão em outros países são rotulados como Equipes Virtuais Globais (DERVEN, 2016); DOGHRI et al., 2021; (SHIRISH; SRIVASTAVA; BOUGHZALA, 2023).

Com isso surgiu o desafio aos gestores de estabelecer novas formas de trabalho e o uso de novos softwares para o controle das atividades (STEFFEN NETO; GLÓRIA JÚNIOR, 2021).

As equipes virtuais utilizam tecnologias de comunicação e colaboração, como videoconferências, mensagens instantâneas, e-mails e ferramentas de compartilhamento de documentos, para interagir e coordenar suas atividades de maneira virtual. O aparecimento de avatares pode impactar não só o desempenho criativo em termos quantitativos, mas também o conteúdo das ideias (BUISINE et al., 2016).

O modelo de equipes virtuais pode gerar redução de custos, aumento da produtividade, menor índice de absenteísmo, menos poluição e menos acidentes (PICU; DINU 2016; CASCIO, 2000; BARUCH, 2000). Por outro lado, trazem, também, alguns desafios como dificuldade de manter o comprometimento dos colaboradores, redução do contato social que pode levar a uma sensação de isolamento, e a necessidade de uma nova dinâmica de liderança (PICU; DINU 2016; CASCIO, 2000; BARUCH, 2000).

Equipes virtuais, em contraste com as equipes tradicionais, trabalham em locais diferentes, em que as tarefas são mais estruturadas e a comunicação é, em grande parte, eletrônica e assíncrona. (KRATZER; VAN ENGELEN, 2005). A diversidade cultural entre membros de equipes virtuais globais provém de diferentes países, o que resulta em uma ampla gama de culturas, tradições e valores. Isso pode enriquecer a equipe, mas também requer sensibilidade cultural para evitar mal-entendidos.

Uma equipe dispersa geograficamente, constituída por pessoas que interagem, normalmente, por meios de comunicação eletrônica e que, portanto, têm pouca (ou nenhuma) interação face a face (MALHOTRA et al., 2007). São pessoas que trabalham juntas, mesmo estando geograficamente separadas (MADUKA., 2018).

Equipes virtuais locais compartilham características comuns, apesar de estarem dispersas dentro da mesma região ou país, localização geográfica próxima as equipes virtuais locais consistem em membros que estão distribuídos em diferentes locais, mas dentro da mesma região geográfica. Isso pode incluir cidades diferentes dentro do mesmo país ou até mesmo unidades organizacionais em diferentes prédios de uma mesma cidade, (ABHARI et al., 2023; DOGHRI et al., 2021; REN et al., 2020; (SHIRISH; SRIVASTAVA; BOUGHZALA, 2023; WEILAND; KNIZHNIK 2022)

Nos casos em que a equipe virtual possui alguns ou todos os membros situados remotamente em outro país, a denominação passa a ser de Equipe Virtual Global, ou *Global Virtual Team* (GVT), com diferenças culturais marcantes (OLAISEN et al.,2017); (SHIRISH; SRIVASTAVA; BOUGHZALA, 2023), e com desafios maiores em sua gestão (BOYRAZ, 2019; DOSSICK et al., 2019). A competência intercultural também pode ser valiosa para interações externas à organização.

Quanto mais diversificada culturalmente a equipe, mais importante se torna compreender os estilos de comunicação preferidos de cada membro, a ponto de quais diretrizes podem se tornar apropriadas (MAYER; BELLO 2012).

2.3 Segurança da Informação

Segurança da Informação pode ser definida como resultado do agrupamento e tratamento de informação que possui valor, preservando os dados, de modo que a segurança visa proteger software, hardware, sistemas, e recursos e serviços contra falhas, ataques e tratamento não autorizado (SANTOS; SILVA, 2021). Qualquer empresa pode estar sujeita a vulnerabilidades que pode comprometer os ativos e dados se não possuírem políticas e procedimentos de segurança bem definidos que podem ser identificados por sistemas de gerenciamento e monitoramento e auditoria (HINTZBERGEN et al., 2018).

Para o desenvolvimento de aplicações seguras são necessários princípios importantes, estes conhecidos como triângulo CIA (TIPTON et al., 2016) que específica quais requisitos para estabelecer, implementar, manter e melhorar continuamente qualquer sistema de gerenciamento de segurança da informação. A norma os princípios são definidos como: (1) Confidencialidade/ *Confidentiality*; (2) Integridade/ *Integrity*; e (3) Disponibilidade/ *Availability*. (ISO, 2013).

O pilar da confidencialidade se refere aos acessos autorizados a qualquer informação, definindo que este devem ser obtidos editados e manipulados apenas por pessoas autorizadas (ISO/IEC,2013) pode-se citar como exemplo, uma pessoa em determinado cargo não possuir interesse organizacional em documentos de um outro departamento e devendo sofrer medidas protetivas aos dados como criptografias, autenticação, *traffic padding* (HINTZBERGEN et al., 2018).

A integridade é necessária para que os dados estejam precisos e atualizados. E inclui políticas contra uso não autorizado, estando ligado ao não repudio e da irretratabilidade (MUSONDA et al., 2019). A integridade garante que as informações continuem completa, sem alteração da forma, se refere a manter a informação no estado desejado pelos seus administradores mesmo estando incorreta e qualquer mudança não autorizada de dados, acidental ou deliberada é uma falha e resultando na violação da integridade dos dados (HINTZBERGEN et al., 2018).

Já a disponibilidade garante que as informações estejam disponíveis para o usuário autorizado que necessita acessá-la, no entanto é necessária uma avaliação direcionado aos usuários de acordo com as políticas estabelecidas pela organização e país, que muitas vezes não são restringidas por questões de segurança da informação (DIANA et al., 2016). Os dados não podem estar inacessíveis a pessoas e autoridades autorizadas não importando a localização e momento. (ISO/IEC,2013).

Com a pandemia causada pela COVID-19, houve um aumento nos números de crimes cibernéticos, as vulnerabilidades cresceram com a pandemia uma vez que o mundo inteiro ficou em isolamento e tendo de recorrer a serviços digitais, as empresas foram obrigadas a migrar seu ambiente de trabalho físico para o remoto ficando exposta a crimes cibernéticos (OLIVEIRA et al., 2023).

Com aumento do uso das ferramentas de videoconferência online com demanda de novos usuários escritos como, o *Messenger, Zoom, Google Meet*, Microsoft Teams (LUCAS BASTOS; NEVES, 2021) dentre outros e trouxe benefícios diante da pandemia, e que também intensificou os ataques cibernéticos.

Conforme a Tabela 1 os principais tipos de ataques virtuais durante a pandemia do Covid-19 está o *Phishing* visa roubar ou danificar dados confidenciais enganado as pessoas para que revelem informações pessoais, como senhas e números de cartão de crédito. MICROSOFT, 2023), em que geralmente está associado à um e-mail escrito e formatado para confundir os usuários, esse e-mail contém um link ou arquivo que desvia o usuário para um site ou programa malicioso (NAGLI, 2022).

Engenharia social é método onde o invasor usa persuasão abusando da confiança ou ingenuidade do indivíduo para obter informações que podem ser utilizadas para ter acesso não autorizado a dispositivos e informações confidenciais (BARROS, 2021).

Um dos tipos frequentes de ataques é de *Ransomwares,* a palavra "ransom" (resgate) sugere que será feita uma extorsão, o processo inicia com o bloqueio do computador, com a criptografia de todos os dados, e depois a exigência de um resgate para liberá-lo (KASPERSKY, 2023). O acesso ao sistema da vítima é conquistado com técnicas de engenharia social ou *phishing*, quando a vítima acessa o arquivo ou link infectado, arquivos ou *devices* são criptografadas dando o início ao processo de sequestro (NAGLI, 2022).

Tabela 1: Principais tipos de ataques cibernéticos durante e pós pandemia

Tipos	Características
Phishing	O *Phishing* visa roubar ou danificar dados confidenciais enganado as pessoas para que revelem informações pessoais, como senhas e números de cartão de crédito. (MICROSOFT, 2023)
Engenharia social	Ataques que levam em consideração o fator humano, usando manipulação e trabalhando com os medos do usuário e tentado obter acesso a informações (NAGLI, 2022)
Desinformação	Compartilhamento de fake News e os processos de desinformação são chaves para manipulação de conceitos e preconceitos dos cidadãos (NAGLI, 2022)
Websites Maliciosos	É feito em conjunto com técnicas de phishing onde e-mails são enviados com assuntos relacionados ao COVID-19 redirecionado os usuários para sites com conteúdo malicioso.(NAGLI, 2022)

Fonte: Autores

2.4 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) é uma regulamentação que visa proteger a privacidade e os direitos dos titulares de dados pessoais no Brasil. Ela se aplica não apenas ao tratamento de dados por empresas, mas também à formação e gestão de equipes virtuais, uma vez que essas equipes frequentemente envolvem o processamento de informações pessoais, mesmo que de forma indireta. Aqui estão algumas diretrizes sobre como a lei é aplicada na criação de equipes virtuais: a liberdade de expressão, de imprensa e da informação, a inovação, o desenvolvimento econômico e tecnológico, a livre iniciativa e concorrência, e os direitos humanos (BRASIL, 2018). Tem como principal base a *General Data Protection Regulation (GDPR)*, legislação europeia para a proteção de dados (CELIDONIO; NEVES; DONÁ, 2020).

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão público que tem a função de aplicar as sanções administrativas e criar metodologias para sua aplicação, estabelecer as atribuições do encarregado, criar padrões para medidas contra o acesso não autorizado, regulamentar o compartilhamento de informações sensíveis entre colaboradores (MARTINS, 2021).

Empresas que formam equipes virtuais devem nomear um *Data Protection Officer* (DPO) responsável por supervisionar o cumprimento da LGPD que atua como um ponto de contato entre a empresa, os membros da equipe virtual e as autoridades de proteção de dados. O DPO deve auditar as operações e mantê-las sempre de acordo com as necessidades da lei e com os requisitos da ANPD (BOTELHO; CAMARGO, 2021).

3. Metodologia

As característica da pesquisas (Tabela 2) incluem sua natureza como qualitativa (GIL, 2019), com uso da metodologia de pesquisa bibliográfica, que procura explicar e discutir um assunto tema ou problema com base em referencias publicadas em livros, periódicos, revistas, enciclopédia, dicionários, jornais, sites, e anais de congressos, buscando conhecer, analisar e explicar contribuições sobre um tema (MARTINS; THEÓPHILO, 2016). A coleta de dados foi baseada em publicações referentes ao tema como; artigos, revistas, base de dados, sites relacionados a tecnologia da informação.

Tabela 2: Características da pesquisa

Etapas	Conteúdo	Autores
Natureza	Qualitativa	Gil (2019)
Metodologia	Pesquisa Bibliográfica	Martins e Theóphilo (2016)
Coleta de Dados	Base de dados, Artigo Científicos	

Fonte: Autores

Procedimentos metodológicos para estudo (Figura 1) são:

1ª Etapa: Definir o tema ou problema que será investigado: início de busca do material, um tema e uma questão de pesquisa foi definido.

2ª Etapa: Definir a metodologia: análise da revisão da literatura (pesquisa bibliográfica: Realizou-se uma pesquisa sobre o tema em base de dados como o Scholar, onde várias publicações foram analisadas como livros e artigos foram selecionados.

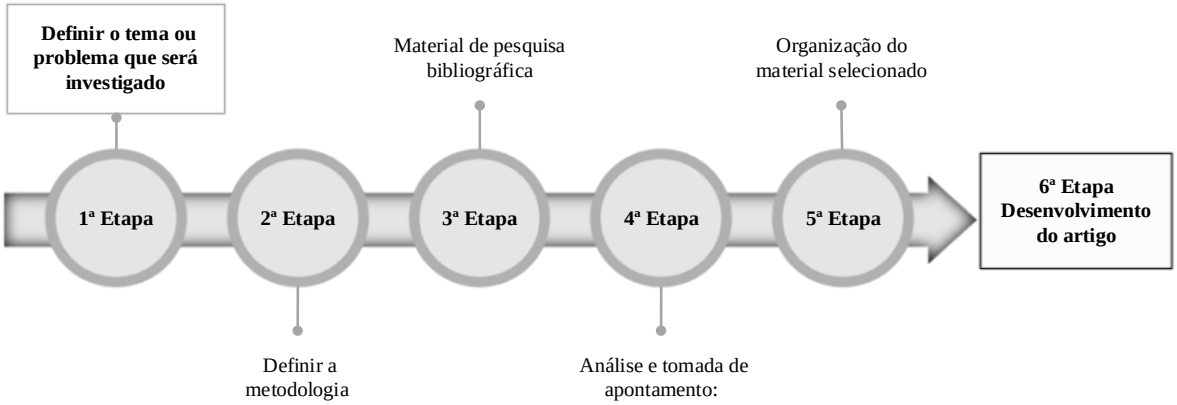
3ª Etapa: Material de pesquisa bibliográfica: Consulta e leitura por obras de referência examinando o material tema, introdução, capítulos, abstract relacionados ao tema, principalmente a bibliografia. As fontes da pesquisa foram de publicações em base de dados e sites confiáveis.

4ª Etapa: Análise e tomada de apontamento: Com o material escolhido inicia-se os apontamentos, ou registro de informações convenientes para a construção da pesquisa bibliográfica, evitando o acúmulo de material excessivo. O material foi escolhido e as fontes foram citadas, com obras e autores referenciados relacionados ao tema.

5ª Etapa: Organização do material selecionado: Leitura do material e das informações com análise nos pontos principais.

6ª Etapa: Desenvolvimento do artigo: O artigo foi escrito baseado nas informações e afirmações da pesquisa realizadas em várias publicações consultadas em base de dados acadêmicas.

Figura 1: Processos Metodológicos



Fonte: Autores

4. Análise e Interpretação dos Resultados

4.1. Diferenciação das Equipes Virtuais Locais e Globais

É possível encontrar na literatura (Tabela 3) que o posicionamento geográfico (D01) das equipes virtuais locais (LVT) apresenta pouco afastamento (HANEBUTH, 2015; PAINTER et al., 2016), pois pode estar dentro de uma mesma região ou país, em contrapartida, a equipe virtual global (GVT) se encontra em localizações distantes, podendo estar em outros países e/ou continentes (DERVEN, 2016); DOGHRI et al., 2021; (SHIRISH; SRIVASTAVA; BOUGHZALA, 2023).

Foi observada uma diferenciação na Cultura (D02), em que as LVT apresentam conformidades, e as GVT podem apresentar divergências, e consequentemente necessidade

de maior entrosamento (OLAISEN et al., 2017; SHIRISH; SRIVASTAVA; BOUGHZALA, 2023).

O Tempo (D03) mostrou-se diferentes nas situações, visto que as equipes virtuais globais podem apresentar mais de um fuso horário. Fato de não ocorrer com as equipes locais.

Outro tópico a ser analisado é a Comunicação (D04) entre os membros da equipe, as equipes locais, por uma questão de proximidade, tendem a falar a mesma língua. O que não ocorre com as equipes globais, podendo haver inúmeras variações linguísticas, que podem comprometer o entendimento.

As Regulamentações (D05) também variam, quando se trata das equipes globais, por ser tratar de um relacionamento internacional, há diferenças nas leis que regem as atividades dos membros das equipes locais, diferentes neste aspecto, pois podem não estar sob as mesmas diretrizes.

Tabela 3: Diferenciação das LVT e GVT

#	Característica	Equipe Virtual Local	Equipe Virtual Global
D01	Posicionamento Geográfico	Dispersos dentro de uma mesma região ou país	Encontram-se em diferentes países e/ou continentes
D02	Cultura	Cultura semelhante, ou com pouca variação	Cultura que pode vir a ser completamente diferente
D03	Tempo	Partilha o mesmo Fuso horário	Pode apresentar diferenças de Fuso horário
D04	Comunicação	Falam a mesma língua, com, em alguns casos, variações regionais	Tendem a falar línguas distintas, podendo comprometer o entendimento mútuo
D05	Regulamentações	Em muitos casos há uma conformidade de regulamentações	Pode haver diferentes regulamentações, necessitando de maior adaptabilidade

Fonte: Autores

4.2 Proposta e Melhorias na Segurança do Ambiente

Esta pesquisa apresenta sugestões de mitigação (Tabela 4) de acordo com as informações encontradas na literatura. O ambiente em equipes virtuais é caracterizado pelo uso de software de comunicação, como o *Teams* (MS). Desta forma, há a necessidade de criar formas de segurança para proteger os membros das equipes e ambiente.

Para garantir a integridade e disponibilidade, há algumas medidas de segurança que podem de forma eficaz prevenir, detectar e responder as ameaças cibernéticas assegurando todos os princípios de segurança da informação para manter o ambiente seguro e mitigar os danos causados pelos ataques, de modo que essa medidas consistem em três fatores principais: as tecnologias que englobam softwares, os serviços com finalidade de proteger e garantir a integridade do sistemas e os dados presentes, essas tecnologias incluem *Virtual Private Network* (VPN), como dispositivo de segurança da rede que monitora e filtra o trafego da rede *Firewall* (M01).

Há também as políticas e práticas que são em resumo regras e normas determinadas que visa garantir a proteção dos dados e de quem manipula, exemplos disso são os procedimentos que devem ser documentados e as políticas de troca de senhas manuais de boas práticas (M05) (OLIVEIRA et al., 2023).

O fator humano também é uma medida pois descreve o comportamento humano como fator de risco frente às tecnologias, de modo que essas medidas giram em torno de capacitação e treinamentos (M02) sobre temas importantes e inerentes a proteção e segurança no ambiente digital, as empresas precisam estar preparadas com profissionais capacitados monitorando as estruturas e recursos tecnológicos assim como seus procedimentos e hábitos especificações técnicas com objetivo de identificar as vulnerabilidades de natureza técnica as vulnerabilidades de natureza humana (OLIVEIRA et al., 2023).

Os administradores de rede devem instalar *firewalls*, sistemas de detecção de intrusão e de prevenção de intrusão (M03), sendo soluções para serem implantadas, como *host* funcionando com base em assinatura ou anomalias, de modo que a redução de falsos alertas e falsos negativos são importantes para a utilização de dessas soluções, principalmente se os ataques forem raros (TANENBAUM; FEAMSTER; WETHERALL, 2021).

A equipe deve utilizar ferramentas e técnicas avançadas de detecção de ameaças para identificar comportamentos que são um risco para ambiente utilizando antivírus (M4) e firewall, para a adoção de práticas como controle de acesso, realização de backup, treinamentos e criptografia (OLIVEIRA et al., 2023) que pode ser usada para manter informações confidenciais garantindo a integridade e autenticidade, na criptografia muitos algoritmos usam permutações e substituições para transformar os textos simples em cifrado.

As ferramentas criptográficas podem ser usadas para proteger o tráfego da rede e o IP *secutity* (*IPsec)* opera na camada de rede codificando fluxos de pacotes de *host* para *host*, e fornece segurança na comunicação, em que os *firewalls* podem efetuar a triagem do tráfego em uma organização. *As redes privadas virtuais* (M01) podem oferecer propriedades de segurança e *as redes sem fio* podem estar seguras com o protocolo de autenticação como *Diffie-Hellman, Kerberos e criptografia* de chave pública (TANENBAUM, 2021). O treinamento dos profissionais (M02) é vital para a empresa OLIVEIRA et al, (2023).

Tabela 4: Mitigações para vulnerabilidades técnicas e humana

#	Item	Mitigação	Autor(es)
M01	Comunicação Computacional	Utilização da VPN, Firewall, IP security (IPsec), Pretty Good Privacy (PGP)	TANENBAUM (2021)
M02	Fator Humano	Capacitação e Treinamento	OLIVEIRA et al, (2023)
M03	Rede/Web	Sistema de detecção de intrusão (IDS), Sistemas de Prevenção de Intrusão (IPS), *Domain Name System Security Extensions* (DNSSEC), *Transport Layer Security* (TLS)	TANENBAUM (2021)
M04	Ferramentas e Técnicas avançadas de detecção de ameaças	Utilizando antivírus e firewall, adoção de práticas como controle de acesso, realização de backup e criptografia	OLIVEIRA et al, (2023); TANENBAUM (2021)
M05	Regulamentações	Políticas e práticas, procedimentos que devem ser documentados	OLIVEIRA et al, (2023)

Fonte: Autores

Para segurança do correio eletrônico (M01) pode ser usado técnicas como *Pretty Good Privacy* (*PGP)* que compacta as mensagens codificando com uma chave pública do receptor, efetuando o *hash* de mensagens assinado para confirmar a integridade, é um pacote completo para segurança de mensagens de correio eletrônico que fornece privacidade, autenticação, assinaturas digitais e compactação de forma fácil de usar.

Há ainda segurança (M3) da Web o *Domain Name System Security Extensions* (DNSSEC) evita o modo o *spoofing* do *Domain Name System* DNS, que relaciona os nomes da Internet aos respectivos endereços, e a utilização do protocolo de transporte seguro ou *Transport Layer Security* (TLS), (M03) para estabelecer sessões autenticadas e seguras entre o cliente e o servidor, é um protocolo que transporta o *HyperText Transfer Protocol* (HTTP), constituindo o *Secure HyperText Transfer Protocol* (HTTPS) com segurança (TANENBAUM, 2021).

5. Conclusão

Com o surgimento da pandemia muitas empresas foram obrigadas a mudarem a forma de trabalho mesmo não estando preparadas com a situação, tiveram de buscar soluções para manter a organização, as equipes, os colaboradores e as informações da empresa em segurança.

Mudaram a forma de trabalhar, do modelo presencial para o remoto, surgindo assim as LVT, equipe em que os membros estão no mesmo país, mas em locais geograficamente distantes, e GVT com membros das equipes estão outro país e com isso alguns desafios, principalmente para gerentes de projetos TI. Com a criação das equipes virtuais tanto local quanto global, alguns desafios surgiram em relação ao distanciamento a cultura, ao horário, a segurança, valores. A utilização da internet e os aplicativos de comunicação como Teams, Zoom, Google Meet e outros ficaram em evidência com muitas empresas e usuários inscritos, de modo que a segurança cibernética foi afetada, com crescente aumento dos ataques e crimes virtuais, como *phishing* e *Ransomware* fazendo vítimas em todo o mundo, e até mesmo grandes empresas.

Diante da situação a segurança da informação fica em evidência buscando soluções para mitigar as vulnerabilidades de natureza humana e as vulnerabilidades de natureza técnica. Dentre as possíveis mitigações os administradores de rede devem instalar firewalls, sistemas de detecção de intrusão e sistemas de prevenção de intrusão, sendo boas soluções para serem implantadas na rede. O fator humano também é fator de risco frente às tecnologias, de modo que essas medidas e prevenção giram em torno de capacitação e treinamentos sobre temas importantes e inerentes a proteção e segurança no ambiente digital, as empresas precisam estar preparadas com profissionais capacitados monitorando as estruturas e recursos tecnológicos assim como seus procedimentos.

As contribuições para prática são a compreensão mais aprofundada das vulnerabilidades específicas enfrentadas por projetos que adotam equipes virtuais, permitindo que as organizações estejam mais preparadas para mitigar os desafios as vulnerabilidades que causam impactos no gerenciamento de projetos das equipes virtuais. A análise comparativa entre equipes virtuais locais e globais contribui para um maior entendimento na tomada de decisão com boas estratégias para lidar como desafios que podem variar em diferentes contextos, permitindo a adoção de abordagens mais direcionadas para enfrentar esses desafios e promover o sucesso de projetos colaborativos virtuais. As contribuições para teoria incluem pesquisas futuras relacionadas a LGPD, quais as dificuldades as empresas enfrentaram para se adequar a LGPD durante e pós pandemia.

Referências

ABHARI, Kaveh; PESAVENTO, Michael; WILLIAMS, David. **Apoiar a inovação participativa durante a pandemia da COVID-19: um estudo comparativo da utilização das redes sociais pelas empresas**. Tecnologia da Informação & Pessoas, v. 5, pág. 2030-2062, 2023.

BARROS, E. G. Acesso sem controle a internet: uma abordagem com engenharia social atraves de wireless fidelity (wifi). **Monumenta-Revista Científica Multidisciplinar**, v. 2, n. 1, p. 59–63, 2021.

BASTOS, N. B. N. DE L.; NEVES, L. N. L. M. Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus). **Revista Tecnológica da Fatec Americana**, v. 9, n. 01, p. 68–83, 2021.

BAX, M. P.; BARBOSA, J. L. **Proposta de mecanismo de consentimento na lei geral de proteção de dados-LGPD**. Seminar on Ontology Research in Brazil; Doctoral and Masters Consortium on Ontologies. **Anais**...Universidade Federal de Minas Gerais, 2020.

BOTELHO, M. C.; CAMARGO, E. P. DO A. O tratamento de dados pessoais pelo poder público na LGPD. **Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)**, v. 9, n. 3, p. 549–580, 2021.

BUISINE, S. et al. Using avatars to tailor ideation process to innovation strategy. **Cognition, Technology & Work**, v. 18, p. 583–594, 2016.

CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira-Um estudo de caso/Methodology for mapping and adequacy of the requirements listed in LGPD (Brazil Data Protection General Law number 13 709/18) in a financial institution-A case study. **Brazilian Journal of Business**, v. 2, n. 4, p. 3626–3648, 2020.

DERVEN, M. Four drivers to enhance global virtual teams. **Industrial and Commercial Training**, v. 48, n. 1, p. 1–8, 2016.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

HINTZBERGEN, J. et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. São Paulo: Brasport, 2018.

KERZNER, H. **Gerenciamento de projetos: uma abordagem sistêmica para planejamento, programação e controle-2a Edição**. São Paulo: Editora Blucher, 2021.

MARTINS, G. DE A.; THEÓPHILO, C. R. **Metodologia da Investigação Científica Para Ciências Sociais Aplicadas**. 3. ed. São Paulo: Atlas, 2016.

MARTINS, R. M. Proteção de dados pessoais e Administração Pública: Protection of personal data and Public Administration. **International Journal of Digital Law**, v. 2, n. 1, p. 133–149, 2021.

NAGLI, L. S. D. Pandemia na pandemia: a escalada de ataques cibernéticos pós COVID-19 Pandemic in pandemic: the climbing of post COVID-19 cyber attacks. **Brazilian Journal of Development**, v. 8, n. 4, p. 28482–28493, 2022.

OLIVEIRA, A. C. DE; LUCAS, T. C.; IQUIAPAZA, R. A. O que a pandemia da covid-19 tem nos ensinado sobre adoção de medidas de precaução? **Texto & Contexto-Enfermagem**, v. 29, 2020.

OLIVEIRA, I. et al. Proposta de arquitetura empresarial para monitoramento e mitigação de riscos relacionados à ameaças cibernéticas. 2023.

PMI. **A Guide to the Project Management Body of Knowledge (PMBOK Guide)**. 6. ed. Pensylvania: Project Management Institute, 2017.

PMI. **Gerenciamento de Projetos e Guia do Conhecimento em Gerenciamento de Proejtos (Guia PMBoK)**. 7. ed. Pennsylvania: Project Management Institute, 2021.

SANTOS, R. B. DOS; SILVA, T. B. P. E. Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 19, p. e021024–e021024, 1 out. 2021.

SHIRISH, A.; SRIVASTAVA, S. C.; BOUGHZALA, I. **Contextualizing Team Adaptation for Fostering Creative Outcomes in Multicultural Virtual Teams: A Mixed Methods Approach**. Association for Information Systems, , 2023. Disponível em: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85163064209&doi=10.17705%2f1jais.00811&partnerID=40&md5=8f7594dfa55eb6f93b5b80b67659b77d>

STEFFEN NETO, F.; GLÓRIA JÚNIOR, I. Os Impactos da Pandemia do COVID 19 nos Projetos de TI em uma Empresa do Terceiro Setor. **Journal of Technology & Information (JTnI)**, v. 1, n. 1, 2021.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Redes de computadores**. 6. ed. São Paulo: Bookman, Porto Alegre, 2021.

TIPTON, S. J.; FORKEY, S.; YOUNG, B. Rumo a métodos de autenticação adequados no acesso a registros médicos eletronicos em conformidade com o triangulo HIPAA e CIA. **Jornal de Sistemas médicos**, 2016.

VAN DYNE, L., ANG, S., NG, K.-Y., ROCKSTUHL, T., TAN, ML E KOH, C, **“Subdimensões do modelo de quatro fatores de inteligência cultural: expansão a conceituação e medição da inteligência cultural”**, Social and Personality Psychology Compass, Vol. 6 Nº 4, 2012.