A SEGURANÇA DA INFORMAÇÃO EM 2021:
Avaliação das mudanças na infraestrutura de tecnologia para o trabalho à distância nas regiões da Zona da Mata e Sul de Minas Gerais

Guilherme Marcolino de Oliveira
Alberane Lúcio Thiago da Cunha

RESUMO

Com a chegada da pandemia do Covid - 19 ao Brasil em 2020, as empresas se depararam com um cenário de inúmeras incertezas quanto à forma de atuação e produção. Para que fosse possível a continuidade dos negócios, fez-se necessária uma adaptação e adequação da estrutura de tecnologia da informação, que, em muitas empresas, era inexistente. Diante disto, o objetivo deste trabalho é identificar as mudanças que foram realizadas para a migração ao trabalho remoto, numa visão mais específica em relação a segurança do tráfego de dados entre empresas e colaboradores na estrutura de home office nas regiões da zona da mata e Sul de Minas Gerais. Os resultados da pesquisa demonstram um aumento nos investimentos em infraestrutura, todavia há uma falta de preparo e treinamento aos usuários que o utilizam.

Palavras-chave: Covid-19; home office; segurança da informação.

1 INTRODUÇÃO

Em razão ao distanciamento social causado pela COVID-19, a proteção de dados e a segurança da informação se tornaram vulneráveis. Empresas e pessoas tiveram que se adequar rapidamente ao trabalho remoto, necessitando uma mudança de logística de pessoal, dispositivos e outros equipamentos, este processo levou muitas empresas a sofrerem ataques e violações aos seus dados (BARBOSA et al., 2021).

Este artigo traz uma análise das mudanças na infraestrutura de segurança da informação para o trabalho à distância nas médias e grandes empresas nas regiões da Zona da Mata e Sul de Minas Gerais, buscando demonstrar que, apesar crescimento nos investimentos em busca por adequações no sistemas de segurança de dados ao longo de quase

*Graduando em Sistemas de Informação pelo Centro Universitário do Sul de Minas (UNIS-MG) - ktagmo@gmail.com
*Especialista em Engenharia de Sistemas (ESAB), Especialista em Metodologias Ativas e Graduado em Tecnologia da Informação (Unis/MG) - alberanelucio@gmail.com

2 anos desde o início da pandemia, a falta de segurança da informação ainda se mostra como um dos maiores riscos aos ativos da empresas.

Este questionamento faz-se necessário para que seja compreendido se o aumento na busca por segurança, visto neste período após o início da pandemia do COVID-19, tem correlação com a migração dos funcionários para o trabalho remoto, e ainda demonstrar quais foram as mudanças sofridas pelo setor para o aumento na segurança do tráfego de dados.

O intuito deste trabalho é entender se a migração para o trabalho remoto impactou a infraestrutura de segurança da informação e neste caso quais foram estas mudanças.

Esta resposta será obtida através de pesquisas bibliográficas e questionários. Na pesquisa bibliográfica foi realizado um apanhado de referências teóricas publicadas por meio de publicações eletrônicas, tais como: livros, artigos científicos e páginas de web sites, buscando ampliar o conhecimento sobre o tema abordado, e no questionário, foi realizada uma pesquisa direcionada a profissionais ligados à área de segurança e infraestrutura de TI das empresas, desenvolvido por meio da escala Likert que se utiliza de cinco opções de resposta (concordo totalmente, concordo, neutro, não concordo, discordo) para a obtenção de dados.

2 REVISÃO DA LITERATURA

Em se tratando de sistemas computacionais, informações e dados se distinguem, onde dados se resumem a elementos ainda não processados e informação é o resultado do processamento desses dados pelo computador.

Sendo assim, compreende-se informação como sendo parte do patrimônio de uma empresa, em outras palavras, algo de alto valor e de fundamental importância para as atividades da empresa e por isso deve ser protegido. Dada essa necessidade de proteção, originou-se a segurança da informação, a qual se atém em proteger a informação de vários tipos de ameaças, para garantir a interruptibilidade dos negócios e reduzir os riscos, permitindo o maior lucro possível. (GALVÃO, 2015).

O princípio da segurança física e lógica compreende a exigência de que os dados estejam protegidos contra desvios ,danos e falhas ou alterações não autorizadas (DONETA, 2006).

A segurança da informação se baseia em quatro princípios básicos para que se possa garantir sua efetividade, são eles:

- Disponibilidade: a informação estará sempre disponível, quando assim for solicitada. Essa característica é de suma importância, principalmente para alguns serviços que demandam 100% do tempo, como por exemplo sites de varejo.
- Integridade: a informação só poderá ser editada ou alterada por quem for autorizado a tal ação, esta é obtida através de um controle de alterações.
- Confidencialidade: a informação só poderá ser acessada pela pessoa autorizada, isto diz respeito ao sigilo da informação. Logo, a confidencialidade assegura o sigilo da informação e impossibilita que pessoas não autorizadas tenham acesso à determinada informação. Esta pode ser obtida através de criptografia.
- Autenticidade: garante a genuinidade da autoria da informação, a autenticidade garante a veracidade do usuário que editou, não importando se o conteúdo é verdadeiro ou falso.

Além dos princípios básicos temos ainda um outro contexto a ser analisado: a classificação da informação levando em conta o seu grau de importância. Ainda, segundo (GALVÃO, 2015), não existe uma padronização que possa ser adotada para todas as instituições, pois cada uma possui características diferentes e específicas ao seu setor e ramo de trabalho. Todavia, é comum que a maioria das empresas privadas utilizem os seguintes graus de classificação: confidencial, privada, sigilosa e pública. Já no setor público, por conseguinte, há uma legislação distinta. De acordo com o Decreto n. 7.724/2012, no art. 26, *"a informação em poder dos órgãos e entidades públicas [...] poderá ser classificada no grau ultrassecreto, secreto ou reservado"*(BRASIL, 2012).

Atualmente, influenciadas pelo advento da globalização, novas conformações sociais, econômicas e tecnológicas, as quais culminaram em profundas alterações na forma de se trabalhar. Segundo Rafalski e Andrade (2015), são exemplos dessas modificações a flexibilização da produção, a terceirização da mão de obra, a produção *just-in-time* (buscar a precisão da cadeia de produção, encaixando as operações e as execuções de acordo

com o nível de demanda), modelos de carreiras com características mais individuais e a maior valorização do capital humano e psicológico no trabalho.

2.1 A segurança da informação em meio à pandemia

Ao longo desses quase 2 anos em que o mundo teve que se adaptar para superar as consequências da COVID - 19, a preocupação com a segurança se mostrou essencial. Hoje em dia a pergunta que deve ser feita por qualquer empresa não é mais "se" haverá uma tentativa de invasão, mas "quando", pois desde pequenas empresas até grandes conglomerados multinacionais tem sido alvo de invasões, sequestro e vazamentos de dados.

Segundo o site Tecmundo (2021) o Brasil está entre os 10 países que mais sofreram com ataques e tentativas de invasão em todo o mundo. Durante os três primeiros meses de 2021, o Brasil liderou o ranking latino de ataques cibernéticos, alvo de 3,2 bilhões de tentativas de ataques. O número corresponde a quase 50% das 7 bilhões de tentativas registradas em toda a América Latina.

Uma pesquisa realizada pela PwC em 2021 feita com 3.249 executivos de negócios e tecnologia em todo o mundo, mostrou que o investimento em cibersegurança sofreu um grande crescimento após o início da pandemia e tem se mostrado um atrativo para investidores que buscam segurança em seus investimentos, se tornando um atrativo para empresas que buscam o crescimento.

2.2 Ameaça x Segurança

A Segurança da informação só existe, pois em algum momento houve um risco ou ameaça que pudesse infligir dano a este ativo. Ainda que, por muito tempo e ainda por muitas instituições, a segurança não tenha a importância adequada, todos de alguma forma implementam softwares ou aplicações para que, mesmo de forma inadequada, minimamente haja a "sensação" de segurança.

Segundo Galvão (2015), a ameaça pode ser entendida como sendo todo e qualquer fator capaz de, porventura, ocasionar um incidente ou problema que possa lesar uma organização ou pessoa de alguma forma.

Segundo o jornal Estadão (2020), com a crise causada pela pandemia, diversas empresas adotaram, de forma urgente, o trabalho remoto, culminando em riscos maiores para aqueles que não possuíam políticas e regras de diretrizes bem definidas. Questões como processos adequados que envolvam segurança da informação durante a pandemia são de vital importância.

Levando em consideração o atual cenário, decorrente da pandemia de 2021, pode-se ver o quão despreparadas e desprotegidas as empresas estavam. Muitas organizações tiveram que se adaptar e implementar novas formas de ampliar a segurança, e cada gestor de sistemas teve a necessidade de se adaptar e gerenciar um novo cenário, o dito home office, forma de trabalho pela qual o funcionário exerce suas funções a distância, fazendo o uso de meios computacionais para atuar junto à empresa, substituindo sua presença física. A utilização de meios como Whatsapp, redes sociais e e-mails pessoais se tornaram alternativas para a transmissão de informações sensíveis, meios aos quais foram utilizados para invasões e roubo de informações (ESTADÃO, 2020).

Cada integrante do sistema, seja ele ligado diretamente à segurança, analista de sistemas e demais especialistas ligados à segurança da informação, ou então o próprio usuário, aquele que se utiliza dos dados processados para obter uma informação e com ela obter valor, tem a necessidade de proteger a informação. Para readequação dos sistemas de Segurança da Informação) houve a procura, por parte das organizações, por ferramentas que oferecessem privacidade e segurança aos dados trafegado entre redes privadas, dentre essas ferramentas será citada a que hoje se tornou a de maior relevância, a VPN “Virtual Private Network”, em português, Rede Privada Virtual.

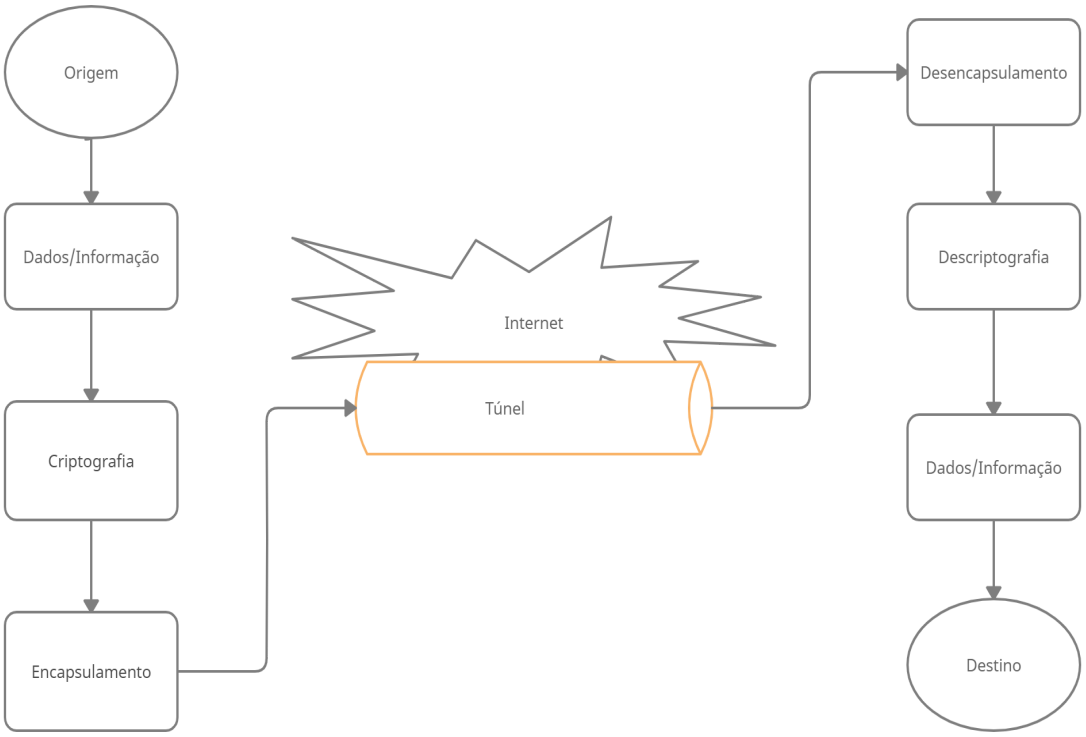
2.2.1 Redes VPN

Segundo Kaspersky (2021), se um usuário necessita trabalhar de forma remota, pode necessitar de acesso a arquivos essenciais na rede de sua empresa. Por motivos de segurança, para o tráfego deste tipo de informação é necessária uma conexão segura. Para se obter acesso à rede de forma segura, na maioria dos casos é utilizado uma conexão VPN. Os serviços de VPN se conectam a servidores privados e usam métodos de criptografia e princípios de segurança da informação para evitar o risco de vazamentos de dados.

Se uma organização possui algumas filiais, e todas necessitam estar interconectadas, há algumas possibilidades, porém o mais empregado é a utilização de uma VPN. Outro exemplo cotidiano do emprego de VPN é o de funcionários que necessitam viajar com muita frequência, ou que operam a distância (home office), e que necessitam de uma conexão que ofereça segurança e privacidade para executar suas funções (GALVÃO, 2015).

Para que haja uma estrutura de intercomunicação é necessário que existam dois pontos, que aqui são denominados origem e destino. Segundo Percília (2006), uma máquina que neste cenário iremos denominar "origem", envia o dado ou informação, o mesmo passa pelo processo de cifragem (criptografia), a seguir ele é encapsulado. O encapsulamento oculta os detalhes de execução do dado e o que resta visível é a sua interface, em outras palavras, o conjunto de todas as mensagens a que ele pode responder. Neste próximo passo entra a maior diferença, o tunelamento, processo que coloca cada pacote de dados dentro de outro pacote, criando uma espécie de envoltório no mesmo. A decodificação, apenas pode ser realizada pelo emissor e pelo receptor, em seguida o dado é desencapsulado, descriptografado sobrando apenas o dado que é entregue ao destinatário. Na figura 1 podemos ver um esquema que exemplifica o que foi relatado:

Figura 1 - Funcionamento VPN



Fonte: (O autor).

É de fundamental importância que uma VPNs não funcione como um software antivírus, apesar de proteger o seu IP e criptografar seu histórico de internet, uma conexão VPN não protege seu computador de possíveis invasões externas. Para tal, devemos utilizar um software antivírus, pois utilizar VPN por si só não o protege de Trojans, vírus, bots ou outros malwares (KASPERSKY, 2021).

2.3 Ataques e Invasões na pandemia do COVID-19

Em Minas Gerais, segundo a polícia civil, o número de cibercrimes teve um aumento de quase 50% em 2020 em comparação a 2019. Ainda segundo dados da polícia civil, de janeiro a maio de 2020, foram registrados 3070 casos de cibercrimes, um crescimento de aproximadamente 25% em relação ao mesmo período do ano anterior (Jornal Daqui, 2020).

Ademais, em uma pesquisa realizada pelo Instituto FSB, realizada com grandes e médias empresas, demonstrou que 68% das indústrias ouvidas pela pesquisa afirmaram que aumentaram seus investimentos em segurança da informação (EXAME, 2021).

O estudo global Índice de Gerenciamento de Acesso de 2021, da Thales, demonstrou que 61% dos entrevistados relataram que as ferramentas tradicionais de segurança, como as redes VPN, ainda são a principal forma de acesso remota oferecida aos colaboradores, apesar da dificuldade na escalabilidade e dos riscos (CANAL TECH, 2021).’

3 MATERIAL E MÉTODOS

Como o objetivo da pesquisa é trazer a realidade dos cenários de implementação e utilização de aplicações objetivando o aumento na segurança da informação após o impacto social trazido pela pandemia, foi realizada uma pesquisa através de um questionário (Apêndice I). O objetivo da aplicação desse questionário é a obtenção de dados para a verificação das mudanças e adequações que as empresas tiveram que fazer para a migração ao trabalho remoto. O questionário foi elaborado e realizado por meio do Google Forms e enviado para instituições e empresas das regiões da Zona da Mata e Sul de Minas Gerais.

As questões foram construídas a partir da escala Likert, onde as opções de resposta apresentam uma afirmação auto-descritiva, por meio de uma escala composta por extremos como “concordo totalmente” e “discordo totalmente”. As empresas pesquisadas têm sede nas regiões da Zona da Mata e Sul de Minas Gerais e são de médio e grande porte. Os questionários foram respondidos pelos responsáveis ou funcionários ligados à área de tecnologia da informação, em um total de trinta e seis participantes.

Por fim, através da análise dos dados obtidos, será demonstrado como este novo cenário social tem impactado na inovação e trazido mudanças na forma de tráfego de dados.

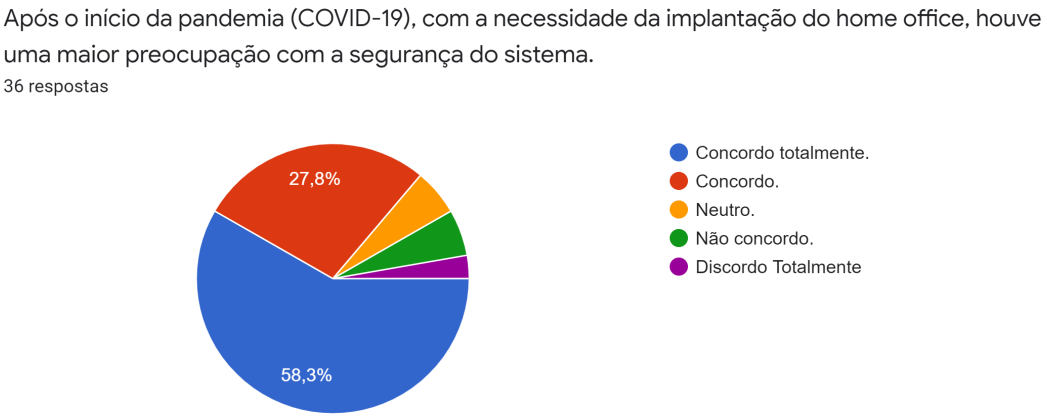
4 RESULTADO E DISCUSSÃO

A pesquisa foi realizada sob o critério de uma escala denominada Likert, onde é apresentada uma afirmação ou uma frase relacionado com a questão a ser tratado e os participantes respondem através de 5 opções e são elas: concordo totalmente, concordo, neutro, não concordo, discordo. Para manter o anonimato, não foram envolvidos nomes ou qualquer dado que identifique o entrevistado, limitando-se apenas às questões pertinentes ao objetivo do artigo, além de cargo e cidade para maior fidelidade dos resultados.

A pesquisa contou com profissionais de diversos cargos e profissões, sendo em sua maioria analistas de sistemas e consultores de TI atuando em diversas cidades da área abrangida pela pesquisa, tendo 50% dos entrevistados pertencendo à cidade de Varginha-MG.

Os resultados obtidos demonstram uma realidade em que a preocupação com a segurança aumentou, onde 86,1% dos entrevistados concordam com esta questão (Gráfico 1).

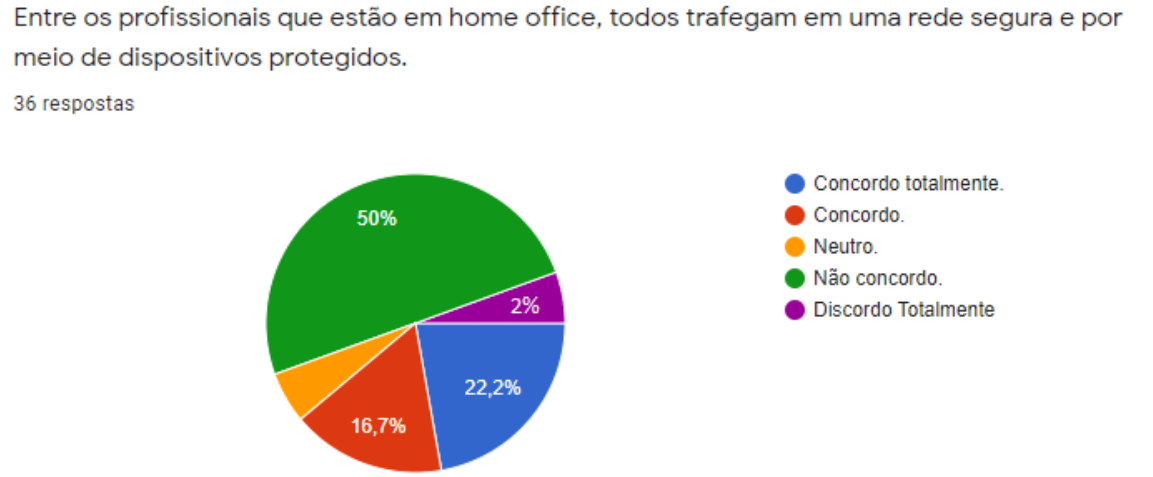
Gráfico 1 - Pesquisa



Fonte: (O autor).

Apesar desse crescimento na busca por segurança, 52% acredita que os colaboradores não utilizam soluções de segurança para o tráfego de dados, como é demonstrado no gráfico a seguir:

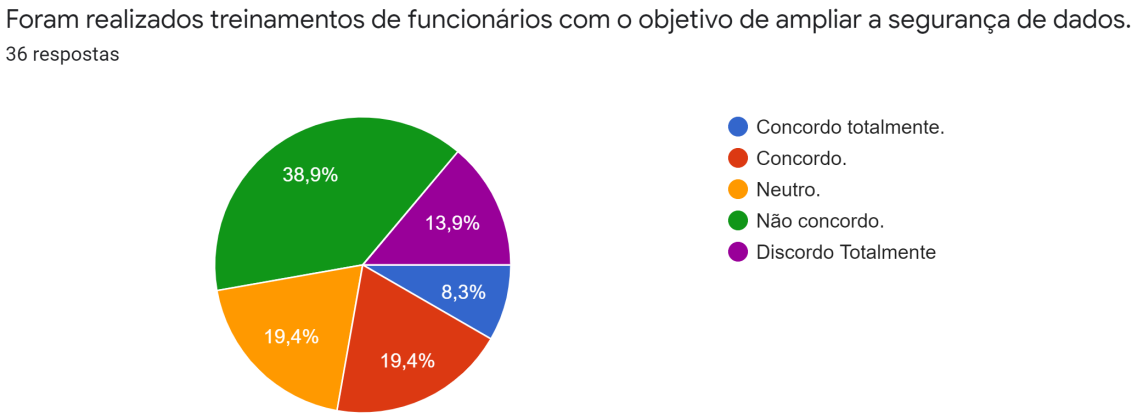
Gráfico 2 - Pesquisa



Fonte: (O autor).

A pesquisa demonstrou ainda que, embora o investimento em infraestrutura visando a segurança esteja em alta, algumas questões, principalmente relacionadas aos usuários, foram colocadas em segundo plano. Treinamentos para a conscientização e operabilidade dos sistemas empregados não foram bem aplicados, como demonstra os resultados:

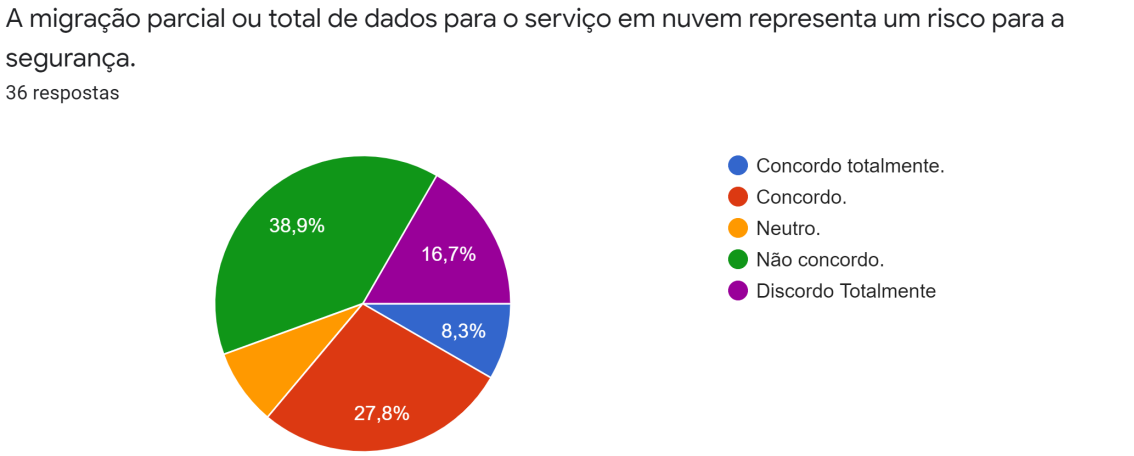
Gráfico 3 - Pesquisa



Fonte: (O autor).

A maioria dos entrevistados admite que uma migração para a utilização de serviços de backup em nuvem representa um ganho significativo para a segurança de dados.

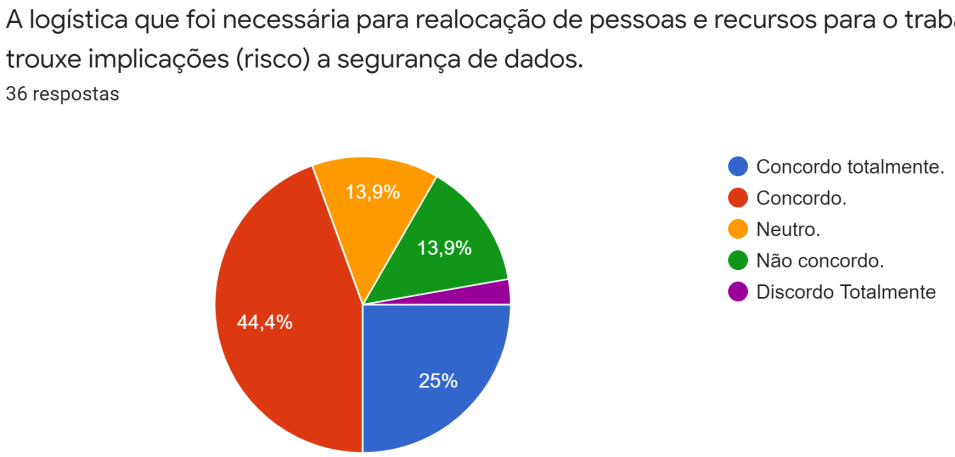
Gráfico 4 - Pesquisa



Fonte: (O autor).

Se tratando da logística necessária para a adaptação e migração para o trabalho home office, esta trouxe prejuízos à segurança da informação, onde 69,4% dos participantes acredita nesta afirmação, como demonstra o gráfico a seguir:

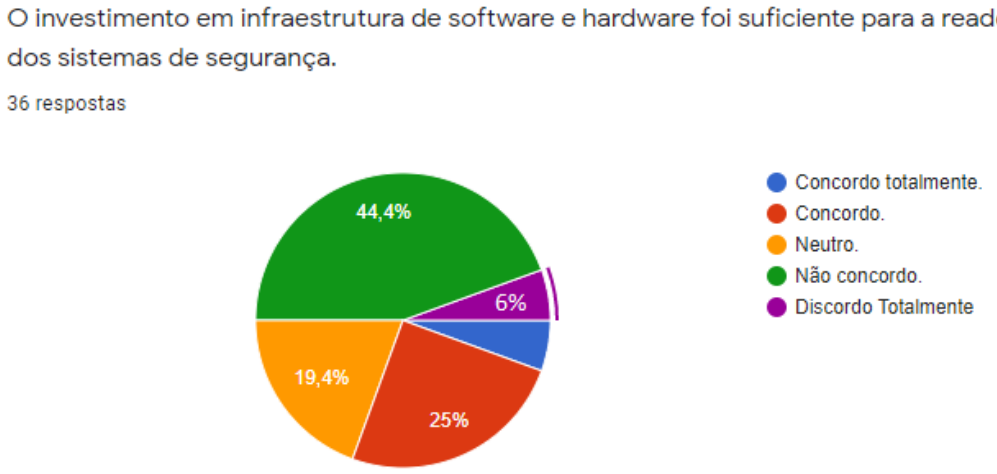
Gráfico 5 - Pesquisa



Fonte: (O autor).

E mais adiante, podemos ver que, por mais que o investimento em segurança tenha aumentado, a falta ou inexistência dela era tamanha que os investimentos foram insuficientes para suprir a demanda existente, conforme demonstrado no gráfico adiante:

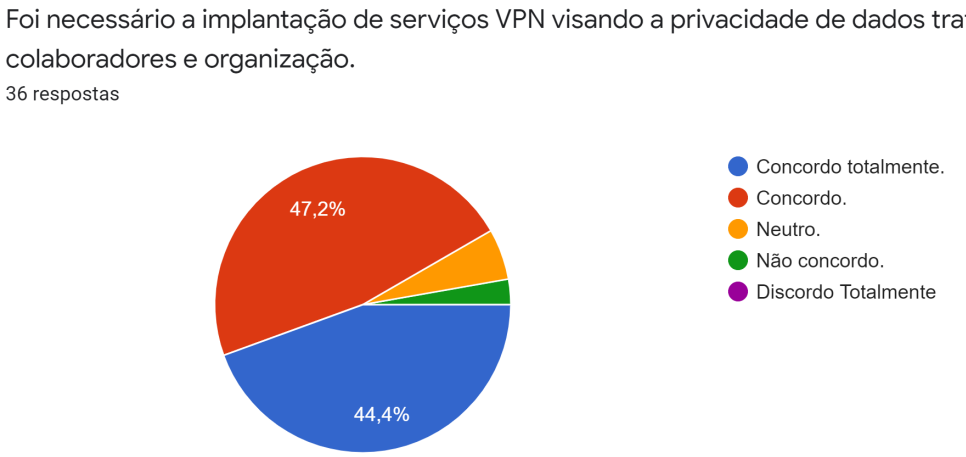
Gráfico 6 - Pesquisa



Fonte: (O autor).

Em se tratando de soluções empregadas para suprir a falta de segurança, 91,6% dos entrevistados afirmam que utilizaram redes VPN (Gráfico 7 - Pesquisa).

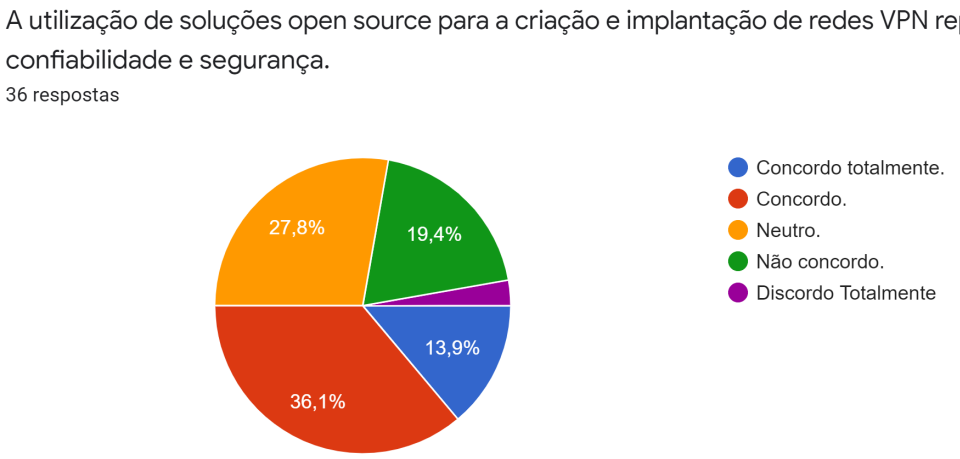
Gráfico 7 - Pesquisa



Fonte: (O autor).

Pode-se destacar ainda que apenas apenas 50% acredite que soluções VPN, open source, tragam algum ganho para a segurança (Gráfico 7 - Pesquisa).

Gráfico 8 - Pesquisa

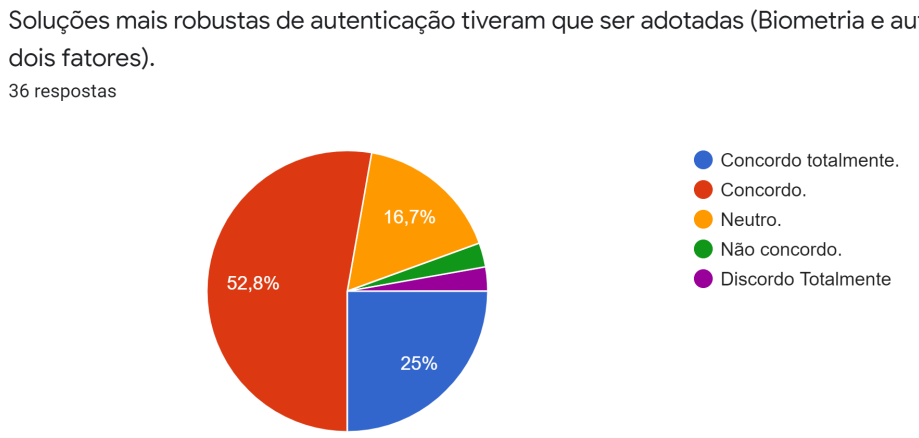


Fonte: (O autor)

A opção neutra tem se mostrado com baixo índice nas outras perguntas e nesta ela se destacou, mostrando um pouco da indecisão, ou desconhecimento em relação à confiabilidade no emprego de soluções open source.

Outras soluções, como a autenticação em dois fatores e o emprego de biometria também estão entre as ferramentas amplamente utilizadas nas empresas para a garantia de autenticidade no tráfego de dados 52,8% e 25% dos entrevistados (Gráfico 9- Pesquisa) concordam ou concordam totalmente, respectivamente.

Gráfico 9 - Pesquisa



Fonte: (O autor).

5 CONCLUSÃO

O futuro, conforme demonstra a reportagem por Gandra (2021), o trabalho remoto, adotado por grandes empresas por causa da pandemia, tende a permanecer na maioria das companhias, mesmo com uma possível volta à normalidade.

É oportuno relembrar a hipótese inicial da pesquisa que dizia que houve um aumento na procura por segurança da informação em função da necessidade do distanciamento social, levando colaboradores a entrar no regime de home office e empresas a buscarem soluções, como a utilização de redes VPN, para a proteção no tráfego de dados.

A hipótese foi comprovada onde 86,1% dos entrevistados confirmam haver um aumento nos investimentos em infraestrutura de segurança de dados após o início da pandemia do Covid -19 e mais especificamente, se tratando em tráfego de dados, 91,6% relatam utilizarem serviços de VPN para o trabalho remoto. Relacionando esses dados

podemos observar que os investimentos foram direcionados ao emprego de soluções de segurança de dados, que em sua maioria foi adotado a utilização de redes VPN.

Neste momento, a partir de questionários com 36 respondentes, podemos observar que houve um aumento nos investimentos ligados à área de segurança, porém a preocupação se concentrou em sistemas e recursos, deixando em segundo plano quem faz a utilização destes sistemas. Treinamentos para a operação e conscientização foram realizados de forma pouco intuitiva e de forma pouco efetiva , isto quando eram realizados.

Percebe-se que apesar de todos os esforços e investimentos, os recursos humanos (usuários) ainda são o ponto de maior insegurança do sistema.

INFORMATION SECURITY IN 2021:

Assessment of changes in technology infrastructure for distance work in the Zona da Mata and southern regions of Minas Gerais -MG

ABSTRACT

Living with the arrival of the Covid - 19 pandemic in Brazil in 2020, companies faced a scenario of numerous uncertainties based on the way they act and produce. In order the business continuity to be possible, it was necessary to adapt and readapt the information technology structure, which, in many companies, was non-existent. Based on this circumstances, the aim of this job is to identify the changes that were made for the migration to remote work, in a more specific view regarding the security of data traffic between companies and employees in the home office structure in zona da mata and southern regions. of Minas Gerais. The survey results show an increase in investments and infrastructure, however there is a lack of preparation and training of the people who need to use these resources.

Palavras-chave: Covid-19; home office; information security.

REFERÊNCIAS

BARBOSA, Juliana Souza; SILVA, Danihanne Borges e; OLIVEIRA, Daniela Cabral de; *et al*. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, v. 10, n. 2, p. e40510212557–e40510212557, 2021. Disponível em: <https://www.rsdjournal.org/index.php/rsd/article/view/12557>. Acesso em: 5 novembro de 2021.

CANAL TECH. **90% dos executivos brasileiros estão preocupados com riscos do home office**. Disponível em: < https://canaltech.com.br/seguranca/90-dos-executivos-brasileiros-estao-preocupados-com-riscos-do-home-office-199845//>. Acesso em: 05 novembro de 2021.

DONETA, Danilo. (2006). **Da privacidade à proteção de dados pessoais.** Editora Renovar 3° Edição, São Paulo, 2021 .

ESTADÃO. **Segurança da informação durante a pandemia: Confira a sua importância**

Disponível em: <https://www.toxicologiapardini.com.br/seguranca-informacao-durante-pandemia/>. Acesso em: 01 dezembro de 2021.

EXAME. **93% das indústrias adotaram serviços de TI no cotidiano durante a pandemia**.

Disponível em:

<https://exame.com/bussola/93-das-industrias-adotaram-servicos-de-ti-no-cotidiano-durante-a-pandemia/>. Acesso em: 05 Novembro de 2021.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. 1° Edição. São Paulo: Pearson, 2015.

GANDRA, Alana (2021). **Trabalho em home office tende a continuar após fim da pandemia** - Agência Brasil <https://agenciabrasil.ebc.com.br/economia/noticia/2021-04/trabalho-em-home-office-tende-continuar-apos-fim-da-pandemia> Acesso em: 24 novembro de 2021.

Jornal Daqui. (2020). Crimes Cibernéticos Crescem Durante a Pandemia da Covid-19. <https://www.daquibh.com.br/crimes-ciberneticos-crescem-durante-apandemia-da-covid-19/> Acesso em: 5 novembro de 2021.

KASPERSKY. kaspersky.com.br, 2021. Centro de recursos. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn>. Acesso em: 31 de agosto de 2021.

KOLBE JÚNIOR, Armando. **Sistema de segurança da informação na era do conhecimento**. 1° Edição. Curitiba: Intersaberes 2017.

KUROSE, James F., ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down**. 3° Edição. São Paulo: Pearson, 2006.

OLHAR DIGITAL. **Ataques ransomware aumentaram 311% em 2020**. Disponível em: < https://olhardigital.com.br/2021/02/02/seguranca/ataques-ransomware-aumentaram-311-em-2020-diz-chainalysis/>. Acesso em: 10 outubro de 2021.

PERCíLIA, Eliene, 2006. "Comunicação de Dados"; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/comunicacao-dados.htm. Acesso em 21 de novembro de 2021.

PWC. pwc.com.br, 2021. Notícias. Disponível em: <https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2020/global-digital-trust-insights.html>. Acesso em: 24 de setembro de 2021.

RODRIGUES Jr., Ed Wilson et ali. *Home office* e a segurança da informação em tempos de pandemia. **Invest**, Cuiabá/MT, volume 3, número 1, p.(1-12), 2021. Disponível em: http://revista.institutoinvest.edu.br/index.php/revistainvest/article/view/27/22. Acesso em: 01 de setembro de 2021.

RAFALSKI, J. C.; ANDRADE, A. L. D. **Home Office: Aspectos Exploratórios do Trabalho a partir de Casa** pepsic, 2015. Disponível em: <http://pepsic.bvsalud.org/pdf/tp/v23n2/v23n2a13.pdf>. Acesso em: 03 de setembro de 2021.

TECMUNDO. tecmundo.com.br, 2021. Notícias. Disponível em: <https://www.tecmundo.com.br/seguranca/223158-ransomware-ataque-comum-entre-empresas-brasileiras-2021.htm>. Acesso em: 24 de setembro de 2021.

APÊNDICE I

Apêndice I- Questionário a ser aplicado às empresas.

Foi utilizado para o questionário a escala Likert, Além das opções de respostas anteriores, os respondentes tiveram um campo para possíveis comentários.

Segue abaixo as questões que compõem o questionário:

- Cidade.
- Função
- Após o início da pandemia (COVID-19), com a necessidade da implantação do home office, houve uma maior preocupação com a segurança do sistema.
- Entre os profissionais que estão em home office, todos trafegam em uma rede segura e por meio de dispositivos protegidos.
- Todos os colaboradores têm plena consciência dos riscos cibernéticos que correm e como eles podem impactar negativamente nos negócios.
- Foram realizados treinamentos de funcionários com o objetivo de ampliar a segurança de dados.
- Segundo uma pesquisa realizada pelo site Olhar Digital, há um aumento nos investimentos direcionados à cibersegurança após o início da pandemia. Isto se aplica a sua realidade?
- A migração parcial ou total de dados para o serviço em nuvem representa um risco para a segurança.
- A Logística que foi necessária para realocação de pessoas e recursos para o trabalho remoto trouxe implicações (risco) a segurança de dados.
- O investimento em infraestrutura de software e hardware foi suficiente para a readequação dos sistemas de segurança.
- Foi necessário a implantação de serviços VPN visando a privacidade de dados trafegados entre colaboradores e organização.
- A utilização de soluções open source para a criação e implantação de redes VPN representa maior confiabilidade e segurança.

- Após o início da pandemia do COVID-19 houve um aumento nos incidentes de segurança da informação.
- A continuidade no modelo de trabalho híbrido implicará em um aumento nos investimentos na infraestrutura de segurança da informação.
- Soluções mais robustas de autenticação tiveram que ser adotadas (Biometria e autenticação em dois fatores.
- Políticas de segurança de dados como a “zero trust” tiveram que ser implementadas.