VIRTUAL PRIVATE NETWORKS - VPN: SUA IMPORTÂNCIA NO CONTEXTO EMPRESARIAL

VIRTUAL PRIVATE NETWORKS - VPN: ITS IMPORTANCE IN THE BUSINESS CONTEXT

Guilherme A. Nicoleti[1], Rogério L. S. Oliveira[2]

[1]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, guilherme.nicoleti@fatec.sp.gov.br
[2]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, rogerio.leao@fatec.sp.gov.br

Trabalho de Graduação apresentado à Faculdade de Tecnologia Prof. José Camargo - Fatec Jales, como requisito parcial para obtenção do título de Tecnólogo em Sistemas para Internet

RESUMO
Com a crescente migração para o home-office, a preocupação com a segurança nas empresas tem crescimento proporcional. Porém, este fato tem sido muito negligenciado pelas organizações. A *Virtual Private Network* (VPN), uma opção segura para conexão remota, criação de ambiente seguro e túneis de compartilhamento de dados, se torna a melhor opção para manter a segurança e integridade das empresas. Diante deste fato, este trabalho possui o objetivo de entender como a VPN funciona: sua importância, protocolos utilizados, aplicação no cenário empresarial, aplicativos para fazer sua conexão, além dos diferentes tipos de conexão que existem. No tocante, contém o referencial teórico utilizado, tópico que apresenta o assunto com informações presentes em artigos, livros, sites, pesquisas e portais de notícias oficiais. Por fim, foi conduzida uma pesquisa quantitativa com o intuito de identificar quantas empresas tem conhecimento da ferramenta, se fazem seu uso e qual aplicativo utilizam para a conexão, elucidando sua importância.
Palavras-chave: VPN; segurança online; home-office.

ABSTRACT
With the increasing migration to remote work, concern for security in companies has grown proportionally. However, this fact has been greatly neglected by organizations. Virtual Private Network (VPN), a secure option for remote connection, creating a secure environment and data sharing tunnels, becomes the best choice to maintain the security and integrity of companies. Given this fact, this work aims to understand how VPN works, its importance, the protocols used, its application in the business scenario, connection applications, as well as the different types of connections that exist. In this regard, it contains the theoretical framework used, a section that presents the subject with information from articles, books, websites, research, and official news portals. Finally, a quantitative research was conducted to identify how many companies are aware of the tool, whether they use it, and which application they use for the connection, elucidating its importance.
Keywords: VPN; web secutiry; home-office.

1 INTRODUÇÃO

Com o advento da pandemia do vírus Sars-CoV-2 - COVID-19[1] as empresas, como forma de manter sua produtividade e funcionamento seguro, aderiram ao regime de trabalho remoto,

[1] Segundo a Fundação Oswaldo Cruz (FIOCRUZ, 2020), o nome Covid se refere a junção das *letras (co)rona (vi)rus (d)isease*, que traduzindo para o português, "doença do coronavírus", já o número 19, refere-se a 2019, ano em que foi divulgado o primeiro caso da doença.

denominado “*home office*”.

Tal regime se demonstrou notoriamente eficaz ao ponto de organizações manterem o regime mesmo no mundo pós-pandêmico. Segundo Gandra (2021), cerca de 18 mil colaboradores (equivalente a aproximadamente 25% do quadro operacional) da mineradora Vale, estão no regime de teletrabalho.

Entretanto, para que o regime *home office* funcione adequadamente, é necessário possuir uma conexão estável e segura com a internet. Ademais, considerando o aspecto privacidade, os usuários da grande rede demonstram grande preocupação.

Segundo dados divulgados pelo Núcleo de Informação e Coordenação do Ponto BR – (NIC.br, 2021), 42% dos usuários da internet maiores de 16 anos relatam ter “muita preocupação” em relação a captação e tratamento de suas informações durante a realização do ato de compra em sites e aplicativos. Em relação a aplicativos bancários, 41% dos entrevistados dizem estar “muito preocupados” e 24% “preocupados” com o tratamento de seus dados sensíveis, dentre eles, seus dados biométricos.

Não só por parte de pessoas físicas surge essa preocupação. Empresas também se mostram muito preocupadas. De acordo com o NIC.br (2021), cerca de 23% das empresas entrevistadas dispuseram de uma área dedicada a proteção da informação e a execução da Lei Geral de Proteção de Dados (LGPD).

Ademais, surge uma necessidade de viabilizar o acesso dos colaboradores as informações da empresa, tornando-se necessário a utilização de Virtual Private Network (VPN) para garantir a integridade do acesso a informações para realização da função contratada.

Representando alta segurança e baixo custo, segundo Nakamura et al. (2016), as VPNs, além de possuir baixo custo com a comunicação, possibilitam maior segurança no tráfego dos dados. Este baixo custo é possível devido ao fato de a organização não precisar manter uma infraestrutura própria de acesso remoto, contratando assim serviços de terceiros para a realização da conectividade remota.

Indo além, conforme Siqueira, Castro e Nakamura (2003) as VPNs podem ser implantadas por meio de *Services Providers* (SP), possuindo como principais vantagens a dispensa de um *software* ou *hardware* específicos para o acesso, que é realizado através de túneis seguros entre os pontos de acesso, para o envio sigiloso dos dados.

Este recurso se chama *Provider-Provisioned VPN* (PPVPN), o que permite serviços como VPNs ponto-a-ponto baseados na arquitetura de protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) como também serviços de comunidades virtuais.

Além disso, a produtividade com o uso de VPNs em ambiente corporativo é evidente, como Oliveira (2020) declara que ao trabalhar em uma organização que possui uma VPN para tráfego de dados e acessos controlados, os colaboradores podem focar em fazer sua atividade principal, como por exemplo, desenvolvimento, com a certeza de que o sistema não será invadido a qualquer momento.

Contudo, somente o fato de se dedicar ao foco em fazer o que lhe é proposto em um ambiente seguro, não se torna o único responsável pelo aumento da produtividade os colaboradores.

Segundo a Pesquisa de Transformação Digital para micro, pequenas e médias empresas (MPMEs), encomendada a realização pela Microsoft (2023) no Brasil, o impacto na produtividade acontece por meio de uma possibilidade oriunda do uso de VPNs. Sendo ela, a possibilidade do modelo de trabalho remoto ou híbrido, que está presente em pelo menos 55% das empresas. Sendo que em pelo menos 71% das pequenas e médias empresas, os colaboradores passam cerca de 50% do tempo em suas casas, realizando sua função de forma remota, comparecendo ao escritório apenas algumas vezes na semana.

Neste contexto, este trabalho busca apresentar como as VPNs funcionam, seus principais objetivos, principais métodos de aplicação no ambiente corporativo, protocolos utilizados e

exemplos de utilização do atual mercado de trabalho.

Assim, o presente trabalho encontra-se organizado como segue. Na Seção 2 é apresentada o referencial teórico do tema abordado. Na Seção 3 é apresentada a metodologia utilizada na produção do trabalho em questão. Na Seção 4 é apresentada a análise dos resultados colhidos durante a confecção do artigo. Por fim, na Seção 5 é apresentada as considerações finais do referido trabalho.

2 REFERECIAL TEÓRICO

Nessa seção são apresentas as principais fontes de informação que embasam este trabalho, tais quais, a importância do uso da VPN no contexto empresarial, tipos de conexões, protocolos utilizados, entre outros.

2.1 IMPORTÂNCIA DO USO DA VPN

Inicialmente, é necessário compreender a importância do uso de VPN em seu negócio, de acordo com Kaspersky (2022), uma boa rede privada, possui como principal função criptografar seu endereço IP, o qual revela sua localização, seus dados de busca e algumas vezes, seus dados pessoais, os quais devem estar protegidos com a utilização de criptografia.

Neste contexto, é necessário a escolha assertiva de conexão VPN que mais se enquadra no contexto de sua utilização, Garcia et al. (2013), destaca seus tipos de conexões VPN:

- SSL[2] VPN, ou pontos de acesso para cliente, que por sua vez, é utilizada principalmente nas empresas que fizeram adesão ao *home-office*;
- VPN site-a-site, isto é, entre hosts de comum acesso, utilizada para mascarar endereços IPs e ocultar intranets, esta por sua vez, possui alta complexidade de implementação;
- VPN cliente-servidor, que é encontrada com maior facilidade em ambientes domésticos, em que o usuário não se conecta com o provedor de internet local, mas sim com seu provador de VPN, cobrindo assim sua atividade na WEB[3].

Além disso, todas as conexões VPN devem possuir autenticação de dois fatores, criptografia de protocolos de transferência de dados na rede e um *kill switch*[4] calibrado. Sendo este, último responsável por desempenhar a função de detecção de interrupção no acesso a VPN, para que seja feito o tratamento do erro e nenhum dado seja comprometido no acesso, acarretando uma falha que pode impactar diretamente no funcionamento correto do sistema de gestão de uma organização.

Com isto, torna-se evidente e indispensável o uso da VPN como método de proteção em organizações que optam por adotarem o *home-office* como método de trabalho. Visto que, ao criar um ambiente controlado com prevenção de erros.

Além de tornar a navegação de seu sistema segura, os próprios colaboradores estarão protegidos contra-ataques de terceiros, pois métodos de invasão que não dependem de ações do usuário para acontecer, diferentemente de *pishing*, estarão impedidos dessa forma.

2.2 TIPOS DE VPN'S EXISTENTES

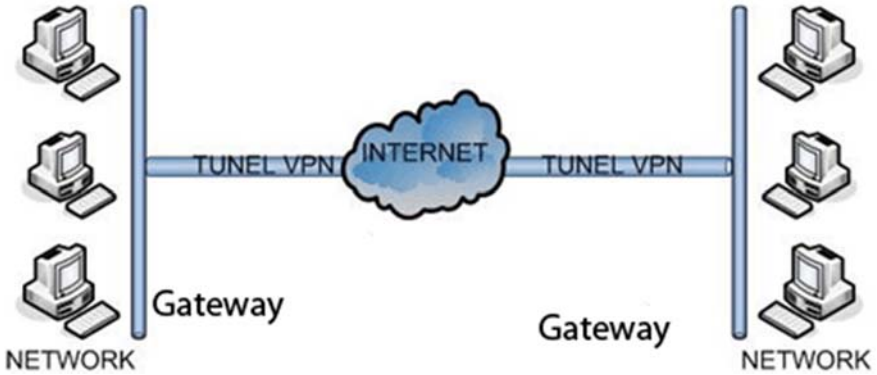
Em primeiro lugar, deve-se entender os três tipos de VPN existentes e seus respectivos contextos de aplicações práticas, sendo eles: *Gateway-to-Gateway*, *Host-to-Host* e por fim, *Host-to-Gateway*.

---

[2] *Security Socket Layer*, que em português é "Camada de Soquete Seguro".
[3] *WEB*, que em português seria "Teia".
[4] Segundo Buxton (2021), *kill switch* ou "bloqueadores de conexão", são dispositivos que bloqueiam a conexão VPN ao detectar alterações na rede em que o host está conectado.

Gateway-to-Gateway: De acordo com Ballesteros (2023), esse tipo de VPN é utilizado em seu contexto para proteger a comunicação de uma rede, como por exemplo, a comunicação de uma grande empresa entre duas redes. Na prática, a aplicação ocorre na comunicação de uma matriz com sua filial, assim como pode ser verificado na Figura 1.

Figura 1 – VPN Gateway-to-Gateway



Fonte: BALLESTEROS, 2023.

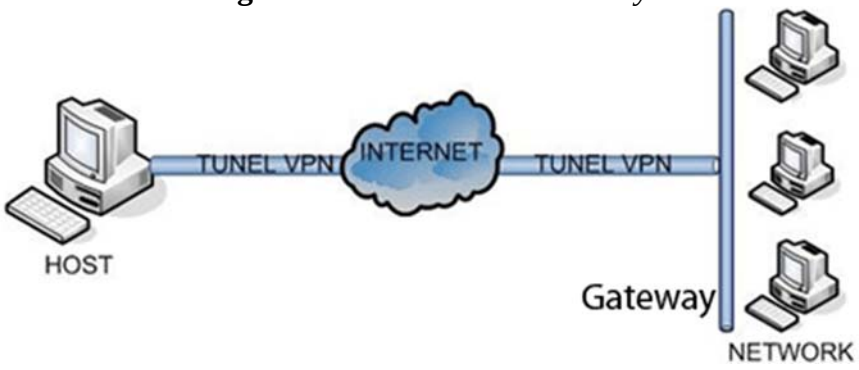
Host-to-Host: Como conceitua Borges, Fagundes e Cunha (2007), esse tipo de conexão se trata de uma conexão entre dois computadores, os quais podem ou não estarem conectados na mesma rede e, seu contexto de utilização prático seria em uma conexão remota de um computador a outro para troca de arquivos, por exemplo, assim como pode ser verificado na Figura 2.

Figura 2 – VPN *Host-to-Host*

Fonte: BALLESTEROS, 2023.

Host-to-Gateway: Esse tipo de VPN se trata da conexão de um computador com uma rede remota, seu contexto de aplicação é no cenário de home-office, em que o funcionário acessa remotamente a rede da empresa, assim como pode ser verificado na Figura 3.

Figura 3 – VPN *Host-to-Gateway*



Fonte: BALLESTEROS, 2023.

2.3 PROTOCOLOS DE CONEXÃO VPN

No tocante, é de extrema importância entender como funciona uma VPN básica para privacidade e segurança no acesso, como conceitua Branco (2021), a VPN oculta o endereço IP do dispositivo que está utilizando a conexão.

De acordo com Pompei, Queiroz e Stolfi (2023), o protocolo *IP Security* (IPSEC) foi criado com o intuito de garantir segurança aos pacotes do protocolo *IPv6*[5], que é o sucessor do *IPv4*[6], essa segurança é garantida em nível de rede de comunicação. Ele apresenta três tipos de componentes principais: o *Autentication Header* (AH), o *Encapsulating Security Payload* (ESP) e o *Internet Key Exchange* (IKE), responsáveis respectivamente pela verificação de integridade do pacote, criptografia e protocolo de negociação de chaves.

Nesse sentido, sobre o *SSL*, Garcia et al. (2013) diz que o SSL atua entre as camadas de transporte e aplicação de dados. Duas camadas que possuem grande flexibilidade para rodar diferentes protocolos, e além disso, ele provê sigilo e segurança dos dados transmitidos, disponibilizando uma organização de dados para reduzir o tráfego e melhorar o desempenho.

Ademais, Borges, Fagundes e Cunha (2007) conceitua sobre o *Point-to-Point Tunneling Protocol* (PPTP), que foi desenvolvido por um fórum empresarial denominado PPTP Fórum com o intuito de facilitar acesso aos computadores remotos, sendo este o mais utilizado no trabalho *home-office*, também sendo este um dos primeiros protocolos VPN que surgiram e hoje, já é acoplado nativamente no sistema operacional *Windows*, a partir da versão 95 do *software*.

O protocolo VPN utiliza-se da conexão com um ISP e um servidor de conexão *point-to-point protocol* (PPP) para estabelecer conexão com o computador remoto, conectado em uma outra rede de seu interesse. Como por exemplo, um colaborador que possui necessidade de conectar remotamente em um computador localizado na sede da empresa por algum motivo fora de seu turno, ele utilizará deste protocolo, através de aplicativos de terceiros para conexão.

Outro protocolo utilizado em conexão VPN é o *Layer Two Forwarding* (L2F), o qual segundo Borges, Fagundes e Cunha (2007), possui um túnel independente de IP, podendo trabalhar com meios como o *Asynchronous Transfer Mode* (ATM) e *Frame Relay*, tecnologias de autenticação de criptografia para garantir segurança e integridade.

Além disso, o L2F faz utilização do PPP assim como o PPTP com a diferença de que, neste protocolo os usuários remotos podem se autenticar via *Remote Authentication Dial In User* (RADIUS), *Terminal Access Controller Access-Control System* (TACACS e TACACS+).

São protocolos que segundo Moraes (2012) são baseados em tunelamentos de transporte utilizando o *Transmission Control Protocol* (TCP), ambos devem ser utilizados em simultaneidade, sendo o RADIUS para controle de acesso ao switch e o TACACS+, uma atualização do legado TACACS, para controle de comandos de usuários com privilégios de administrador para alterar as configurações do switch de internet.

Contudo, existe o *Layer Two Tunneling Protocol* (L2TP), sendo este a atualização do L2F, que fez a coligação dos protocolos PPTP e L2F, oferecendo flexibilidade e escalabilidade do PPTP, juntamente com a privacidade e segurança do L2F, permitindo a autenticação por ATM e *Frame Relay*.

Este último, de acordo com Borges, Fagundes e Cunha (2007), foi desenvolvido para que suporte dois modos de tunelamento, o voluntário e o compulsório, funcionando do seguinte modo respectivamente: Tendo início da conexão no computador remoto, possuindo flexibilidade para usuários que estão em trânsito, pois os permitem conectar a partir de qualquer ISP, pois o provedor não possui participação nos túneis. Já o compulsório é iniciado pelo servidor, sendo essa a principal diferença entre os túneis. Além disso, o segundo necessita de

[5] *Internet Protocol Version 6*
[6] *Internet Protocol Version 4*

acesso a rede pré-configurada para que sejam relacionadas as terminações de cada túnel, baseando-se nas informações autenticadas pelo usuário.

Em suma, cada protocolo possui sua particularidade para utilização assertiva ,e podem ser combinados para que cada um com sua particularidade, colabore com a melhoria da segurança e da privacidade da conexão, fatores que vão depender do aplicativo que será utilizado para fazer a comunicação VPN.

2.4 APLICATIVOS PARA FAZER A CONEXÃO VPN

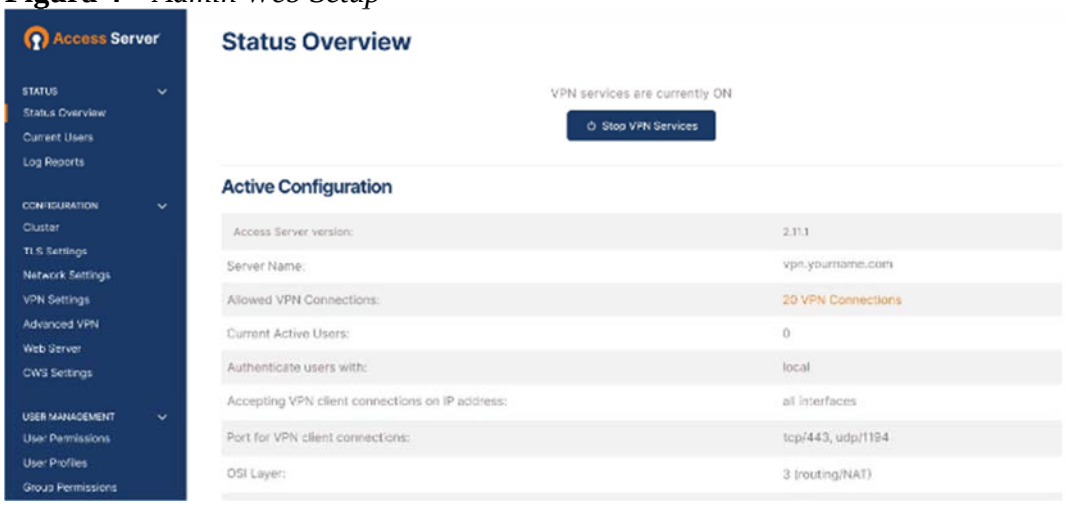
Dois aplicativos muito utilizados para realizar a conexão VPN são o *OpenVPN* e o *Radmin VPN*, cada um utilizado por um público distinto, sendo eles, empresas que querem criar um ambiente controlado para acesso e, pessoas que querem criar uma *LAN*[7] simples para jogos online e transferências de arquivo, respectivamente.

2.4.1 *Open VPN*

Segundo documentação do *OpenVPN*, escrita por Yonan (2018), o aplicativo é uma VPN de código aberto e tem o propósito de ser uma ferramenta VPN universal que oferece grande confiabilidade e flexibilidade ao usuário, suportando protocolos SSL, tunelamento TCP ou *User Datagram Protocol* (UDP), suportando endereços IP dinâmicos e *Dynamic Host Configuration Protocol* (DHCPs), além de possuir portabilidade para outros sistemas operacionais.

É possível configurá-lo através de uma *interface web* disponibilizada pelo próprio software. A interface é intuitiva com cores sóbrias e opções claras de configuração, como n Figura 4:

Figura 4 – *Admin Web Setup*



Fonte: OPENVPN, 2023.

Suas configurações geralmente são feitas através do terminal do sistema operacional, podendo ser tanto *Windows*, quanto *MacOS* ou *Linux*, utilizando o prefixo "—" (dois traços), as quais são disponibilizadas na documentação *online* do *OpenVPN*, como a Figura 5:

[7] *Local Area Network*, no português seria "Rede Local".

Figura 5 – Terminal de configuração do *OpenVPN*

```
#
# Sample OpenVPN configuration file for
# using a pre-shared static key.
#
# '#' or ';' may be used to delimit comments.

# Use a dynamic tun device.
dev tun

# Our remote peer
remote mypeer.mydomain

# 10.1.0.1 is our local VPN endpoint
# 10.1.0.2 is our remote VPN endpoint
ifconfig 10.1.0.1 10.1.0.2

# Our pre-shared static key
secret static.key
```

Fonte: OPENVPN, 2023.

Por fim, assim como um renomado aplicativo de conexão VPN, ele possibilita a configuração de *server-mode* ou *cliente-mode*, fatores que o próprio usuário pode definir. Sendo o primeiro possibilitando com que seu *host* se torne o próprio servidor, que receberá uma conexão externa, por outro lado, a segunda configuração irá definir o *host* como um cliente, o qual apenas fará requisições de conexão em vez de receber.

2.4.2 Radmin VPN

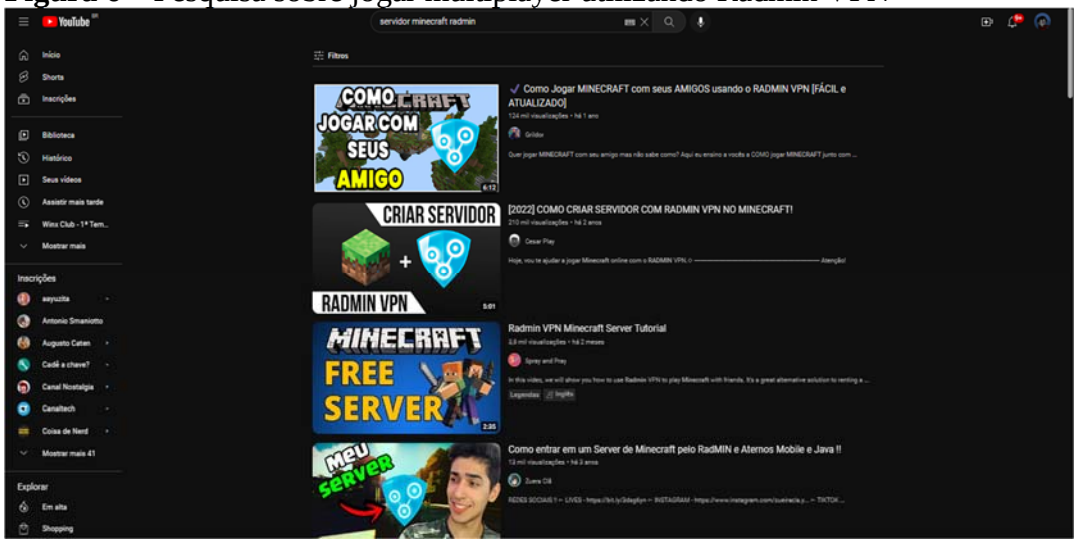
Em primeira instância, é necessário entender a utilização do Radmin VPN. Segundo sua documentação oficial, sua aplicação é simples e intuitiva, além de ser gratuita e flexível, podendo ser utilizada para criação de redes *LAN*, possibilitando jogar jogos *online*, criar túneis de transferência de arquivos e até mesmo trabalhar remotamente, utilizando-se de conexão remota a outra rede ou computador.

Algumas de suas vantagens são sua gratuidade, ou seja, é uma aplicação gratuita, livre de quaisquer custos para sua utilização. Sua política de não-coleta de logs, sem salvar dados do usuário, sua segurança, pois permite a criação de tuneis com criptografia ponto-a-ponto de 256-bits utilizando protocolo *Advanced Encryption Standard* (AES), suas atualizações automáticas e, sua facilidade de uso.

Entretanto, não é um software para uso corporativo, possuindo grande popularidade e utilização nos cenários dos games, especialmente pelos jogadores do jogo *Minecraft*, o *game* que teve sua maior popularidade nos anos de 2010; consiste em um mundo aberto em que o jogador pode expressar sua criatividade fazendo construções, vilas, casas, castelos, tudo o que quiser com blocos de textura de *16bits*.

A utilização do software pelos jogadores de Minecraft consiste na criação de redes *LAN*, para que, os *players* possam entrar nos jogos uns dos outros, e contribuir para suas construções e criações dentro do *game*, como é mostrado na Figura 6.

Figura 6 – Pesquisa sobre jogar multiplayer utilizando Radmin VPN



Fonte: Elaborado pelos autores.

Em suma, sua utilização profissional é mínima, fato que fora comprovado com a pesquisa deste trabalho. Tal fator acontece devido a sua segurança que também é mínima, sendo utilizada somente para tarefas básicas que não envolvem vazamento de dados sensíveis ou que não necessitem de alta segurança como um aplicativo bancário ou acesso ao banco de dados de uma empresa.

2.5 O AUMENTO DA PRODUTIVIDADE DOS COLABORADORES COM O *HOME-OFFICE*, POSSIBILITADO PELAS VPNS

O trabalho remoto, ou como ficou conhecido nos últimos anos como *home-office*, teve sua alta durante a pandemia do Sars-CoV-2, vírus que causou a pandemia da Covid-19, que segundo a Organização Mundial da Saúde (OMS) durou de 11 de março de 2020, até meados de 2022, com efeitos que perduram até os dias atuais.

Segundo pesquisa realizada pela Unicamp, dirigida por Bridi et al. (2020), com o intuito de verificar as condições de adaptação dos brasileiros ao modelo de teletrabalho/*home-office* durante a pandemia da Covid-19, foi verificado que 25,05% tiveram um aumento de meta de produtividade no período da pandemia.

Outros fatores que devem ser destacados, são os pontos positivos que os participantes relataram, sendo eles, a flexibilidade de horários, deslocamento e menor preocupação com a aparência, no geral, 48% relatam fatores tanto positivos quanto negativos. Já os pontos negativos relatados são a falta de interação com colegas de trabalho, mais interrupções e dificuldade de separar o pessoal do profissional.

Por fim, cabe ressaltar que 40,29% dos profissionais entrevistados afirmam que preferem continuar no modelo de home-office após a pandemia, fator que perdurou e pode ser comprovado com as atuais divulgações de vagas de emprego; antes, anúncios de vagas em regime *home-office* eram poucos divulgados, hoje em dia são muito mais e representam o sonho de muitas pessoas, principalmente dos profissionais da área de tecnologia e informação (TI).

3 METODOLOGIA

Para o desenvolvimento do artigo em questão, inicialmente foi conduzido levantamento de informações em livros, sites de empresas de renome nacional etc. Levando em consideração

conceitos em torno de VPNs, como elas funcionam, como garantem um ambiente controlado seguro e o aumento da produtividade pelo *home-office* possibilitado pela aplicação das VPNs.

Sendo assim, com o objetivo de compreender melhor como as empresas da área da Tecnologia da Informação, dentre elas, empresas de desenvolvimento, suporte, provedores de rede e agências de marketing digital, do noroeste paulista entendem como conceito de VPNs e seu método de aplicação possuem determinada importância. Fora conduzida uma pesquisa on-line, feita por meio da ferramenta “Google Forms”, no período de 27/03/2023 a 06/04/2023, período resultando na coleta de 50 respostas.

A pesquisa conduzida, fora de caráter quantitativa para compreender quantas empresas fazem utilização do protocolo, o meio para aplicação da VPN, seu objetivo por parte das empresas e qual o grau de importância atribuído a cada respectiva empresa ao protocolo citado.

A aplicação da pesquisa fora feita no público-alvo, utilizando aplicativos como o *WhatsApp* para comunicação das empresas dos ramos citados anteriormente, a fim de coletar dados concretos de acordo com o tema do trabalho proposto

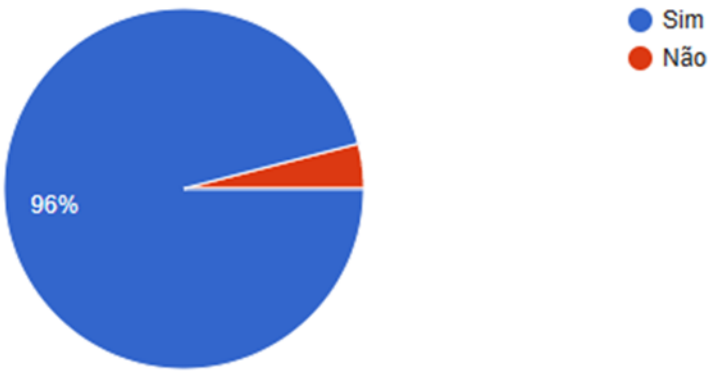
Por fim, a pesquisa aplicada contou com 06 (seis) perguntas, dentre as quais podem-se destacar: “Você sabe o que é uma VPN?”, “Você utiliza VPN em sua empresa?” Se sim, por quê?”, “Se não utiliza, por quê?” e “Se você utiliza de um software para fazer a ligação VPN, indique qual:”.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Nessa seção, são apresentadas as análises dos resultados coletados com a pesquisa citada na seção anterior, a qual contou com 50 respostas. A pesquisa foi conduzida com o intuito de entender se as empresas do noroeste paulista sabem do que a VPN se trata, se fazem sua utilização, se não fazem e qual aplicativo utilizam para fazer a conexão da forma que melhor atenda a demanda de seu negócio.

Inicialmente, foi abordada se as empresas entrevistadas possuem conhecimento sobre a VPN, se elas sabem o que é uma VPN, como mostra o Gráfico 1.

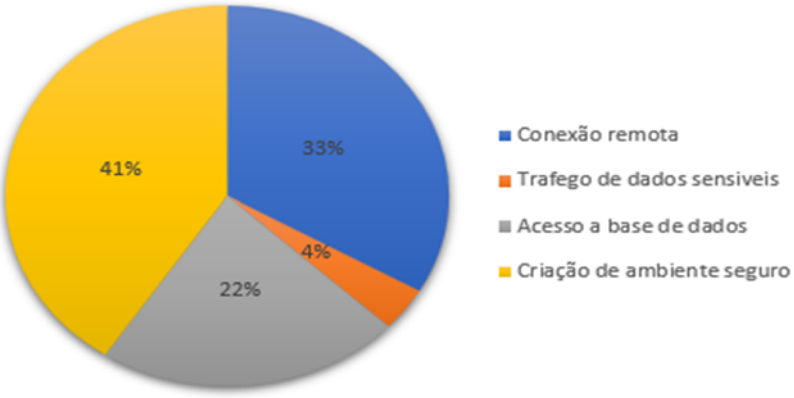
Gráfico 1 – Conhecimento sobre VPN nos correspondentes



Fonte: Elaborado pelos autores.

Com isto, os participantes que assinalaram que sabem o que é uma VPN, descreveram quais atividades utilizam a ferramenta em suas empresas. As 27 respostas coletadas foram: Criação de ambiente seguro (41%), Conexão remota (33%), Acesso a base de dados (22%) e Tráfego de dados sensíveis (4%), assim como pode ser observado no Gráfico 2.

Gráfico 2 – Utilização da VPN nas empresas

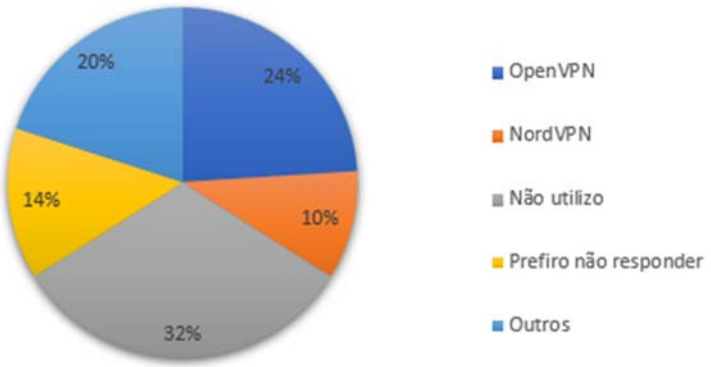


Fonte: Elaborado pelos autores.

Entretanto, é necessário entender o motivo pelo qual os entrevistados não fazem a utilização da VPN nas empresas, visto que a maioria tem ciência do que se tratam estes protocolos, fator que foi abordado no Gráfico 1. Sendo assim, recebem destaque os motivos de "Não há necessidade", "Não há interesse dos superiores" e "Não conheço muito bem a tecnologia", sendo que em sua maioria, os respondentes são empresas de desenvolvimento de software, organizações que deveriam em tese serem as mais preocupadas com segurança em seu funcionamento.

Ademais, o software utilizado é de extrema importância para o bom funcionamento e aplicação dos protocolos VP. A escolha requer que fatores diversos sejam levados em conta e que seja feita uma análise minuciosa do objetivo da aplicação dos protocolos e, de acordo com o Gráfico 3, pode-se notar que a maior parcela dos entrevistados faz uso dos dois maiores softwares de VPN do mercado na atualidade, sendo eles o OpenVPN (24%) e o NordVPN (10%). Contudo, 14% dos entrevistados preferem não expor qual software é utilizado pela organização, por motivos de privacidade.

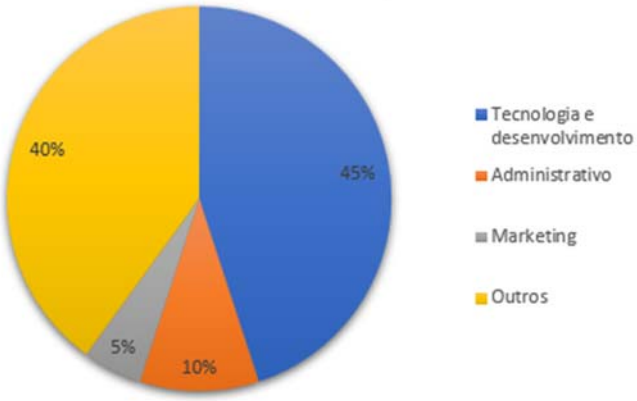
Gráfico 3 – *Software* para ligação VPN



Fonte: Elaborado pelos autores.

Com isso, para melhor descrever o perfil dos entrevistados, foi abordado o ramo da empresa em que a pesquisa foi aplicada. Pode-se verificar no Gráfico 4, que as principais respondentes foram as empresas dos ramos de Desenvolvimento de *Software* (20%), Administrativo (10%) e de Marketing (6%).

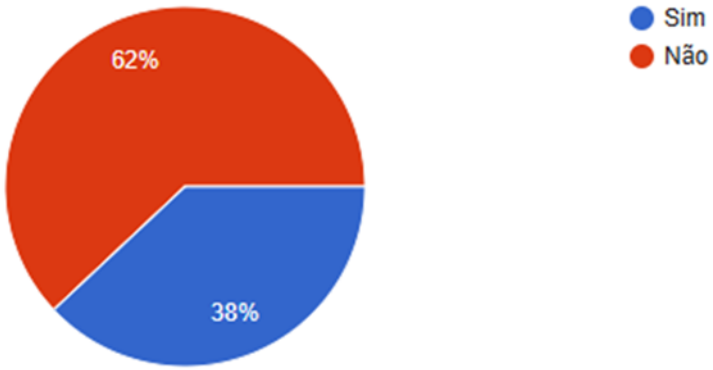
Gráfico 4 – Ramo das empresas entrevistadas



Fonte: Elaborado pelos autores.

Neste sentido, é necessário entender se as empresas entrevistadas lidam com algum dado sensível, os quais são definidos de acordo com a LGPD (2019) como dados biométricos, que tenham ligação com raça, cor, religião, sexualidade, dados médicos, de pagamento entre outros. Segundo o Gráfico 5, é constatado que a maioria dos entrevistados (62%) não lidam com dados sensíveis.

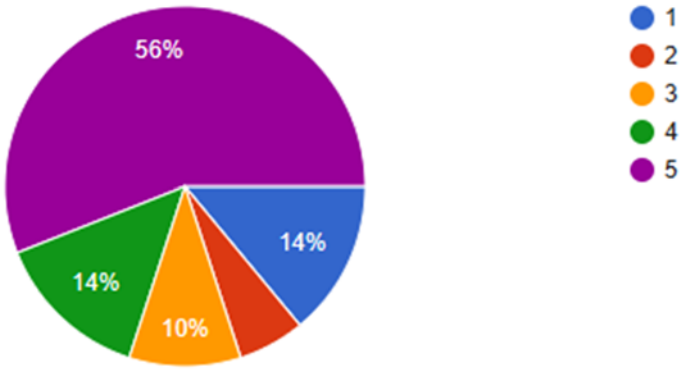
Gráfico 5 – Empresas que lidam com dados sensíveis



Fonte: Elaborado pelos autores.

Por fim, com o objetivo de compreender a consideração da importância da VPN para os entrevistados, foi questionado qual a importância para eles, em uma escala de 1 a 5, sendo 1, totalmente dispensável e 5, indispensável. Pode-se constatar utilizando o Gráfico 6, que a maioria dos entrevistados (56%) consideram a VPN indispensável, enquanto apenas 14% a consideram totalmente dispensável.

Gráfico 6 – Importância da utilização da VPN



Fonte: Elaborado pelos autores.

5 CONSIDERAÇÕES FINAIS

Inicialmente, o intuito de desenvolvimento desta pesquisa foi demonstrar a utilização da VPN nas empresas com foco em segurança e *home-office,* fatores que tomaram importância e proporções gigantescas no mundo durante e pós a pandemia da Covid-19, mostrando a VPN como opção segura para a resolução dos problemas de segurança e migração para o *home-office*.

Em suma, é de extrema importância pontuar que por mais que os respondentes do questionário possuam conhecimento sobre a ferramenta, saibam de sua aplicação e benefícios, seu uso é negligenciado, pois, ao analisar os Gráficos 1 e 6, nota-se que a maioria massiva dos participantes sabem do que se trata e consideram o protocolo importante, sendo assim, confirmando o intuito da pesquisa e deste trabalho.

Tal fato é preocupante, pois em um mundo pós pandêmico, com a tecnologia em maior expansão que nunca, negligenciar a segurança de uma empresa seria, em uma simples analogia, como um médico negligenciar um eletrocardiograma ou um exame de sangue em um pré-operatório, exames que mostram a saúde do coração e coagulação do sangue do paciente, demonstrando que as empresas correm perigo de terem seus sistemas invadidos, além de terem seus dados e de seus clientes expostos, fatores que podem comprometer seu funcionamento por completo.

Ao final, pode-se concluir que a aplicação da pesquisa atingiu seu objetivo final em elucidar essa negligência com a segurança, por mais que as pessoas saibam sobre prevenção. Os trabalhos de regime *home-office* no mundo pandêmico e pós-pandêmico tendem a crescer e por isso, espera-se com este trabalho, incentivar e alertar sobre a aplicação das VPNs para criação de conexões seguras, principalmente em ambientes empresariais, mas também em ambientes residenciais.

REFERÊNCIAS

BALLESTEROS, H. M. S. **VPN, Virtual Private Network**. Disponível em: https://www.gta.ufrj.br/grad/08_1/vpn/tiposarq.html. Acesso em: 13 abr. 2023.

BORGES, F.; FAGUNDES, B. A.; CUNHA, G. N. **VPN**: protocolos e segurança. 2007. Disponível em: https://www.lncc.br/~borges/doc/VPN%20Protocolos%20e%20Seguranca.pdf. Acesso em: 15 jun. 2023.

BRANCO, D. C. **Como funciona uma VPN?** 2021. Disponível em: https://canaltech.com.br/seguranca/como-funciona-uma-vpn-200530/. Acesso em: 1 dez. 2022.

BRIDI, M. A *et al*. **O trabalho remoto/home-office no contexto da pandemia COVID-19**. 2020. Disponível em: https://www.eco.unicamp.br/remir/images/Artigos_2020/ARTIGO_REMIR.pdf. Acesso em: 25 abr. 2023.

BUXTON, O. **VPN com Kill Switch**: o que é e como funciona? 2021. Disponível em: https://www.avg.com/pt/signal/what-is-a-vpn-kill-switch. Acesso em: 15 jun. 2023.

FUNDAÇÃO OSWALDO CRUZ – FIOCRUZ. **Por que a doença causada pelo novo coronavírus recebeu o nome de Covid-19?** 2020. Disponível em: https://portal.fiocruz.br/pergunta/por-que-doenca-causada-pelo-novo-coronavirus-recebeu-o-nome-de-covid-19#:~:text=Compartilhar%3A,que%20%C3%A9%20o%20novo%20coronav%C3%ADrus%3F. Acesso em: 15 jun. 2023.

GANDRA, A. **Trabalho em home office tende a continuar após fim da pandemia**: empresas avaliam que teletrabalho trouxe benefícios para todos. 2021. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2021-04/trabalho-em-home-office-tende-continuar-apos-fim-da-pandemia#:~:text=Favorabilidade,l%C3%ADder%20do%20programa%20Jornada%20Vale. Acesso em: 3 nov. 2021.

GARCIA, D. R. *et al*. **Redes Virtuais Privadas e IPsec**. 2013. Disponível em: https://www.gta.ufrj.br/grad/13_1/vpn_ipsec/index.html. Acesso em: 1 dez. 2022.

KASPERSKY. **O que é uma VPN e como funciona?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn. Acesso em: 30 nov. 2022.

MICROSOFT. **98% das MPMEs em transformação digital reconhecem o impacto positivo da tecnologia nos negócios**. 2023. Disponível em: https://news.microsoft.com/pt-br/98-das-mpmes-em-transformacao-digital-reconhecem-o-impacto-positivo-da-tecnologia-nos-negocios/. Acesso em: 23 mar. 2023.

MORAES, A. M. S. P. **RADIUS e TACACS+**: dois protocolos complementares. 2012. Disponível em: https://alexandremspmoraes.wordpress.com/2012/01/09/a-velha-discussao-sobre-radius-e-tacacs/. Acesso em: 18 abr. 2023.

NAKAMURA, E. T. *et al*. **Análise de segurança do acesso remoto VPN**. 2016. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Estadual de Campinas, Campinas, 2016.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR – NIC.br (ed.). **Privacidade e proteção de dados pessoais**: Perspectivas de indivíduos, empresas e organizações públicas no Brasil 2021. São Paulo: CGI, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 3 nov. 2022.

OLIVEIRA, A. **O que é Rede Virtual Privada (VPN) e vantagens na utilização por empresas**. 2020. Disponível em: https://www.profissionaisti.com.br/o-que-e-rede-virtual-privada-vpn-e-vantagens-na-utilizacao-por-empresas/. Acesso em: 23 mar. 2023.

POMPEI, L. S.; QUEIROZ, R. T.; STOLFI, R. O. **Segurança em VPN**. Disponível em: https://www.ic.unicamp.br/~rdahab/cursos/mp202/Welcome_files/trabalhos/VPN/texto/Texto%20(.html).html. Acesso em: 18 abr. 2023.

SIQUEIRA, M. A.; CASTRO, M. C.; NAKAMURA, E. T. Análise dos aspectos de segurança das VPNs MPLS. *In*: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS – SBSEG, 3., 2003, Natal. **Anais eletrônicos**[...]. Porto Alegre: Sociedade Brasileira de Computação, 2003. p. 88-95. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/21254/21079. Acesso em: 18 abr. 2023.

YONAN, J. **Reference manual for OpenVPN 2.4**. 2018. Disponível em: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/. Acesso em: 18 abr. 2023.