INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES
CAMPUS MACAPÁ

RAIMUNDO SIQUEIRA DE SOUSA FILHO
HALEM RAMON GOMES DE SÁ

HOME OFFICE: TENDÊNCIAS DE SEGURANÇA DA INFORMAÇÃO NO CENÁRIO DE PANDEMIA DE COVID-19

MACAPÁ
2023

RAIMUNDO SIQUEIRA DE SOUSA FILHO
HALEM RAMON GOMES DE SÁ

HOME OFFICE: TENDÊNCIAS DE SEGURANÇA DA INFORMAÇÃO NO CENÁRIO DE PANDEMIA DE COVID-19

Trabalho de Conclusão de Curso apresentado a coordenação do curso Superior de Tecnologia em Redes de Computadores, como requisito avaliativo para obtenção do título de Tecnólogo em Redes de Computadores.
Orientador: Esp. Francisco Sanches da Silva Junior.

MACAPÁ
2023

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

F512h Filho, Raimundo Sigueira de Souza
Home office: tendências de segurança da informação no cenário da pandemia de covid-19

/ Raimundo Sigueira de Souza Filho, Harlem Ramon Gomes Sá. -Macapá, 2021.
41 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2021.

Orientador: Esp. Francisco Sanches Silva Junior.

1. Home Office. 2. Segurança da Informação. I. Sá, Harlem Ramon Gomes. I. Junior, Esp. Francisco Sanches , orient. II. Junior, Francisco Sanches da Silva , coorient. III. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP

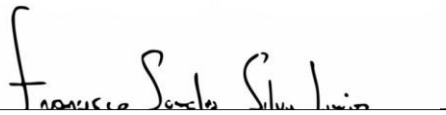
com os dados fornecidos pelo(a) autor

RAIMUNDO SIQUEIRA DE SOUSA FILHO
HARLEM RAMON GOMES DE SÁ

HOME OFFICE: TENDÊNCIAS DE SEGURANÇA DA INFORMAÇÃO NO CENÁRIO DE PANDEMIA DE COVID-19

Trabalho de Conclusão de Curso apresentado a coordenação do curso Superior de Tecnologia em Redes de Computadores, como requisito avaliativo para obtenção do título de Tecnólogo em Redes de Computadores.
Orientador: Esp. Francisco Sanches da Silva Junior.

BANCA EXAMINADORA



Prof. Prof. Esp. Francisco Sanches

Prof. Esp. Erika Bezerra

Prof. Me. Klessis Lopes

Apresentado em: 29/06/2021.

Nota: 97

RESUMO

Este estudo teve o objetivo identificar as tendências de segurança da informação para o trabalho em *Home Office* no cenário de pandemia de covid-19. Para isso foi necessário conhecer os métodos de segurança da informação utilizados em *home office*, descrever vulnerabilidades, e, apontar as dificuldades de implantação desses sistemas para a recente demanda. Como procedimentos metodológicos, optamos pela construção de uma Revisão Integrativa (RI) de literatura. As buscas de artigos recentes na internet foram realizadas utilizando descritores na base de dados eletrônica Google Acadêmico. Como resultados apresentamos sete tendências de segurança da informação para a pandemia de covid-19: 1) Aplicações de aperfeiçoamento de tráfego (VPN e firewall); 2) Atualizações de antivírus; 3) Armazenamento em nuvem; 4) Gerenciamento de senhas; 5) Rotinas de backups; 6) Treinamento de pessoal; 7) Cargos especializados para a gestão de segurança cibernética. Foram apresentados e discutidos métodos, vulnerabilidades; dificuldades e tendências de segurança da informação no atual período de distanciamento social. O presente estudo reforça a importância do investimento em segurança da informação, perante o aumento de ataques a sistemas de rede na pandemia de covid-19.

Palavras-chave: segurança da informação; covid-19; proteção de dados; *home office*.

ABSTRACT

This study aimed to identify information security trends for Home Office work in the covid-19 pandemic scenario. For this it was necessary to know the information security methods used in the home office, describe vulnerabilities, and point out the difficulties of implementing these systems for the recent demand. As methodological procedures, we chose to build an Integrative Review (IR) of literature. Searches for recent articles on the internet were performed using descriptors in the electronic database Google Scholar. As a result, we present seven information security trends for the covid-19 pandemic: 1) Traffic improvement applications (VPN and firewall); 2) Antivirus updates; 3) Cloud storage; 4) Password management; 5) Backup routines; 6) Staff training; 7) Specialized positions for cyber security management. Methods, vulnerabilities were discussed; difficulties and trends in computer network security in the current period of social distance. This study reinforces the importance of investment in information security, given the increase in attacks on network applications in the covid-19 pandemic.

Keywords**:** information security; covid-19; data protection; home office.

SUMÁRIO

1 INTRODUÇÃO

A covid-19 é uma doença causada pelo Novo Coronavírus, vírus denominado SARS-CoV-2, que apresenta um espectro clínico variando de infecções assintomáticas a quadros graves e morte, sendo identificado pela primeira vez em dezembro de 2019, em Wuhan, na China (BRASIL, 2021).

No Brasil, o primeiro caso foi notificado pelo Ministério da Saúde no dia 26 de fevereiro de 2020, no Estado de São Paulo, desde então, os números aumentaram diariamente (OLIVEIRA; LUCAS; IQUIAPAZA, 2020). Dados mais recentes, a nível mundial, apontaram 118.569.219 casos confirmados e 2.629.357 mortes (CSSE/COVID-19 DATA, 2021).

Além dos efeitos sobre a saúde, a covid-19 também resultou em impactos significativos sobre a economia mundial. Medidas de segurança, adotadas mundialmente, como o distanciamento social e lockdown, resultaram no fechamento de empresas e paralisação de linhas de produção, assim, implicando na necessidade de adaptação imediata das relações de trabalho (AQUINO et al., 2020). O *home office*, solução adotada por boa parte das empresas, expressou novos desafios, principalmente para aquelas que contavam exclusivamente com o trabalho presencial (LOSEKANN; MOURÃO, 2020).

Assim, a realidade imposta pela pandemia intensificou o uso do ciberespaço por instituições, demandando que funcionários trabalhassem à distância, bancos que priorizem serviços on-line, lojas adotem sistemas de compras e venda pela internet, e na área da Educação, aulas tiveram que se adaptar ao ensino remoto (MEDEIROS et al., 2020). Esta forma de executar atividades laborais, que já era tendência, sofreu uma aceleração aguda durante a pandemia, fazendo com que nossa sociedade se tornasse cada vez mais digital.

No entanto, a operacionalização de diversas formas de trabalho em meio virtual, inclusive pela administração pública, levantou diversos problemas para implementação do modelo, em especial os relacionados à segurança e privacidade. Dessa forma, a pandemia do Novo Coronavírus não é a única preocupação para as empresas, pois além do risco da covid-19, houve aumento de ataques cibernéticos, isso devido a virtualização de diversos serviços e o grande número de usuários conectados (CARDOSO, 2020; ROLFINI, 2020). Os ataques causam incidentes de segurança da informação, que podem resultar em interrupções de negociações, quebrando os pilares da segurança da informação, a confidencialidade, integridade e disponibilidade da informação (TEXEIRA; DIEL, 2020).

Logo, os profissionais de TI (Tecnologia da Informação) tiveram que intensificar métodos de segurança da informação para atender à crescente demanda de mercado. Em tempos de distanciamento social, a segurança cibernética passa a ter um papel fundamental para pessoas se comunicarem e trabalharem em casa, sem danos como roubo de informação.

Com as medidas de distanciamento social decorrentes da pandemia de covid-19, houve a necessidade de adaptação imediata para novas relações de trabalho (AQUINO et al., 2020). O *home office* foi a solução adotada por muitas empresas, porém, representando novos desafios, como segurança cibernética (RODRIGUES Jr. et al., 2021).

A Segurança da Informação é uma área muito abrangente e que exige o uso de diversas tecnologias e procedimentos (RODRIGUES Jr. et al., 2021). As empresas devem estar preparadas para enfrentar ataques cibernéticos e outras formas de incidentes, que podem gerar desde danos a páginas da web, a roubos e adulterações de informações.

Desta forma, partindo das literaturas consultadas e considerando a crescente demanda por segurança nos sistemas de empresas trabalhando em *home office*, o presente estudo adotou a seguinte questão norteadora como problema de pesquisa: Quais as tendências de Segurança da Informação para o trabalho em *home office* no cenário de pandemia de covid-19?

A motivação para escolha deste tema, foi o aumento considerável de registros de ataques cibernéticos para a pandemia de covid-19 no Brasil (RODRIGUES Jr. et al., 2021). Rolfini (2020) e Cardoso (2020), por exemplo, apontaram um crescimento de cerca de 600% de crimes digitais no início da pandemia. Tais registros, são interpretados como consequência de pessoas estarem mais conectadas, devido ao distanciamento social, e assim, correndo mais riscos de crimes digitais.

Dado o exposto, o desenvolvimento de estudos sobre a segurança informação no cenário de pandemia são de extrema relevância. Visto a crescente operacionalização do ciberespaço, impulsionada pela pandemia de covid-19, que exigiu inovações, desafios e lições.

Este estudo visa, através de Revisão Integrativa (RI), contribuir para construção de conhecimento na área de segurança da informação, apresentando informações atualizadas baseadas em publicações recentes. Tem como o objetivo identificar as tendências de segurança da informação para o trabalho em *Home Office* no cenário de pandemia de covid-19, e para isso foi necessário, conhecer as formas de segurança da informação; descrever as vulnerabilidades das empresas; e, apontar as principais dificuldades de implantação de sistemas de segurança de empresas para adequar ao *home office*.

1.1 Pandemia de COVID-19

A doença viral conhecida como covid-19, causada pelo novo coronavírus SARS - CoV2 (Severe Acute Respiratory Syndrome – Coronavirus 2), foi identificada no final de 2019 na cidade de Wuhan na China (LIMA; SOUSA; LIMA, 2020). A doença rapidamente se espalhou pelo mundo (BORGES et al., 2020), sendo que, em 11 de março de 2020, a Organização Mundial da Saúde (OMS) declarou oficialmente o surto de covid-19 como uma pandemia global (GARCIA; DUARTE, 2020), contabilizando 88.352 casos diagnosticados em 67 países, com 3.001 óbitos, naquela data. Dados mais recentes, a nível mundial, apontam 118.569.219 casos confirmados e 2.629.357 mortes, no início de 2021 (CSSE/COVID-19 DATA, 2021).

No Brasil, o primeiro caso foi notificado pelo Ministério da Saúde no dia 26 de fevereiro de 2020, no Estado de São Paulo, e desde então, os números foram aumentando diariamente (CAETANO et al., 2020). Registros apontam 12,5 milhões de casos e 312 mil mortes até o início de 2021 (CSSE/COVID-19 DATA, 2021). Os cuidados com a Pandemia foram intensificados em larga escala a partir de março de 2020, com o distanciamento social sendo incentivado como forma de prevenção à doença (ROSENVALD et al., 2020).

A transmissão do vírus acontece de uma pessoa doente para outra por meio de gotículas de saliva, catarro, pelo espirro ou tosse, sendo facilitada pelo contato próximo (SOUSA et al., 2020). Quanto ao aspecto fisiopatológico é vasto, causando desde sintomas de um resfriado comum até síndromes respiratórias graves e morte (D'ANGELO et al., 2020). O período de incubação pode ser de 2 a 14 dias, os sintomas mais comuns são febre, tosse e dificuldade para respirar (GREENHALGH; KOH; CAR, 2020).

A grande maioria dos países afetados adotou políticas de distanciamento social e lockdown, desta forma, gerando um cenário de população em suas residências, empresas de portas fechadas, com poucos estabelecimentos abertos, como serviços essenciais e de Saúde (AQUINO et al., 2020). Neste cenário, empresas tiveram que se adaptar a novas formas de trabalho, com crescimento e novas ofertas de serviços digitais e *home office*.

No final de 2020 e início de 2021, foram identificadas variantes do SARS-CoV-2 se espalhando globalmente (OPAS/OMS, 2021). Com o recente desenvolvimento e autorização de vacinas, muitos países têm implementado planos de distribuição em fases que priorizam aqueles com maior risco de complicações, como os idosos, e aqueles com alto risco de exposição e transmissão, como os profissionais de saúde.

1.2 Desafios do *home office* na pandemia

Devido a pandemia atual, o trabalho remoto se tornou a nova realidade para muitas empresas (DRUMMOND, 2020). O termo *home office*, também conhecido como teletrabalho, trabalho remoto, ou trabalho em casa, vem sendo utilizado para formas de trabalho à distância (RODRIGUES Jr. et al., 2021). A palavra passou a ser recorrente na pandemia de covid-19, porém não é uma expressão tão recente, a modalidade já era uma tendência de muitas corporações (BRIK; BRIK, 2013).

Certas empresas defendem que o *home office* tem crescido de forma relevante em produtividade, com redução dos custos organizacionais, como menor consumo de energia, água, diminuição de escritórios físicos (SANTOS et al., 2020).

As empresas passaram a ter novos desafios, recursos foram investidos para possibilitar acesso a equipamentos e ferramentas de comunicação remota. As organizações tiveram que estabelecer políticas e normas internas para implementar e assegurar o teletrabalho (LOSEKANN; MOURÃO, 2020). Para os trabalhadores, surgiram desafios como o rápido aprendizado de novas tecnologias e o estabelecimento de novas dinâmicas de interação e comunicação. Neste novo cenário, o funcionário passa a controlar seu tempo e rendimento buscando o equilíbrio entre qualidade de vida pessoal e profissional (BRIK; BRIK, 2013).

É importante ressaltar que as empresas devem voltar atenção não apenas para a capacidade de ampliação de serviços digitais, mas também para recursos essenciais de segurança cibernética, que garantam a proteção e segurança de dados da empresa ou de clientes. Desta forma, a segurança da informação teve que ser revista para incorporar a rotina de trabalho remoto, pois para os novos serviços, ferramentas e aplicações é necessário oferecer a máxima segurança (BORTOLUZZI, 2006).

Com intuito de beneficiar a funcionalidade, segurança e gerenciamento da rede privada, torna-se um dos grandes desafios a busca de meios para viabilizar novas infraestruturas de TI (tecnologia da Informação) para uma grande quantidade de usuários remotos. Assim, as equipes de tecnologia da informação, tiveram que efetuar rápidas mudanças, em um curto período, para o atendimento da nova demanda exigida resultante da pandemia de covid-19.

1.3 Segurança em sistemas de informação e vulnerabilidades

A segurança física das empresas sempre foi uma grande preocupação, mais recentemente, com a pandemia de covid-19, os investimentos na proteção de informações passaram a ser uma prioridade (TEXEIRA; DIEL, 2020).

A segurança da informação pode ser definida como um “conjunto de orientações, normas, procedimentos, políticas e demais ações que tem como objetivo proteger o recurso da informação (FONTES, 2006, p.11). Trata-se uma área muito abrangente e que exige o uso de diversas tecnologias e procedimentos, necessitando de constante atualização.

Com a utilização da internet, a segurança de dados pessoais ficou, ainda mais, comprometida. Neste contexto, temos a “segurança cibernética”, como uma evolução de segurança da informação, também pode ser chamada de segurança digital ou do espaço cibernético (FONTES, 2006).

Para Rodrigues Jr. et al. (2021), a segurança da informação não é considerada uma ciência exata, pois seria classificada como gestão de riscos. Fontes (2006), destaca que a segurança da informação é a proteção oferecida para atingir os objetivos apropriados da proteção de dados: a integridade, a disponibilidade e a confidencialidade.

Com a pandemia de covid-19, devido ao aumento de conectividade e maior adesão da população por serviços via internet, o número de vítimas de crimes digitais aumentou consideravelmente (ROLFINI, 2020). Criminosos cibernéticos, os hackers se aproveitam do cenário de pânico para distribuir *fake news* e softwares maliciosos (malware) como vírus, ransomwares e afins, visando indivíduos, empresas e outras organizações, para roubar dados pessoais, extorquir e desviar dinheiro (AZEVEDO; OLIVEIRA, 2020; MEDEIROS et al., 2020; BARBOSA et al., 2021).

Segundo Laudon e Laudon (2006), o termo hacker é utilizado para definir pessoa que conseguem acesso não autorizado a uma rede de computadores, com o intuito de obter lucro, intervindo criminosamente. Hackers utilizam softwares maliciosos que tem como característica infectar os computadores e dispositivos de várias maneiras, assumindo diversas formas. Tais ameaças se multiplicam diariamente e possuem inúmeras variações como spyware, adware, phishing, vírus, trojans, worms, rootkits, ransomware (GARCIA, 2020).

Outro problema crescente relacionado a segurança da informação, é a propagação de *fake news*, ou seja, notícias falsas. Com a chegada da pandemia, houve uma intensa disseminação informações falsas sobre covid-19, principalmente por redes sociais.

As *fake news* que circulam na internet, também afetam a segurança da informação, têm o intuído de propagar informações inverídicas tanto em sites, quanto em redes sociais, através de links, mensagens, anúncios ou perfis falsos com finalidade ideológica de denegrir a

imagem de uma pessoa, enganar ou distorcer informações, entre outras situações (AZEVEDO; OLIVEIRA, 2020). São propagadas por criminosos virtuais, atuam no processo de desinformação, ponto-chave no cenário atual para ataques digitais (NAGLI, 2020). As *fake news* são consideradas como ataques cibernéticos, pois muitas vezes são acompanhadas de vírus e aplicativos maliciosos contribuindo para o agravamento da situação atual de calamidade (AZEVEDO; OLIVEIRA, 2020).

Atualmente, há legislação específica, diretamente ligada a segurança da informação. Segundo Barbosa et al. (2021), a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Segundo Pinheiro (2018), o surgimento de regulamentações de proteção de dados pessoais foi diretamente relacionado a segurança de negócios da economia digital viabilizados pelos avanços tecnológicos e pela globalização.

1.4 Tendências de segurança para *home office*

Atualmente na pandemia, trabalhadores e seus respectivos computadores, fora de seu habitual ambiente de trabalho, correm risco de perder parte da segurança da informação por não possuírem os recursos necessários para segurança de dados em suas residências (MARASCA et al., 2020). Dessa forma, trabalhar em *home office* expõe as informações diversas e confidenciais exclusivas de uma corporação, estando sujeitas a violação de dados (TEXEIRA;/ DIEL, 2020). Para que isso não aconteça no trabalho remoto, é necessário investimento em infraestrutura e sistemas de segurança da informação.

Quando se trata de segurança de sistemas de computadores, as aplicações mais reconhecidas são os antivírus. Certamente, sua utilização é extremamente necessária, principalmente em computadores de uso pessoal utilizados para trabalho (RODRIGUES Jr. et al., 2021). No entanto, outros métodos podem ser recomendados para proteção de empresas, pois a segurança da informação abrange um leque amplo de métodos, processos, requisitos em que vulnerabilidades são consideradas para o planejamento e implementação de sistemas de segurança, desde a infraestrutura (redes, servidores etc.) até a arquitetura e próprios sistemas e aplicativos (LAUDON; LAUDON, 2006).

Dentre os métodos recentes para evitar ciberataques, estão o controle de usuários, cloud computer, criação de políticas de segurança, uso de VPN (Virtual Private Networks),

firewall, virtualização de servidores (VARELLA, 2019). O firewall, por exemplo, é dispositivo que promove a segurança de uma rede, trabalha fazendo o monitoramento do tráfego (LAUDON; LAUDON, 2006). A conexão dos funcionários à rede corporativa VPN, representa uma forma bastante segura de acessar uma rede coorporativa, sendo muito indicada para evitar interrupções e falhas como vazamentos de dados, também contribuindo para a segurança em trabalho remoto (LEITE, 2017; OKANO et al., 2020). Além dessas aplicações, é essencial uma equipe de TI especializada para garantir toda a funcionalidade e efetividade dos sistemas de segurança (RODRIGUES, 2020).

2 PROCEDIMENTOS METODOLÓGICOS

Para alcançar os objetivos deste estudo, optamos por utilizar o método de Revisão Integrativa da literatura, sendo uma abordagem metodológica muito ampla referente as revisões bibliográficas, que possibilita síntese e análise do conhecimento científico já produzido sobre o tema investigado (SOUZA; SILVA; CARVALHO, 2010). Por esse método são utilizados artigos recentes buscados em base de dados eletrônicas utilizando descritores (palavras-chave).

Foram selecionadas publicações com enfoque nas tendências de segurança cibernética aplicadas ao *home office*, tendo em vista a nova demanda de recursos e funções exigidas pelo mercado no cenário de pandemia e o crescimento de ataques cibernéticos.

2.1 Desenho do estudo

Trata-se de um estudo exploratório e descritivo, de abordagem qualitativa. A natureza exploratória de um estudo visa familiarizar-se com o problema de pesquisa, e, o estudo descritivo tem a finalidade de observar, descrever e documentar os aspectos de uma situação (SAUNDERS; LEWIS; THORNHILL, 2009). A abordagem qualitativa trata de informações não quantificáveis e os dados são analisados indutivamente (GIL, 2008).

Segundo Mendes, Silveira e Galvão (2008), uma RI é guiada por uma questão norteadora de pesquisa que orienta a busca de dados bibliográficos, para análise e comparação, assim permitindo que se obtenha conclusões gerais sobre o problema de pesquisa, possibilitando gerar novos conhecimentos e apontar lacunas que possam ser preenchidas por estudos posteriores. As bases para a construção de uma RI seguem principalmente nos estudos de Whitemore e Knafl (2005), Broome (2006), Mendes, Silveira, Galvão (2008) e Souza, Silva e Carvalho (2010).

2.2 Revisão Integrativa

A Construção de uma RI é constituída por seis fases distintas (WHITEMORE; KNAFL, 2005; BROOME, 2006; MENDES; SILVEIRA; GALVÃO, 2008; SOUZA; SILVA; CARVALHO, 2010): 1) Elaboração da pergunta norteadora; 2) Busca ou amostragem na literatura (critérios de inclusão e exclusão); 3) Definição das informações a serem extraídas;4)

Avaliação dos dados incluídos na revisão interativa; 5) Interpretação dos resultados e discussão; 6) Apresentação da revisão integrativa.

2.2.1 Primeira fase: Elaboração da pergunta norteadora

Fase de definição de um problema e a formulação da questão de pesquisa, também, identifica as informações coletadas de cada estudo selecionado (MENDES; SILVEIRA; GALVÃO, 2008. A pergunta norteadora deve ser elaborada de forma clara e específica, e relacionada a um raciocínio teórico, esta etapa conduzira a RI (SOUZA; SILVA; CARVALHO, 2010).

Quais as tendências de segurança da informação para o trabalho em *Home Office* no cenário de pandemia de covid-19?

2.2.2 Segunda fase: Busca ou amostragem na literatura (critérios de inclusão e exclusão)

A busca em bases de dados eletrônicas deve ser diversificada e ampla, com a internet se tem ótimas ferramentas para busca de bibliografia, no entanto, devesse selecionar criteriosamente os trabalhos a serem incluídos na revisão, assim como expor tais estudos (ERCOLE; MELO; ALCOFORADO, 2014). O ideal para a inclusão na amostra, seria selecionar de todos os artigos encontrados relacionados a temática, ou até mesmo a aplicação de uma seleção aleatória, no entanto, caso não seja possível a inclusão de muitos trabalhos, critérios de inclusão e exclusão devem ser bem definidos e expostos, sempre em concordância com a questão norteadora (SOUZA; SILVA; CARVALHO, 2010).

O procedimento de inclusão e exclusão de artigos deve ser conduzido de maneira criteriosa e transparente, todos os passos devem ser descritos. A delimitação e boa seleção dos descritores atestará confiabilidade e representatividade da amostra, indicando a qualidade da pesquisa (MENDES; SILVEIRA; GALVÃO, 2008).

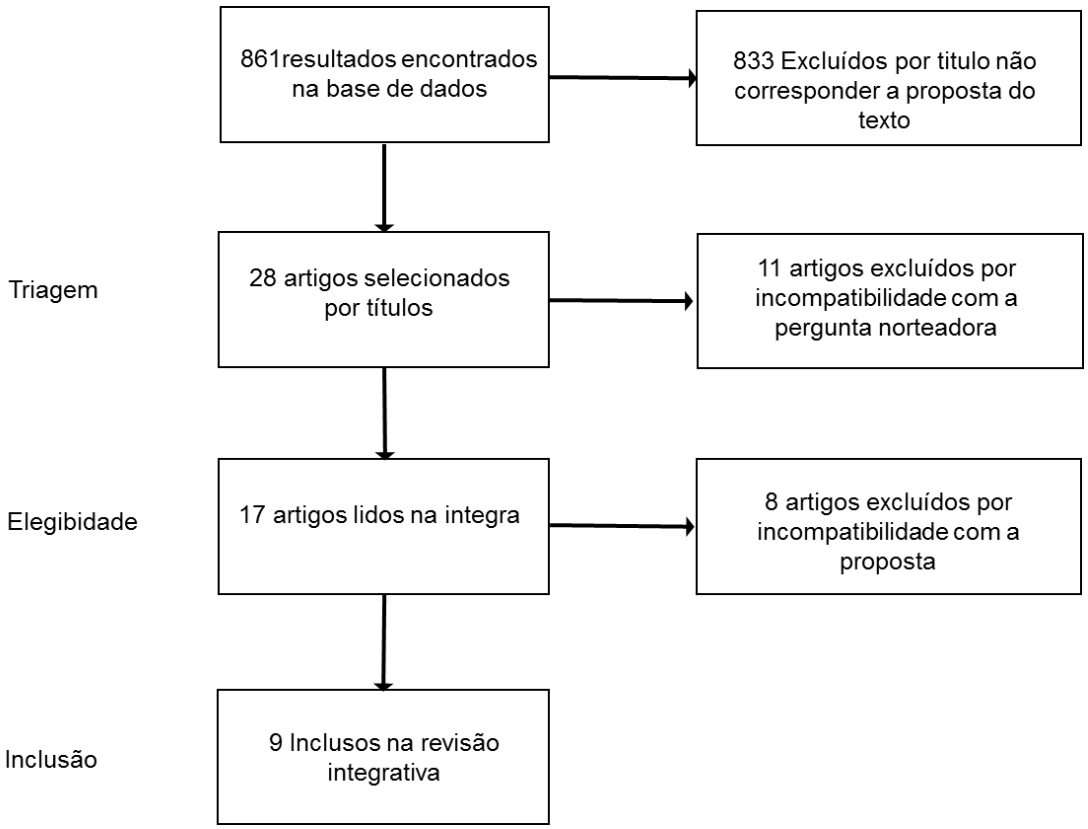
A busca de artigos para o presente estudo foi realizada através da base de dados Google Acadêmico, visando publicações completas com resumos disponíveis e indexadas. Como instrumento de pesquisa foram elencados os descritores: “segurança da informação” “covid-19”, “proteção de dados” e “*home office*” cruzados com operador booleano AND.

Os critérios de inclusão adotados foram: publicações relacionadas com a temática da proposta da pesquisa; artigos completos publicados entre os anos de 2015 e 2021; publicações divulgadas em língua portuguesa, inglesa e espanhola.

Foram excluídos artigos de revisão, editorias, resumos de congresso, monografias, dissertações e teses e artigos duplicados.

O resultado da busca apresentou um total de 861 resultados, porém, somente 9 foram inclusos para RI, através de critérios de elegibilidade como afinidade com proposta da pesquisa e compatibilidade com a pergunta norteadora. O fluxograma abaixo (figura 1), mostra como ocorreu a seleção dos artigos.

Figura 1 – Fluxograma de seleção de artigos nas diferentes etapas



Fonte: Produzido pelos autores, 2021.

2.2.3 Terceira fase: Definição das informações a serem extraídas dos estudos selecionados

Esta etapa consiste na definição das informações a serem extraídas dos artigos selecionados, é importante utilizar instrumentos para reunir, sintetizar e apresentar as informações-chave dos trabalhos (MENDES; SILVEIRA; GALVÃO, 2008). A elaboração de quadros proporciona uma síntese de cada artigo que permite ao leitor observar resultados e conclusões evidenciados em cada artigo (POMPEO; ROSSI; GALVÃO, 2009).

Ao término da leitura crítica dos 9 artigos selecionados, que integram esta revisão, foi elaborado um instrumento (apresentado nos resultados) para reunir e sintetizar as informações-chave da amostragem com autores, ano, título, objetivos, métodos e resultados (Quadro 1).

2.2.4 Quarta fase: Avaliação dos dados incluídos na revisão interativa

Segundo Pompeo, Rossi e Galvão (2009), essa é a fase em que os artigos selecionados são analisados criticamente em relação aos critérios de importância das informações e representatividade. Esta etapa é equivalente à análise dos dados em uma pesquisa convencional, utilizando os métodos apropriados.

A análise crítica dos trabalhos selecionados foi realizada observando aspectos metodológicos, assim como os foram comparados os resultados por similaridade. Os dados foram analisados de forma minuciosa, buscando respostas para a questão norteadora da pesquisa.

2.2.5 Quinta fase: Interpretação dos resultados e discussão

Esta etapa da pesquisa, conforme abordado por Mendes, Silveira e Galvão (2008), corresponde à fase de discussão dos principais resultados de uma pesquisa convencional. Assim, os resultados obtidos são discutidos com enfoque na resolução dos questionamentos (BOTELHO; CUNHA; MACEDO, 2011). Por conseguinte, os dados evidenciados nos artigos são comparados com a finalidade de integrar o conhecimento a ser apresentado na pesquisa.

Dessa forma, os resultados obtidos foram expostos e ilustrados através de quadros informativos e comentários. A discussão dos resultados foi realizada minunciosamente frente à bibliografia selecionada, buscando interpretação dos conteúdos, abordando temáticas relevantes aos resultados e descrevendo conceitos complementares, sempre buscando alienamento com objeto de pesquisa proposto pela questão norteadora.

2.2.6 Sexta fase: Apresentação da revisão integrativa/síntese do conhecimento

De acordo com Botelho, Cunha e Macedo (2011), esta é a última etapa da revisão, o trabalho elaborado deve descrever todas as etapas trilhadas na pesquisa. Os resultados devem

ser apresentados de forma criteriosa e clara, de modo a permitir ao leitor avaliar criticamente os resultas (POMPEO; ROSSI; GALVÃO, 2009).

Para finalizar esta RI, tendo resultados expostos e a discussão apresentada de forma minuciosa e detalhada, o trabalho foi concluído com as considerações finais sendo apresentadas. Por último, foi realizada elaboração do resumo das evidências disponíveis. A síntese do conhecimento é exposta no seguinte tópico, resultados.

3 RESULTADOS

Este tópico apresenta os resultados deste estudo, através de explanação do tema, descrição de conceitos, apresentação de quadros e comentários que sintetizam informações correspondentes a questão norteadora e os objetivos deste estudo.

O Quadro 1 apresenta as características gerais dos 9 estudos selecionados para a RI.

Quadro 1 – Síntese de dados informativos da amostragem dos 9 artigos selecionados conforme autores, ano, título, base, objetivos, métodos e resultados

AUTORES/ANO TÍTULO DO ARTIGO	OBJETIVOS	MÉTODOS	RESULTADOS
AZEVEDO; OLIVEIRA, 2020. O impacto das *fake news* na segurança da informação e sua influência no cotidiano das pessoas.	Discutir a vulnerabilidade das informações em questão da segurança e a confiabilidade das notícias divulgadas na *Web*.	Estudo quantitativo, de caráter exploratório e descritivo, realizado por meio de questionário.	Após as análises apresentadas, foi observado que apesar das pessoas conhecerem o conceito de *fake news*, a maioria delas acabaram sendo vítimas destas notícias falsas.
LEMA, 2021. La gestión de la información durante etapas de teletrabajo en la época de la covid-19.	Discutir sobre sistemas de informação e as medidas de segurança que foram aplicadas para reduzir os riscos cibernéticos derivados do trabalho remoto.	Estudo descritivo, com abordagem quantitativa, por meio da estratégia de pesquisa documental.	Recomendações para organizações e trabalhadores de um instituições públicas ou privadas, que auxiliam na implementação de medidas de segurança.
MEDEIROS *et al*., 2020. O uso do ciberespaço pela administração pública na pandemia da covid-19: diagnósticos e vulnerabilidades.	Analisa o uso e a operacionalização do ciberespaço pela Administração Pública no combate ao SARS-CoV-2.	Estudo descritivo, com abordagem quantitativa, por meio da estratégia de pesquisa documental.	Apresenta um diagnóstico das vulnerabilidades e desafios referentes a essa crescente operacionalização.
NAGLI, 2020. Pandemia na pandemia: a escalada de ataques cibernéticos pós-covid-19.	Descrever impactos e métodos de prevenção para o que aqui se denomina Pandemia na Pandemia, a escalada de ataques virtuais pós-covid-19,	Estudo exploratório, com abordagem e qualitativa, por meio da estratégia de pesquisa documental e entrevistas com especialistas em segurança da informação	São apresentadas as medidas recentemente denominadas Higiene Digital, e recomendadas medidas de segurança da informação com base em custo x benefício para empresas.
OKANO *et al.*, 2020. Impactos da pandemia	Compreender e analisar as principais dificuldades, no	Estudo de casos múltiplos com perspectiva	Como resultados, os dois modelos comprovam que as

covid-19 em empresas de grande porte: avaliação das mudanças na infraestrutura de tecnologia para o teletrabalho sob as óticas das teorias das capacidades dinâmicas e estrutura adaptativa.	âmbito de TI de três empresas de grande porte para adequar sua infraestrutura de TIC ao novo cenário.	longitudinal e os frameworks Modelo de Pesquisa de Capacidades Dinâmicas e o Modelo de Apropriação de Tecnologia com abordagem de natureza exploratória.	empresas A, B e C tiveram condições de suportar as novas demandas, adaptando as suas infraestruturas de TICs para o novo cenário causado pela pandemia da covid-19, forçando os colaboradores a adotarem a nova forma de trabalho.
PERES et al., 2021. Segurança e legitimidade no trabalho remoto - Relato de experiência em um Hospital Público e Universitário.	Apresentar os esforços necessários para viabilizar o teletrabalho em uma das ações de enfrentamento à covid-19 no Hospital de Clínicas de Porto Alegre.	Pesquisa de natureza aplicada, com abordagem qualitativa do tipo exploratória, com métodos adequados, utilizando técnicas de observação participante.	Trabalho remoto consolidado, diminuindo, assim, as chances de contaminação por covid-19.
RODRIGUES Jr. et al. 2021. *Home office* e a segurança da informação em tempos de pandemia.	Informar e apresentar práticas que possam auxiliar na manutenção da segurança cibernética no *home office*.	Estudo descritivo, com abordagem e qualitativa, por meio da estratégia de pesquisa documental.	Foram apontados os possíveis vetores danosos e cuidados com a segurança em *home office* para o período de pandemia.
SILVA *et al*., 2020. A estratégia de tecnologia da informação e os sistemas emergentes no plano de gerenciamento de crise da covid-19 no Instituto Nacional de Câncer.	Apresentar a estratégia desenvolvida pela equipe de Tecnologia de Informação do INCA, para dar suporte ao Plano Institucional da Covd-19.	Estudo exploratório, documental de abordagem qualitativa e utilização de dois estudos correlatos.	Criação de um Comitê de Gestão de Crise responsável por elaborar um plano estratégico institucional emergencial para tratar a questão.
SUAREZ et al., 2020. Importancia de la seguridad informática y ciberseguridad en el mundo actual.	Discorrer sobre sistemas de informação e as medidas de segurança que foram aplicadas para reduzir os riscos cibernéticos derivados do trabalho remoto.	Estudo descritivo, com abordagem qualitativa, por meio da estratégia de pesquisa documental.	Foram destacadas opções para investimento como softwares, hardwares e serviços de segurança e treinamento de pessoal com intuito de evitar ciberataques.

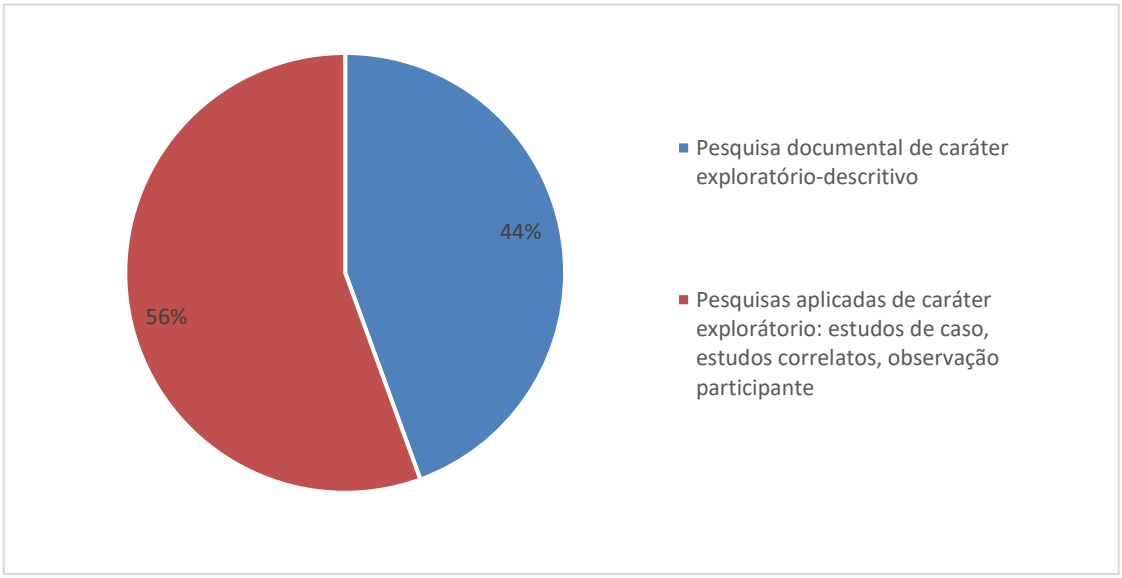
Fonte: Produzido pelos autores, 2021.

Em relação ao ano de publicação dos trabalhos inclusos no estudo, apesar de se estabelecer um período de 2015 a 2021, com filtragem nas buscas, os 9 artigos selecionados, compatíveis com a proposta, são publicações dos anos 2020 e 2021, isso dado ao fato de se tratar de um tema recente envolvendo a pandemia de covid-19.

Quanto aos trabalhos em língua estrangeira, dois artigos estavam disponíveis somente em língua espanhola (22,2 % da amostra), foram inclusos por se enquadrarem nos requisitos para pesquisa. Ressalta-se que maioria dos trabalhos está disponível em português e língua estrangeira.

Com relação à metodologia utilizada nos trabalhos selecionados (gráfico 1), quatro trabalhos apresentam caráter exploratório-descritivo e documental, representando 44% da amostra, os outros cinco trabalhos, além do caráter exploratório, tratam-se de pesquisas aplicadas com outros tipos de delineamentos de pesquisa (Gil, 2008), como estudos de caso, estudos correlatos e observação participante, representando 56% da amostra.

Gráfico 1 – Metodologia dos estudos da amostra



Fonte: Produzido pelos autores, 2021.

3.1 Métodos de segurança da informação utilizadas em *home office* na pandemia

Em relação ao primeiro objetivo específico proposto pelo estudo, foi possível conhecer ferramentas e métodos de segurança da informação abordados nos trabalhos selecionados. Sendo as aplicações mais abordadas, na segurança para sistemas de *home office*, o uso de VPN, firewall e pacotes de antivírus, conforme observado no quadro 02.

Quadro 2 – Métodos de segurança da informação aplicados ao *home office* na pandemia.

MÉTODO DE SEGURANÇA	AUTORES
VPN (Virtual Private Network)	LEMA, 2021 NAGLI, 2020 OKANO et al., 2020 PERES et al., 2020 RODRIGUES Jr. et al., 2021 SILVA *et al*., 2020 SUAREZ et al., 2020
Firewall	NAGLI, 2020 OKANO et al., 2020 PERES et al., 2020 RODRIGUES Jr. et al., 2021 SUAREZ et al., 2020
Antivírus	LEMA, 2021 NAGLI, 2020 OKANO et al., 2020 RODRIGUES Jr. et al. 2021 SUAREZ et al., 2020
Autenticação de senhas em duplo fator	PERES et al., 2020 NAGLI, 2020

Fonte: Produzido pelo próprio autor, 2021.

Embora quando se aborde segurança da informação corporativa, comumente possa-se aludir a antivírus, é importante, também, conhecer outas formas de proteção de dados, como aplicações que visem o aperfeiçoamento do tráfego seguro de informações como VPN e firewall. A autenticação de senhas em dois fatores com auxílio de aplicativos como o Google Authenticator, é um método cada vez mais comum e garante maior segurança ao acesso a redes privadas.

3.2 Vulnerabilidades das empresas frente ao trabalho em *home office*

As principais vulnerabilidades e ataques descritos para os sistemas via *home office* na pandemia foram aplicações maliciosas (*malwares*) como vírus, ransomwares, spywares e afins, seguidos por *Phishing* e *fake news* (quadro 3), sendo as formas de ataques mais citadas nos artigos da amostragem.

Softwares maliciosos ao invadirem um sistema digital pode causar diversos tipos de danos, desde assumir o controle do maquina, monitorar ações e até mesmo enviar dados confidenciais para a base do *hacker* (MEDEIROS et al., 2020; NAGLI, 2020; SUAREZ et al., 2020). Frequentemente, são distribuídos em conjunto com outras técnicas de ataque como o *phishing* e sites maliciosos.

Os vírus, comumente, infectam outros arquivos do sistema com a intenção de modificá-los para destruir intencionalmente os dados armazenados. Ataques de *ransomwares* tem ganhado bastante notoriedade na pandemia, causando transtornos a empresas privadas e agências governamentais (MEDEIROS et al., 2020; NAGLI, 2020; SUAREZ et al., 2020). São agentes maliciosos que agem como sequestradores de informações exigindo resgate para restaurar as funções (MEDEIROS et al., 2020; NAGLI, 2020; SUAREZ et al., 2020).

O phishing é considerada a técnica mais utilizada para distribuição de conteúdo malicioso e captura de informação, ocorre através do envio de e-mail, anexos e links falsos que direcionam o usuário para aplicativos maliciosos (LEMA, 2021; NAGLI, 2020, SUAREZ et al., 2020).

As *fakes news* foram amplamente disseminadas na pandemia do Novo Coronavírus, gerando a chamada “infodemia”, termo que reflete uma superabundância de informações falsas fortemente divulgados no período da pandemia, essa explosão de conteúdos falsos na internet resulta dúvidas e insegurança, prejudicando os cuidados com saúde físicas e mental da população (AZEVEDO; OLIVEIRA, 2020; MEDEIROS et al., 2020; NAGLI, 2020).

Além de contribuírem para a desinformação da população, as *fake news* também são muito apontadas como formas de ataque a segurança da informação, pois muitas vezes, as pessoas procurando informações sobre a covid-19, são guiados por essas notícias falsas a links fraudulentos conectados a aplicativos maliciosos (AZEVEDO; OLIVEIRA, 2020; MEDEIROS et al., 2020; NAGLI, 2020). Por conseguinte, a disseminação de vírus e afins, *phishing* e *fake news* são formas de ataques intricadamente relacionados.

Lema (2021) reporta que ataques de *phishing*, *malspams* e *ransomware* aumentaram na pandemia, utilizando justamente anúncios e links para compra de produtos de proteção individual contra a covid-19.

Quadro 3 – Vulnerabilidades relacionadas a empresas diante dos sistemas via *home office* na pandemia de covid-19.

VULNERABILIDADE / ATAQUES CIBERNÉTICOS	AUTORES
Vírus, *Ransomwares, malspams, trojans, Spyware, Adware* e afins	LEMA, 2021 MEDEIROS et al., 2020 NAGLI, 2020 OKANO et al., 2020 RODRIGUES Jr. et al., 2021 SUAREZ et al., 2020
*Phishing (*Envio de links maliciosos por e-mail ou aplicativos de comunicação)	LEMA, 2021 MEDEIROS et al., 2020 NAGLI, 2020 SUAREZ et al., 2020
Fake News	AZEVEDO; OLIVEIRA, 2020. MEDEIROS et al., 2020 NAGLI, 2020
Ataque *Cross-Site Scripting*	RODRIGUES Jr. et al., 2021 SUAREZ et al., 2020
DDoS Attack	MEDEIROS et al., 2020 NAGLI, 2020
Uso incorreto da tecnologia	SUAREZ et al., 2020 NAGLI, 2020
SQL Injection	SUAREZ et al., 2020

EAC/ Email Account Compromise (Ataques de Comprometimento de Conta de Email)	SUAREZ et al., 2020

Fonte: Produzido pelo próprio autor, 2021.

3.3. Principais dificuldades na implantação de sistemas de segurança

As principais dificuldades apontadas na implantação de sistemas de segurança em empresas para adequação ao *home office* são apresentadas no quadro 4. Neste estudo identificamos que a aquisição de Infraestrutura e equipamentos foram os foram as dificuldades mais mencionadas, seguido por fatores humanos como treinamento e atualização de funcionários ou mesmo a falta de profissionais especializados em segurança da informação (quadro 4).

Quadro 4 – Principais dificuldades da implantação de sistemas de segurança de empresas para adequar ao *home office*.

DIFICULDADES	AUTORES
Infraestrutura e equipamentos	AZEVEDO; OLIVEIRA, 2020 MEDEIROS et al., 2020 NAGLI, 2020 OKANO et al., 2020 SUAREZ et al., 2020
Fator humano (treinamento e atualização)	AZEVEDO; OLIVEIRA, 2020 NAGLI, 2020 PERES et al., 2020 SUAREZ et al., 2020
Falta de profissionais de segurança	NAGLI, 2020

da informação	RODRIGUES Jr. et al., 2021

Fonte: Produzido pelos autores, 2021.

3.4 Tendências de segurança da informação no cenário de pandemia

Como forma de resposta a questão norteadora da pesquisa, foram identificas as tendências de segurança da informação no cenário de pandemia, apresentadas no quadro 5.

Quadro 5 – Tendências de segurança da informação no cenário de pandemia.

TENDÊNCIAS DE SEGURANÇA	AUTORES
Proteção do tráfego de informações (VPN e Firewall)	LEMA, 2021 NAGLI, 2020 OKANO et al., 2020 PERES et al., 2020 RODRIGUES Jr. et al., 2021 SILVA *et al*., 2020 SUAREZ et al., 2020
Aumentar o ciclo de atualizações de Antivírus, *Anti-spyware*, *Anti-malware* e afins	LEMA, 2021 NAGLI, 2020 OKANO et al., 2020 RODRIGUES Jr. et al. 2021 SUAREZ et al., 2020
Evitar o uso de pendrives e HDs externos *(Cloud computing)*	LEMA, 2021 OKANO et al., 2020 PERES et al., 2020 RODRIGUES Jr. et al. 2021
Gerenciamento de senhas (autenticação de senhas em duplo	NAGLI, 2020 PERES et al., 2020

fator)	
Rotina de *backups*	MEDEIROS et al., 2020 RODRIGUES Jr. et al. 2021
Treinamento de pessoal	NAGLI, 2020 OKANO et al., 2020
Especialistas para cargos de *Chief Information Security Office* e *Chief Information Officer*	RODRIGUES Jr. et al. 2021

Fonte: Produzido pelos autores, 2021.

O aperfeiçoamento da proteção das conexões para tráfego de informações, com uso de VPN e *firewall*, tem sido apontado como uma das principais tendências de proteção em redes. A substituição do armazenamento físico, como *pendrives* e HDs externos, por armazenamento em nuvem "*Cloud computing*", também, tem sido apontada como uma forte tendência atual, assim como o gerenciamento de senhas e estabelecimento de rotinas de backups de todos os arquivos e documentos.

No combate a vírus de computador, além de um bom pacote aplicações, deve-se estar atento às atualizações de Antivírus, *Anti-spyware*, *Anti-malware* e afins. Treinamento de pessoal é essencial, pois mesmo com as melhores infraestruturas de segurança da informação, sem o treinamento adequado para o uso da tecnologia, as maiores vulnerabilidades poderão ser resultado de falha humana. A criação de cargos especializados em segurança da informação como, *Chief Information Security Officer* e *Chief Information Officer*, visam garantir o planejamento e implementação de processos e estratégias de segurança de acordo com as normas determinadas pelas leis de proteção de dados.

4 DISCUSSÃO

O presente estudo apresenta informações sobre o conhecimento científico do impacto da pandemia de covid-19 sobre a segurança da informação perante as novas relações de trabalho. Pois conforme o exposto, os cuidados com a pandemia intensificaram uma tendência atual de expansão do *home office* por muitas empresas, com intuito de evitar maiores impactos econômicos resultantes da paralisação de várias formas de trabalho presencial.

Rodrigues Jr. et al. (2021), ressaltam que em meio a uma das maiores ameaças da humanidade (Novo Coronavírus), além do risco biológico, tal situação proporcionou aos cibercriminosos novas oportunidades para práticas delituosas, pois com a população fragilizada, passando mais tempo on-line em suas casas, utilizando a internet, mais do que nunca, para comunicação com a família, realização de trabalhos, compras, pagamentos e entretenimento, ou mesmo, buscando por informações relacionadas a pandemia. Esta nova rotina de atividades no ciberespaço despertou o interesse de golpistas em lucrarem na pandemia.

Conforme o exposto nos resultados apresentados, através desta RI obtivemos a resposta para nossa questão norteadora. Assim, temos como principais tendências identificadas na segurança da informação, os meios de aperfeiçoamento na proteção das conexões para tráfego de informações, como o uso de VPN e *firewall* abordados em 77,8% dos artigos analisados (7 publicações) (LEMA, 2021; NAGLI, 2020; OKANO et al., 2020; PERES et al., 2020; RODRIGUES Jr. et al., 2021; SILVA et al., 2020; SUAREZ et al., 2020) (quadro 4).

Tais estratégias de segurança foram abordadas como propostas para controle de vulnerabilidades, ou mesmo, como métodos aplicados na prática empresarial, dependendo da linha de estudo do trabalho selecionado, como observado no quadro 01, que expõe o perfil metodológico utilizado para cada artigo selecionado. Desta forma, observa-se que determinados trabalhos descrevem suas experiências com uso prático de determinadas aplicações na segurança da informação (PERES et al., 2020; SILVA et al., 2020; OKANO et al., 2020), enquanto outros, exploram e descrevem quais os meios mais indicados para combater determinado tipo de ameaça (LEMA, 2021; MEDEIROS et al., 2020; NAGLI, 2020; OKANO et al., 2020; RODRIGUES Jr. et al., 2021; SUAREZ et al., 2020).

Outra tendência bastante citada nas publicações selecionadas foi o aumento dos ciclos de atualizações de softwares de segurança (antivírus e afins), método citado em 55,6% das

publicações (5 artigos) (LEMA, 2021; NAGLI, 2020; OKANO et al., 2020; RODRIGUES Jr. et al. 2021; SUAREZ et al., 2020). O uso de antivírus é um dos métodos mais reconhecidos na proteção de sistemas digitais, no entanto, existem outros meios de proteção, dependendo da ameaça ou vulnerabilidade. Desta forma, o tipo de antivírus a ser usado depende das necessidades ou requisitos de cada usuário, sendo de vital importância manter o pacote de antivírus atualizado para obter o melhor nível de proteção (LEMA, 2021; NAGLI, 2020; OKANO et al., 2020; RODRIGUES Jr. et al. 2021; SUAREZ et al., 2020).

O uso de computação em nuvem foi citado em 4 artigos da amostra (LEMA, 2021; OKANO et al., 2020; PERES et al., 2020; RODRIGUES Jr. et al. 202), algo bastante representativo, sendo a terceira tendência mais citada para segurança da informação. Tal estratégia, muito comum atualmente, vem sendo indicada por evitar o uso de drives físicos como pendrives e HDs externos (LEMA, 2021; RODRIGUES Jr. et al. 2021), e, devido a seus serviços serem acessados de qualquer lugar via rede, não havendo necessidade de instalação de softwares ou de armazenar dados

O gerenciamento de senhas é cada vez mais comum atualmente, porém, foi citado por apenas 2 autores (NAGLI, 2020; PERES et al., 2020), é considerado uma medida bastante efetiva na redução do roubo de identidade. Aplicativos autenticadores como o do Google e o da Microsoft podem ser utilizados nesse processo. Por exemplo, no trabalho de Peres et al. (2020), um relato de experiência sobre a viabilização do teletrabalho no Hospital de Clínicas de Porto Alegre, os autores descrevem o uso da autenticação em dois fatores com o Google Authenticator para liberação ao acesso remoto à VPN do hospital.

O estabelecimento de rotinas de backups de todos os dados e arquivos, também, foi considerado como tendência atual por dois artigos (MEDEIROS et al., 2020; RODRIGUES Jr. et al. 2021). Considerado como um plano de ação, caso os cibercriminosos consigam invadir a rede da empresa, backups podem minimizar os danos com a preservação de arquivos ou dados comprometidos. Medeiros et al. (2020), relata, casos de ataques de *ransomware* em que as realizações de constantes backups do sistema evitaram maiores danos.

Em relação a métodos que envolvam o fator humano, como treinamento de pessoal e criação de novos cargos, estratégias citadas por Nagli (2020), Okano et al. (2020) e Rodrigues Jr. et al. (2021), refletem exigências trazidas pela Lei Geral de Proteção de Dados Pessoais (AZEVEDO; OLIVEIRA, 2020; RODRIGUES Jr. et al., 2021). Desta forma, o treinamento de pessoal e o investimento em profissionais especializados em segurança da informação para cargos de os *Chief Information Security Officer* e *Chief Information Officer*, são fortes tendências para a segurança da inormação, pois ocupando esses cargos, profissionais

qualificados deverão planejar e implementar processos e estratégias de segurança, seguindo orientações da legislação específica vigente (RODRIGUES Jr. et al., 2021).

Como parte dos resultados, também, podemos conhecer ferramentas e métodos de proteção de redes mais utilizados na pandemia (Quadro 2). Como já descrito, a proteção do tráfego de informações (VPN e firewall) foi o método mais citada como tendências de segurança da inormação. No entanto, sendo mais específico, obtivemos o uso de VPN presente em 7 dos 9 artigos, representando 77,8% da amostra, sendo citado por Lema (2021), Nagli (2020), Okano et al. (2020), Peres et al. (2020), Rodrigues Jr. et al. (2021), Silva et al. (2020) e Suarez et al. (2020).

O uso de firewall foi citado em 5 artigos, ou seja, 55,6% da amostra, estando presente nos trabalhos de Nagli (2020), Okano et al. (2020), Peres et al. (2020), Rodrigues Jr. et al. (2021) e Suarez et al. (2020). Uma rede de computadores privada ao utilizar um meio público de comunicação, ou seja, a internet, entrará em contato com um meio inseguro, sendo recomendado do uso de protocolos de segurança que envolvam firewall ou VPNs.

Como forma de proteção de conexões e tráfego de informações, o firewall age basicamente monitorando a entrada e saída de dados da rede ou computador, atuando como um filtro. Caso o pacote de entrada de informações seja sinalizado como perigoso na filtragem do firewall, não será permitido o acesso a ele (NAGLI, 2020; OKANO et al. 2020).

A VPN ou Rede Privada Virtual é uma rede privada e protegida constituída através da Internet, ela agrega soluções de segurança como criptografia, autenticação e protocolos que visam a proteção do tráfego de dados (LEMA, 2021; NAGLI, 2020; OKANO et al., 2020). Trata-se de uma forma de extensão de rede segura que criada sem dispositivos conectados uns aos outros fisicamente (SUAREZ et al., 2020). Ao usar uma VPN, o usuário se conecta aos serviços de Internet do provedor, mas não de uma forma direta, garantindo a confidencialidade dos dados.

Além de VPN e firewall para proteção de tráfego, ressalta-se o uso de antivírus como um método considerado essencial e sempre recomendado para segurança da informação, enquanto a autenticação de senhas por duplo fatores vem sendo cada vez mais comum para o acesso a redes privadas.

Com relação as vulnerabilidades e ataques cibernéticos descritos nos resultados (quadro 3), pode-se observar que as formas mais abordadas nos artigos foram ataques por aplicativos maliciosos, *phishing* e *fake news*. Ameaças de aplicativos maliciosos (Vírus, *ransomwares*, *malspams*, trojans, *Spyware*, *Adware* etc.) foram aludidos em 7 artigos, representando 77,8% da amostra (AZEVEDO; OLIVEIRA, 2020; LEMA, 2021; MEDEIROS

et al., 2020; NAGLI, 2020; OKANO et al., 2020; RODRIGUES Jr. et al., 2021; SUAREZ et al., 2020). Ataques por técnica de *phishing* foram citados em 4 artigos (MEDEIROS et al., 2020; NAGLI, 2020; SUÁREZ et al., 2020; LEMA, 2021), ou seja 44,4% da amostragem. A disseminação de *fake news* foi referenciada em 33,3% dos artigos da revisão, estando presente em 3 artigos (AZEVEDO; OLIVEIRA, 2020; MEDEIROS et al., 2020; NAGLI, 2020).

Outras formas de ataques e vulnerabilidades descritas foram, o ataque de Cross-site scripting (RODRIGUES Jr. et al., 2021; SUÁREZ et al., 2020), DDoS Attack (MEDEIROS et al., 2020; NAGLI, 2020, "uso incorreto da tecnologia" (SUÁREZ et al., 2020; NAGLI, 2020), além de SQL Injection e EAC, descritas apenas por Suárez et al. (2020), em seu artigo sobre a importância da segurança cibernética e os tipos de ciberataques a nível mundial.

Junto com o aumento de ataques no período de pandemia, registros apontam a criação domínios que sugerem conter informações sobre o Novo Coronavírus e cuidados com a pandemia, porém, na verdade, são domínios maliciosos considerados de alto risco (NAGLI, 2020; RODRIGUES Jr. et al., 2021). Tais informações indicam uma crescente onda de técnicas como *phishing*, para a disseminação de *fake news* e aplicativos maliciosos, assim podemos observar que os ataques envolvendo *phishing* e *fake news* e aplicativos maliciosos basicamente agem em conjunto.

Dentre os aplicativos maliciosos, os *ransomwares* tem sido os mais abordados recentemente, inclusive abalando a administração pública (MEDEIROS et al., 2020). Trata-se de uma forma de *malware* que age em um esquema de sequestro de informações, que pode ser instalado por técnica de *phishing* (LEMA, 2021; MEDEIROS et al., 2020; NAGLI, 2020; SUAREZ et al., 2020). Os *ransomwares* agem criptografando o conteúdo de um dispositivo restringindo o acesso ao sistema infectado, assim, há cobrança um resgate em criptomoedas, caso não ocorra o pagamento, arquivos podem ser perdidos e até mesmo publicados (MEDEIROS et al., 2020; NAGLI, 2020).

A técnica de *phishing* é muito utilizada para a distribuição de conteúdo malicioso e captura de informação, onde geralmente é utilizado um e-mail com intuito de a confundir o usuário e fazê-lo a acessar arquivo ou link que o desvia para um site ou programa malicioso (LEMA, 2021; MEDEIROS et al., 2020; NAGLI, 2020; SUAREZ et al., 2020).

As *fake news* são encontradas em portais de notícias e outros sites, também são enviadas por e-mail ou redes sociais, apresentando temas chamativos e imagens manipuladas. Desta forma, atraem a atenção de usuários, guiados pela curiosidade ou busca de informação, que ao clicarem nos links dessas notícias, são direcionados para sites maliciosos ou para

instalação de vírus, *spywares* e afins (AZEVEDO; OLIVEIRA, 2020; MEDEIROS et al., 2020; NAGLI, 2020).

A “infodemia” criada na pandemia do Novo Coronavírus, não só representa a disseminação de informações falsas a respeito da doença, mas também, como já descrito, contribuí para ataques cibernéticos envolvendo *phishing* e aplicativos maliciosos, tendo em vista usuários na busca de informações sobre a covid-19.

Medeiros et al. (2020), Nagli (2020), Rodrigues Jr. et al. (2021) e Suárez et al. (2020) abordaram ataques e vulnerabilidades como *Cross-site scripting*, Ataque DDoS, *SQL Injection,* que são mais direcionadas a sites e bancos de dados. Apesar de serem menos citadas nos artigos em geral, tratam-se de ataques bem comuns reportados há tempos.

O Cross-site scripting, ocorre nas aplicações que recebem dados do usuário e o enviam ao navegador sem validação ou codificação. Permite roubo da sessão do usuário, roubo de dados, reescrever da página e redirecionar do usuário a outra página (RODRIGUES Jr. et al., 2021; SUÁREZ et al., 2020).

O Ataque DDoS é uma forma de negação de serviço, implica em tornar os recursos de um sistema indisponíveis para os usuários, comum a servidores web, não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga (MEDEIROS et al., 2020; NAGLI, 2020).

O SQL *Injection* é uma técnica de ataque baseada na manipulação do código SQL, o ataque ocorre em aplicações que recebem dados do usuário e os envia a um interpretador sem validar ou codificar os dados, permitindo realizar diversas modificações nas aplicações e informações, inclusive apagar ou criar novos dados (SUAREZ et al., 2020).

No caso do ataque de EAC (*E-mail Account Compromise*), ou Ataques de Comprometimento de Conta de E-mail, trata-se de uma invasão e-mails comerciais ou pessoais, por meio da criação de contas de e-mail com domínios semelhantes ao do usuário ou instituições, mascarando sua conta de e-mail como legítima, geralmente envolve fraudes solicitando pagamentos por transferência eletrônica (SUÁREZ et al., 2020).

Em relação ao “uso incorreto da tecnologia”, Suárez et al. (2020) destaca a importância de empresas investirem no treinamento técnico dos funcionários, pois estes seriam o elo mais fraco da cadeia de segurança, e caso este elo não seja fortalecido, se tornará a base do problema da segurança da informação. Nagli (2020) expõe que muitas vezes a causa da violação da segurança é o uso indevido de computadores, dispositivos móveis ou aplicações de segurança por funcionários.

Sobre as principais dificuldades apontadas na implantação de sistemas de segurança da informação (quadro 4), a aquisição de Infraestrutura e equipamentos foi a mais registrada, sendo citada em 5 artigos (AZEVEDO; OLIVEIRA, 2020; MEDEIROS et al., 2020; NAGLI, 2020; OKANO et al., 2020; SUAREZ et al., 2020), representando 55,6% da amostra. O "fator humano" foi apontado em 4 publicações (AZEVEDO; OLIVEIRA, 2020; NAGLI, 2020; PERES et al., 2020; SUAREZ et al., 2020), correspondendo a 44,4 % dos artigos. A "falta de profissionais de segurança da informação" apontado em apenas 2 publicações (NAGLI, 2020; RODRIGUES Jr. et al., 2021), representando 22,2 % das publicações.

Um grande desafio para as empresas foi viabilizar nova infraestrutura de TI em pouco tempo para uma grande quantidade de usuários remotos. Para Nagli (2020), muitas empresas tiveram suas primeiras experiências de trabalho remoto somente ao se adaptar para pandemia, em um cenário de calamidade repleto de novos desafios. Alguns estabelecimentos, por exemplo, enfrentaram desde a falta de computadores para aluguel, passando pela inexperiência de funcionários, até o pouco embasamento para criação de políticas de segurança da informação para a aplicação do trabalho remoto (RODRIGUES Jr. et al., 2021).

Segundo Rodrigues Jr. et al. (2021), para adoção do *home office* uma empresa deve garantir ferramentas que possibilitem o funcionamento de redes de computadores e Internet em segurança, para que assim os funcionários consigam executar suas tarefas sem riscos. Ressalta-se que grandes empresas ou empresas estatais, apesar de apresentarem menores dificuldades para implantação de tecnologias de segurança, tem como desafios o treinamento, capacitação de pessoal e estímulo a produtividade.

Em relação ao fator humano, boa parte dos ataques a segurança da informação de empresas é causada por falha humana em cuidados técnicos, problemas na configuração dos sistemas e mal-uso das ferramentas de segurança (NAGLI, 2020; SUAREZ et al., 2020). Assim refletindo falta de treinamento adequado e atualização de funcionários.

A falta de profissionais especializados na área de segurança cibernética é uma dificuldade apontada por Nagli (2020) e Rodrigues Jr. et al (2021), os autores reforçam a importância destes profissionais para a implementação ações e políticas de segurança, assim como implantação ferramentas, que envolvam a proteção de dados e informações da companhia.

Na atual pandemia de covid-19, as empresas devem optar por serviços atualizados e de última geração, porem a busca por recursos adequados ao momento, pode ser algo bastante oneroso, principalmente para pequenas empresas. Uma forma de amenizar tal

situação emergencial seriam o estímulo a programas de auxílio ao empreendedor à implantação de métodos de segura da informação e correção das vulnerabilidades.

5 CONSIDERAÇÕES FINAIS

O presente estudo de revisão possibilitou identificar as tendências de segurança da informação no cenário de pandemia da covid-19, através do conhecimento de métodos de segurança da informação, descrevendo vulnerabilidades e apontando as principais dificuldades da implantação de sistemas de segurança para o trabalho a distância na pandemia.

Com relação a adaptação ao atual cenário de crise sanitária, houve um período muito curto, no entanto, a modalidade de trabalho *home office*, que antes era uma opção em curso para algumas empresas, teve uma exacerbada requisição, devido a pandemia e ao distanciamento social, atualmente impostos. Porém, representa uma forma eficaz de continuar os serviços diversos, a fim de evitar mais danos econômicos.

A adequação para a digitalização de múltiplos serviços, foi um grande desafio para muitas empresas, antes sem uma estrutura de TI robusta, muitas tiveram um grande custo para suportar a demanda de tráfego de dados, enquanto outras tiveram seus serviços paralisados. Além disso, enfrentaram dificuldades como o treinamento para uso de novas as ferramentas, reuniões remotas e ensino remoto.

Nunca a população foi tão dependente da tecnologia, cada vez mais conectados e vivendo um mundo mais virtual, utilizando a Internet de diversas formas, exigindo aplicações das tecnologias da informação e comunicação em função da adaptação para o “novo normal”. Nesse sentido, a modalidade de trabalho *home office* oferece várias oportunidades e desafios.

Porém, a rápida adaptação para o trabalho em online, também resultou em amplas formas de vulnerabilidades, refletido nos altos registros de crimes digitais no período pandemia, principalmente envolvendo aplicativos maliciosos, técnicas de *phishing* e a ampla disseminação de *fake news*.

A disseminação de notícias falsas foi um dos principais ataques registrados no cenário da segurança da informação na pandemia. O compartilhamento de *fake news*, além de atuar no processo de desinformação prejudicando os cuidados com a saúde físicas e mental da população, também, se trata de uma forma de ataque cibernético que atua na invasão de sistemas de informação e redes de computadores. É inevitável uma maior preocupação com a segurança de dados, desta forma, investir segurança cibernética fará total diferença no combate ao ataque de hackers.

Uso das tecnologias digitais para adequação de empresas ao *home office* representam imensos desafios na área de segurança da informação, seja na implementação de

infraestrutura e treinamento de pessoal, visando o total respeito aos direitos fundamentais de privacidade. As empresas devem estar preparadas para enfrentar ameaças cibernéticas ou poderão sofrer graves consequências de incidentes relacionados à segurança da informação.

O presente estudo reforça a importância do investimento em segurança da informação no atual cenário da pandemia de covid-19. Com o aumento do número de ataques a aplicações web, torna-se de fundamental que as empresas optem por serviços de segurança da informação atualizados, para garantir o bom funcionamento de suas atividades e segurança de dados. Programas de auxílio ao empreendedor poderiam fornecer recursos básicos a pequenas empresas, contribuindo para o fornecimento de infraestrutura segura da informação adequada para a correção das vulnerabilidades.

REFERÊNCIAS

AQUINO, Estela M. L. et al. Medidas de distanciamento social no controle da pandemia de COVID-19**:** potenciais impactos e desafios no Brasil. **Ciênc. saúde coletiva**, Rio de Janeiro , v. 25, supl. 1, p. 2423-2446, jun. 2020.

AZEVEDO, Viviane Ramalho de; OLIVEIRA, Adriano Caires de. O impacto das *fake news* na segurança da informação e sua influência no cotidiano das pessoas. **SEGeT**, Resende, v.17, jan. 2020.

BARBOSA, Juliana Souza et al. A proteção de dados e segurança da informação na pandemia COVID-19**:** contexto nacional. **Research, Society and Development**, São Paulo, v. 10, n. 2, e40510212557, fev. 2021.

BORGES, Letícia Lima et al. Enfermagem Militar na "Operação Regresso ao Brasil": evacuação aeromédica na pandemia do coronavirus. **Rev. Bras. Enferm.**, Brasília, v. 73, supl. 2, e20200297, jun. 2020.

BORTOLUZZI, Michel. **Análise crítica da aplicação de uma política de segurança da informação (PSI) em empresa do setor financeiro**: um estudo de caso. 2016. 112 f. Monografia de graduação (Tecnologias da Informação e Comunicação) Universidade Federal de Santa Catarina, Santa Catarina, 2016.

BOTELHO, Louise Lira Roedel; CUNHA, Cristiano Castro de Almeida; MACEDO, Marcelo. O método da revisão integrativa nos estudos organizacionais. **Gestão e Sociedade**. Belo Horizonte, v.5, n. 11, p. 121-136, maio-ago. 2011.

BRASIL. Ministério da Saúde. **Coronavírus:** o que você precisa saber e como prevenir o contágio. Disponível em: https://saude.gov.br/saude-de-a-z/coronavírus. Acesso em 18 de fev. 2021.

BRIK**,** Marina Sell**;** BRIK**,** André. **Trabalho portátil**: Produtividade, economia e qualidade de vida no *home office* das empresas. Curitiba: AB, 2021.

BROOME, Marion. English. Integrative literature reviews for the development of concepts. *In*: RODGERS, Beth. L.; KNAFL, Kathleen Astin A.(orgs). **Concept development *in* nursing:** foundations, techniques and applications. Philadelphia: W.B Saunders Company; 2000. p.231-50.

CAETANO, Rosângela et al. Desafios e oportunidades para telessaúde em tempos da pandemia pela COVID-19: uma reflexão sobre os espaços e iniciativas no contexto brasileiro. **Cad. Saúde Pública**, Rio de Janeiro, v. 36, n. 5, e00088920, jun. 2020.

CARDOSO, Nágila Magalhães. A Pandemia do Cibercrime. **Revista Eletrônica Direito & TI**, Canoas, v. 1, n. 12, p. 8, 26 jun. 2020.

CSSE/COVID-19 DATA. GitHub - CSSEGISandData/COVID-19: Novel Coronavirus (COVID-19) Cases, provided by JHU CSSE [2021]. Disponível em:

https://dadoscoronavirus.dasa.com.br/?_ga=2.104610434.325351966.1617685714-139279481.1617685714#lp-pom-block-960. Acesso em: 28 mar. 2021.

D'ANGELO, Isabele Bandeira de Moraes et al. O avanço do coronavírus e os desafios para o cuidado da saúde nas comunidades vulneráveis no Estado de Pernambuco, Brasil. **Research, Society and Development**, Vargem Grande Paulista, v. 9, n. 8, p. e855986428. Jul. 2020.

DRUMMOND, Giulia de Pinho. Teletrabalho**:** duração do trabalho e impactos da Covid-19. **Revista do Tribunal Regional do Trabalho da 10ª Região**, Brasília, v. 24, n. 1, p. 109-117, ago. 2020.

ERCOLE, Flávia Falci; MELO, Laís Samara de; ALCOFORADO, Carla Lúcia Goulart Constant. Revisão Integrativa versus Revisão Sistemática. **Ver. Min. Enferm**., Minas Gerais, v. 18, n. 1, p. 1-260, jan. / mar. 2014.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. São Paulo: saraiva, 2006.

GARCIA, Fábio Luiz. **Defesa cibernética brasileira:** panorama atual e evolução das ameaças e vulnerabilidades existentes no Ciberespaço. 2020. 25f. Monografia (Especialização em Ciências Militares) - Escola de Formação Complementar do Exército e Colégio Militar de Salvador, Salvador. 2020.

GARCIA, Leila Posenato; DUARTE, Elisete. Intervenções não farmacológicas para o enfrentamento à epidemia da COVID-19 no Brasil. **Epidemiol. Serv. Saúde**, Brasília, v. 29, n. 2, e2020222, abr. 2020.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. São Paulo: Atlas, 2008.

GREENHALGH, Trisha; KOH, Gerald Choon Huat; CAR, Josip. Covid-19: avaliação remota em Atenção Primária à Saúde. **Ver. Bras. Med. Fam. Com**, Rio de Janeiro, v. 15, n. 42, p. 2461, abr. 2020.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais:** administrando a empresa digital. 5. ed. São Paulo: Person Pretice Hall, 2006.

LEITE, Hudson Oliveira. **O impacto da segurança da informação nas empresas de prestação de serviços bancários:** um estudo em uma empresa personalizadora de cartões de pagamento bandeirados. 2017. 119 f. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento) - Faculdade de Ciências Empresariais, UNIVERSIDADE FUMEC, Belo Horizonte, 2017.

LEMA, Luis López. La gestión de la información durante etapas de teletrabajo en la época de la COVID-19. **Perspectivas**. Buenos Aires, n. 3, p. 91-109, jan. 2021.

LIMA, Luana Nepomuceno Gondim Costa; SOUSA, Maisa Silva de; LIMA, Karla Valéria Batista. As descobertas genômicas do SARS-CoV-2 e suas implicações na pandemia de COVID-19. J. **Health Biol. Sci.** Belém, v. 8, n. 1, p. 1-9, jan. 2020.

LOSEKANN, Gonçalves Caldeira Brant; CARDOSO, Helena Cardoso. **Desafios do teletrabalho na pandemia Covid-19**: quando o home vira office. **Caderno de Administração**, Maringá, v. 28, p. 71-75, 5 jun. 2020.

MARASCA, Aline Riboli et al. Avaliação psicológica online: considerações a partir da pandemia do novo coronavírus (COVID-19) para a prática e o ensino no contexto a distância**. Estud. psicol.**, Campinas, v. 37, e200085, jun. 2020.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco; BATISTA JR, Eliezer; ROCHA, Henrique Ribeiro da. O uso do ciberespaço pela administração pública na pandemia da COVID-19: diagnósticos e vulnerabilidades. **Rev. Adm. Pública**, Rio de Janeiro, v. 54, n. 4, p. 650-662, Ago. 2020.

MENDES, Karina Dal Sasso; SILVEIRA, Renata Cristina de Campos Pereira; GALVAO, Cristina Maria. Revisão integrativa: método de pesquisa para a incorporação de evidências na saúde e na enfermagem. **Texto & contexto - Enfermagem**, Florianópolis, v. 17, n. 4, p. 758-764, dez. 2008.

NAGLI, Luiz Sergio Dutra**.** Pandemia na pandemia: a escalada de ataques cibernéticos pós Covid-19. **Repos. FGV de Conf**. nov. 2020.

OKANO, Marcelo; SANTOS, Henry de Castro Lobo dos; HONORATO, William Johnny; VIANA, Alex Maia; URSINI, Edson L. Impactos da pandemia Covid-19 em empresas de grande porte**:** avaliação das mudanças na infraestrutura de tecnologia para o teletrabalho sob as óticas das teorias das capacidades dinâmicas e estrutura adaptativa. **Research, Society and Development**, Vargem Grande Paulista, v. 9, n. 9, e756997852, set. 2020.

OLIVEIRA, Adriana Cristina de; LUCAS, Thabata Coaglio; IQUIAPAZA, Robert Aldo. O que a pandemia da covid-19 tem nos ensinado sobre adoção de medidas de precaução?. **Texto contexto - enferm**., Florianópolis, v. 29, e20200106, maio 2020.

OPAS/OMS. ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE / ORGANIZAÇÃO MUNDIAL DA SAÚDE. Ocorrência de variantes de SARS-CoV-2 nas Américas**,** 20 de janeiro de 2021. Brasilia, D.F.: **Organização Pan-Americana da Saúde**. 2021.

PERES, Milena de Avila et al. Segurança e legitimidade no trabalho remoto - Relato de experiência em um Hospital Público e Universitário. **Clinical & Biomedical Research**, Porto Alegre, v. 40, n. 2, fev. 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

POMPEO, Daniele Alcalá; ROSSI, Lídia Aparecida; GALVAO, Cristina Maria. Revisão integrativa: etapa inicial do processo de validação de diagnóstico de enfermagem. **Acta Paulista de Enfermagem**, São Paulo, v. 22, n. 4, p. 434-438, abr. 2009.

RODRIGUES JR., Ed Wilson; NOGUEIRA, Edson Rodrigo Luciano; MENDES, Gabriel Fonseca; CAMPOS, Lucas Afonso da Silva. *Home office* e a segurança da informação em tempos de pandemia. **Ver. El. Fac. Inv. Ciên. Tecn.**, Cuiabá, v. 3 n. 1, jan. 2021.

ROLFINI, Fabiana. **Cibercrime:** ataques no Brasil aumentam mais de 300% com a pandemia. Olhar digital, 2020. Disponível em: https://olhardigital.com.br /fique_seguro /noticia/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/103030. Acesso em: 27 de outubro de 2020.

ROSENVALD et al. **Coronavírus e responsabilidade civil**: Impactos contratuais e extracontratuais. Indaiatuba: foco, 2020.

SANTOS, Mónica; ALMEIDA, Armando; LOPES, Catarina; OLIVEIRA, Tiago. Teletrabalho na perspectiva da Saúde Ocupacional. **Revista Portuguesa de Saúde Ocupacional on line,** Gondomar v. 10, p.1-35, set. 2020.

SAUNDERS, Mark; LEWIS, Philip; THORNHILL, Adrian. **Research Methods for Business Students**. 5. ed. Lodon: Pearson Education, 2009.

SILVA, Sandro Luis Freire de Castro; SANTOS, Rodrigo Pereira dos; FORNAZIN, Marcelo; GONÇALVES, Antônio Augusto. A estratégia de tecnologia da informação e os sistemas emergentes no plano de gerenciamento de crise da Covid-19 no Instituto Nacional de Câncer. **Ver. Adm. Hosp. Inov. Saúde**, Belo Horizonte, n. 17, n. 2, e-2177-2754, abr/jun 2020.

SOUSA, Anderson Reis de et al. **Tecnologias educativas em saúde e enfermagem no enfrentamento à pandemia do coronavírus.** 1. ed. Piracanjuba-GO: Conhecimento Livre, 2020.

SOUZA, Marcela Tavares de; SILVA, Michelly Dias da; CARVALHO, Rachel de. Revisão integrativa: o que é e como fazer. **Einstein.** São Paulo, v. 8, n. 1, p. 102-106, mar. 2010.

SUÁREZ, José Luis Gamboa**. Importancia de la seguridad informática y ciberseguridad en el mundo actual. Inst. Rep. Univ Pil Col**. Bogotá, ago. 2020.

TEIXEIRA, Lucas Costa; DIEL, Vinicius Schvambach. **Engenharia Social e segurança da informação**: análise focada nos profissionais de uma empresa de tecnologia. 2020. 134 f. Monografia (Bacharelado em Sistemas da Informação) - Universidade do Sul de Santa Catarina, Florianópolis, 2020.

VARELLA, Walter Augusto. **Implementação e migração para computação em nuvem**. São Paulo: SENAC, 2019.

WHITTEMORE, Robin; KNAFL, Kathleen. The integrative review**:** updated methodology. **Journal of advanced nursing**. v.52, n. 5, p. 546–553, dez. 2005.