

**FACULDADE DE TECNOLOGIA DE SÃO PAULO**

**VINICIUS CASTILHO GAIA**

**QUAIS MEDIDAS DE CIBERSEGURANÇA AS EMPRESAS TIVERAM DE TOMAR  
DURANTE A PANDEMIA EM RELAÇÃO À MODALIDADE HOME OFFICE?**

**SÃO PAULO**

**JUNHO / 2021**

**FACULDADE DE TECNOLOGIA DE SÃO PAULO**

**VINICIUS CASTILHO GAIA**

**QUAIS MEDIDAS DE CIBERSEGURANÇA AS EMPRESAS TIVERAM DE TOMAR  
DURANTE A PANDEMIA EM RELAÇÃO À MODALIDADE HOME OFFICE?**

Trabalho submetido como exigência parcial

para a obtenção do Grau de Tecnólogo em

Análise e Desenvolvimento de Sistemas.

Orientadora: Mestre Edméa Pujol Cantón.

**SÃO PAULO**

**JUNHO / 2021**

**FACULDADE DE TECNOLOGIA DE SÃO PAULO**

VINICIUS CASTILHO GAIA

**QUAIS MEDIDAS DE CIBERSEGURANÇA AS EMPRESAS TIVERAM DE TOMAR DURANTE A PANDEMIA EM RELAÇÃO À MODALIDADE HOME OFFICE?**

Trabalho submetido como exigência parcial para a obtenção do  
Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Parecer do Professor Orientador

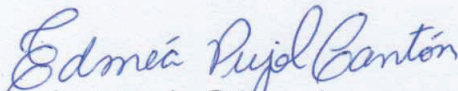
O Trabalho de Conclusão de Curso do aluno Vinicius Castilho Gaia atendeu à todas as exigências do DTI e da Fatec - SP.

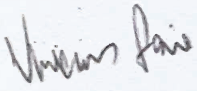
Conceito/Nota Final: 10.0

Atesto o conteúdo contido na postagem do ambiente TEAMS pelo aluno e assinada por mim para avaliação do TCC.

Orientadora: Mestre Edméa Pujol Cantón.

SÃO PAULO, 21 de junho de 2021.

  
Assinatura do Orientador

  
Assinatura do aluno

## **DEDICATÓRIA**

Dedico esse trabalho a todos meus familiares e amigos, os quais me apoiaram e incentivaram durante o processo inteiro de realização desse projeto.

## **AGRADECIMENTOS**

Agradeço primeiramente a meus familiares e amigos, por todo o apoio no decorrer dessa jornada e por não me deixar desanimar e continuar sempre buscando a conclusão dessa etapa de minha vida.

Muito obrigado a meus professores, que me auxiliaram de inúmeras maneiras durante esse período, transmitindo todo conhecimento possível e sempre me guiando pelo melhor caminho para minha formação, não apenas profissional, como também pessoal.

Muito obrigado aos profissionais e técnicos da faculdade, pelo esforço dedicado a me ajudar na concretização de minhas ideias e pela contribuição na produção de meus projetos.

E por fim, muito obrigado a Edméa Pujol Cantón, minha orientadora, pela confiança em meu trabalho e pela colaboração com tudo que precisei para desenvolvê-lo.

*“Família é muito mais do que sangue e um nome.  
São as pessoas que ficaram ao seu lado quando você precisou delas  
e que fizeram você sorrir quando sentiu que não conseguiria mais.”*

Autor desconhecido

## RESUMO

GAIA, Vinicius Castilho. **Quais medidas de cibersegurança as empresas tiveram de tomar durante a pandemia em relação à modalidade home office?** 2021. 31 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas) - Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2021.

A área de segurança da informação está em constante crescente no mundo empresarial. Baseado nisso, muitas empresas buscam investir nesse setor, a fim de garantir mais proteção para os negócios.

O propósito deste estudo foi analisar o cenário de segurança da informação nas organizações e identificar as mudanças ocorridas devido a pandemia do coronavírus, como a crescente do home office.

A abordagem englobou levantamento e análise de dados, pesquisas, relatórios e estudos, tanto referentes a pandemia quanto a área de segurança da informação no contexto geral.

Entre os objetivos desse projeto, estão os de impactar as empresas, de forma a alertar sobre os perigos que possam prejudicar sua organização e conscientizar as pessoas para que possam se comportar de maneira mais adequada em ambientes virtuais.

**Palavras-chave:** cibersegurança, home, office, segurança, informação, trabalho, remoto, pandemia, coronavírus.

## ABSTRACT

GAIA, Vinicius Castilho. **What cybersecurity measures did companies have to take during the pandemic in relation to the home office modality?** 2021. 31 s. Term Paper (Higher Technology Degree in Systems Analysis and Development) - Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2021.

The area of information security is constantly growing in the business world. Based on this, many companies are looking to invest in this sector in order to ensure more protection for the business.

The purpose of this study was to analyze the information security scenario in organizations and identify the changes that occurred due to the coronavirus pandemic, such as the growing of home office.

The approach included data collection and analysis, surveys, reports and studies, both referring to the pandemic and the area of information security in the general context.

Among the objectives of this project are the ones to impact companies, in order to warn about the dangers that may harm their organization and raise people awareness so that they can behave more appropriately in virtual environments.

**Keywords:** cybersecurity, home, office, information, security, remote, work, pandemic, coronavirus.



## SUMÁRIO

INTRODUÇÃO.....	13
1. SEGURANÇA DA INFORMAÇÃO.....	17
1.1. Cibersegurança.....	17
1.2. Valor empresarial.....	17
2. TRABALHO REMOTO.....	18
2.1. Home office.....	18
2.2. Principais benefícios.....	19
2.3. Principais dificuldades.....	19
2.4. Expectativas para o futuro.....	20
3. SOLUÇÕES.....	21
3.1. Principais ameaças.....	21
3.2. Principais alvos.....	22
3.3. Rede Privada Virtual.....	23
3.4. Criptografia.....	24
3.5. Autenticação.....	24
3.6. Antivírus.....	24
3.7. Conscientização.....	25
CONCLUSÃO.....	26
REFERÊNCIAS BIBLIOGRÁFICAS.....	27

## LISTA DE FIGURAS

FIGURA 1 – VPN <i>Tunnel</i> .....	23
------------------------------------	----

## **LISTA DE GRÁFICOS**

GRÁFICO 1 – Aumento de trabalhadores remotos com o início da pandemia.....	18
GRÁFICO 2 – Nos próximos 12 meses, as empresas pretendem:.....	20
GRÁFICO 3 - Distribuição de ataques empresariais.....	22

## LISTA DE TABELAS

TABELA 1 – <i>Additional data</i> .....	25
---	----

## LISTA DE ABREVIATURAS E SIGLAS

COVID-19.....*Corona Virus Disease 2019*

MFA.....*Multi-Factor Authentication*

OMS.....*Organização Mundial da Saúde*

SARS-CoV-2.....*Severe Acute Respiratory Syndrome Coronavirus 2*

TI.....*Tecnologia da Informação*

VPN.....*Virtual Private Network*

Wi-Fi.....*Wireless Fidelity*

## INTRODUÇÃO

### Contextualização histórica

Aproximadamente no final do ano de 2019, o mundo começava a tomar conhecimento sobre um novo vírus, que a princípio afetava apenas China, mais precisamente a cidade de Wuhan, capital da província de Hubei, e, portanto, não causou tanto alarde mundo a fora. Até então, com somente alguns casos registrados, pouco se sabia sobre o vírus e o que esse poderia causar a humanidade, situação que não demorou muito a mudar, e logo chamar a atenção de todos ao redor do planeta.

COVID-19 é a doença causada pelo vírus SARS-CoV-2, a qual pode apresentar-se como uma infecção branda, mas pode também desencadear pneumonia, insuficiência respiratória e até a morte.

Mesmo com a quarentena decretada na cidade de Wuhan, considerada o epicentro da pandemia, a doença não ficou restrita àquela localidade e logo espalhou-se, primeiramente, pela China, em seguida, Ásia e, assim, para outros países no mundo todo.

Com o aumento de casos da doença registrados pelo mundo, milhares de mortos em centenas de países, a Organização Mundial de Saúde (OMS) optou por decretar estado de pandemia.

### Apresentação do Problema

Antes da pandemia e da necessidade de aplicação do distanciamento social, trabalhar na própria casa era visto como um sonho, almejado por muitos. Com essa prática se tornando cada vez mais comum, essa concepção foi alterada, mostrando aos poucos todas as adversidades que caminhavam juntas e eram ofuscadas pela parte gloriosa dessa ideia.

Home office, trabalho a distância, teletrabalho, trabalho remoto, entre tantos outros termos, tem a mesma função: definir esse regime, onde as pessoas passam a não precisar mais ir até o escritório para exercer suas funções diárias e obrigações relacionadas a empresa onde são contratadas. Um conceito que já era conhecido por

todos a muito tempo, porém diversas empresas relutavam contra esse processo, com medo de consequências improdutivas. Já com a pandemia estabelecida, muitas empresas se viram obrigadas a se adaptar a fim de não sofrer mais baixas além do inevitável.

O trabalho a distância tem muitos benefícios, tanto para as empresas quanto para seus funcionários, mas nem tudo na vida acontece como a gente quer, a vida é cheia de incertezas e desafios. Para funcionários, o grande problema dessa questão está relacionado a conciliar o trabalho com o ambiente familiar, principalmente quando tem crianças envolvidas, as quais no momento também estão sendo obrigadas a realizar seus estudos remotamente.

Já as empresas ganham novas preocupações, além da dificuldade de implementar esse regime de trabalho a sua rotina, também irão indiretamente perder grande parte do controle sobre a rotina do empregado, o que envolve suas práticas durante o expediente, principalmente envolvendo os dados e equipamentos das empresas. Isso tudo depende da familiaridade dos funcionários com as novas ferramentas, principalmente de comunicação, além da inerente preocupação com o comportamento e cuidado dos trabalhadores ao acessarem os ambientes virtuais da empresa.

Neste novo contexto em que estamos vivendo, quais medidas de cibersegurança as empresas tiveram de tomar durante a pandemia em relação à modalidade home office?

## **Objetivo Geral**

No projeto apresentado a seguir, trataremos sobre os impactos causados pela pandemia do coronavírus no ambiente corporativo, onde pretendemos abordar tecnologias, ferramentas, práticas e comportamentos que serviram, servem e continuarão servindo por algum tempo, de apoio as empresas durante esse período, principalmente no que diz respeito a adaptação ao cenário e os desafios do regime de trabalho remoto, mais especificamente do home office, focando no âmbito da segurança da informação, mais especificamente da cibersegurança.

## **Objetivos Específicos**

Os objetivos específicos do presente trabalho são:

- pesquisar ferramentas disponíveis de cibersegurança focadas no regime de trabalho home office;
- identificar as ferramentas que foram adotadas por empresas do setor financeiro;
- apresentar as soluções que obtiveram maior sucesso.

## **Justificativa**

A principal motivação para o desenvolvimento desse estudo foram as duas mais recentes vivências profissionais do autor, ambas situadas em lados completamente opostos dessa mesma história, ambientadas durante o período pandêmico.

A primeira delas ocorreu no início do surto. Enquanto grande parte das empresas adotaram o regime de teletrabalho, instituindo o distanciamento social e visando a proteção da saúde das pessoas, a empresa em que o autor trabalhava não optou por essa mudança e durante um ano esteve correndo riscos a fim de manter seu emprego.

A seguinte, vem ocorrendo durante o desenvolvimento desse projeto. Ao deixar o primeiro emprego, o autor teve a oportunidade de entrar em uma nova empresa, a qual está trabalhando atualmente, e nela foi aderido o conceito de home office, no qual está experienciando pela primeira vez em sua carreira. Com essa mudança, outras preocupações surgiram em seu cotidiano e agregaram aos objetos desse estudo, principalmente se relacionando a segurança da informação e a proteção de dados sensíveis.

## **Metodologia de Pesquisa**

O presente trabalho foi realizado através diversos estudos e consulta a objetos referentes ao assunto em questão e fundamentado em variados artigos publicados na internet, seguindo a premissa de pesquisa bibliográfica.



Segundo Marconi e Lakatos em “Fundamentos de Metodologia Científica”, pesquisa bibliográfica trata-se do levantamento de toda e qualquer informação já publicada, em forma de livros, revistas, publicações, artigos, ou qualquer outra forma de reprodução textual.

Essa variante da metodologia de pesquisa tem como objetivo construir o contato do pesquisador diretamente com todo o material disponível sobre um determinado assunto, assim auxiliando-o na análise de seus estudos ou na manipulação de suas informações, agregando ao seu trabalho.

### **Estrutura do Trabalho**

Na introdução, foi realizada uma contextualização histórica, em seguida apresentada a consequente questão problema do trabalho. Além disso, foram apresentados também os objetivos do projeto, tanto o geral quanto os específicos. Por fim, foi relatada a justificativa que motivou o desenvolvimento do estudo e a metodologia de pesquisa utilizada no decorrer do processo.

O desenvolvimento foi repartido em três capítulos, onde o primeiro busca ambientar a área de estudo, no caso segurança da informação, apresentando aspectos técnicos e aprofundando conceitos que servirão de base para o restante do projeto.

A partir do segundo capítulo, o foco passa a ser o trabalho remoto e suas características, abordando possíveis problemas relacionados a essa modalidade de emprego e as principais mudanças e seus agravantes que surgiram devido a pandemia do coronavírus.

Assim, o terceiro e último capítulo desse estudo visa trazer soluções e recomendações para as situações previamente levantadas, a fim de alinhar o ambiente empresarial e prover melhorias para ambos os lados dessa história, empregados e empregadores.

A conclusão ressalta os pontos levantados, os resultados obtidos e as sugestões para o futuro próximo.

## **1. SEGURANÇA DA INFORMAÇÃO**

A segurança da informação é uma área da informática que envolve a análise e proteção de informações e dados que circulam em determinada rede. Seu principal foco é o gerenciamento de riscos e ameaças, podendo envolver outros conceitos menores como a cibersegurança, objeto que pode ser mais relacionado a esse estudo.

### **1.1. Cibersegurança**

A cibersegurança é um segmento mais restrito da área de segurança da informação, a qual trata especificamente das ferramentas e comportamentos que são utilizados a favor da proteção de dados nos ambientes virtuais. Ela serve para analisar e tratar ameaças que possam atingir dados e informações, que transitam e são armazenadas em sistemas digitais interligados.

Portanto, podemos associar a cibersegurança a segurança da infraestrutura da empresa, cuidando assim para que softwares, hardwares e redes não sofram ataques cibernéticos, protegendo a informação digital presente nesse ambiente.

### **1.2. Valor empresarial**

A ideia básica de segurança é evitar problemas, amenizar ameaças e diminuir riscos, não apenas virtualmente. Tratando de segurança da informação, principalmente no âmbito empresarial, estamos falando de níveis ainda mais rigorosos, sempre que possível levando essas ocorrências o mais próximos possível da inexistência. Isso se deve ao fato que os dados e informações são considerados os bens mais preciosos para uma empresa.

Com isso, podemos ter uma visão mais clara sobre a importância que as organizações devem colocar em cima dos investimentos da área de segurança da informação, visando a proteção de dados sensíveis que, caso indevidamente acessados, possam comprometer não apenas a segurança, mas todos os setores da empresa.

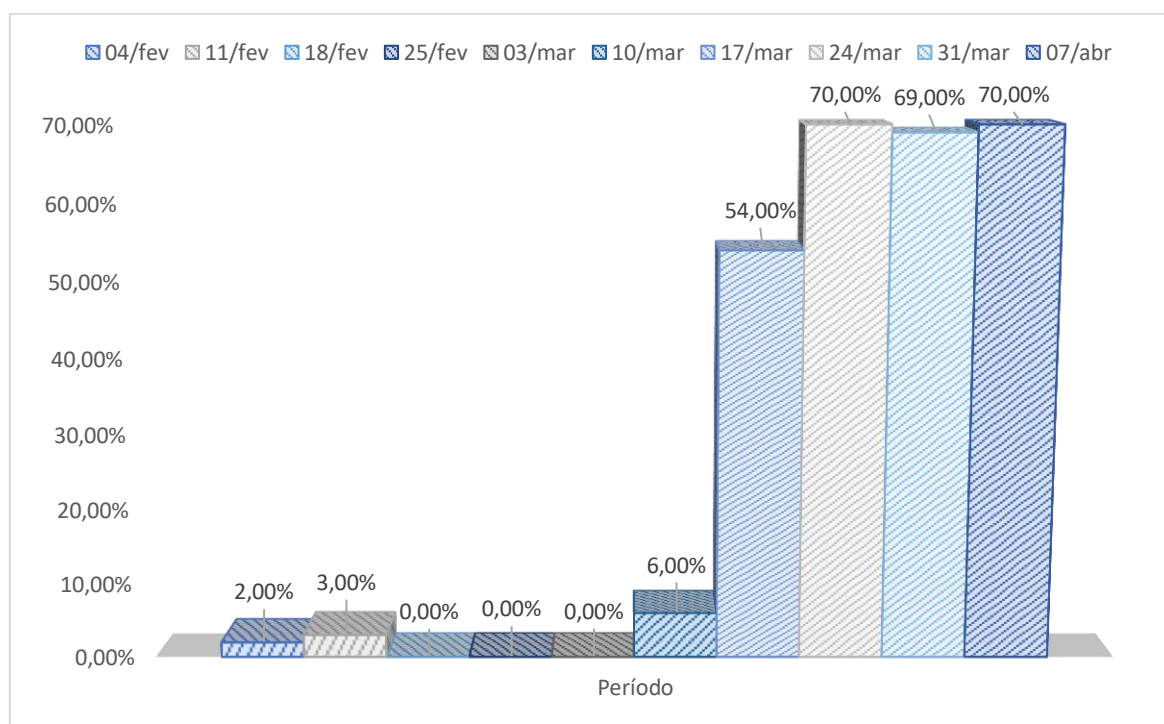
## 2. TRABALHO REMOTO

O teletrabalho ou trabalho a distância, como também é conhecido, é uma modalidade de trabalho onde o funcionário realiza suas atividades profissionais a distância, seja de um ambiente *coworking*, um restaurante, um shopping, ou até mesmo da própria casa, essa última opção, nesse caso se mostra como um escritório domiciliar, mais conhecido pelo termo em inglês, *home office*, o qual será diretamente relacionado ao presente projeto.

### 2.1. Home office

O escritório domiciliar é a variante do trabalho remoto onde o funcionário exerce suas funções de dentro da própria residência. Essa modalidade de prestação de serviços é comum há muito tempo, mas se tornou ainda mais presente no período de pandemia, conforme visto no gráfico abaixo, a fim de evitar que as pessoas saiam de suas casas, ao menos que fosse inevitável, visando assim reforçar o isolamento social que é proposto pelas autoridades de saúde mundiais contra a disseminação do vírus e a proliferação da doença por ele causada.

GRÁFICO 1 – Aumento de trabalhadores remotos com o início da pandemia



Fonte: Adaptado de VMware Carbon Black, 2020.

Enquanto o trabalho remoto se refere as atividades do trabalhador que podem ser realizadas a distância, durante uma viagem por exemplo, entre outras diversas possibilidades, onde poderia trabalhar de qualquer lugar do mundo, o termo home office está restrito a jornada de trabalho realizada necessariamente na própria casa, de forma esporádica ou permanentemente.

## **2.2. Principais benefícios**

A possibilidade de trabalhar de casa tende a trazer diversas vantagens, tanto para as empresas quanto para os funcionários, e isso vem mostrando resultados na prática durante o último ano e meio.

Para empresas, podemos destacar a redução de custos, devido à falta de um escritório alocado em um espaço físico para se manter, a empresa pode vir a economizar em suas principais despesas como aluguel, energia elétrica e água. Apesar de surgirem outros custos como o fornecimento de computadores e internet para que o funcionário possa seguir realizando suas funções em casa, essa troca tende a ser mais favorável a empresa.

Enquanto para os funcionários, muitos já consideram o fato de poder trabalhar da própria casa um benefício, isso devido à melhora na qualidade de vida por poder evitar os problemas presentes na rotina da grande maioria dos trabalhadores como o tempo perdido e o estresse causado pelo trânsito ou pelo transporte público.

## **2.3. Principais dificuldades**

Apesar de demandar menos investimento, o home office traz consigo alguns problemas que devem ser enfrentados por seus adeptos. Empresas e funcionários devem andar juntos para garantir a continuidade dos negócios. Os aspectos que demandam mais atenção são a comunicação, a rotina e o compromisso.

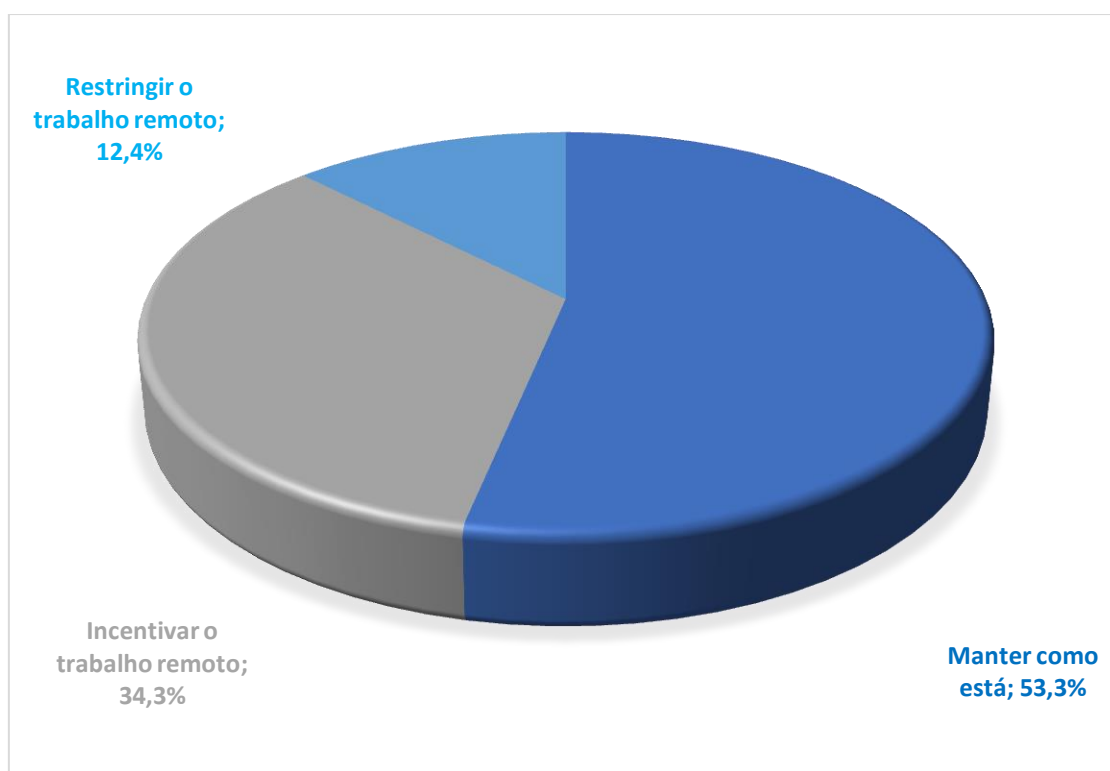
As pessoas devem estar familiarizadas com as ferramentas de comunicação utilizadas nesse modelo de negócio para garantir o fluxo do trabalho. Reuniões podem ou não ser mantidas, mas é sempre importante manter o acompanhamento de atividades e o feedback para os superiores.

Além disso, muitos tem a visão deturbada do home office onde o funcionário fica completamente à vontade para trabalhar a hora que quiser e da maneira que quiser. Apesar da flexibilidade inclusa nesse regime de trabalho, é importante manter as rotinas, como o respeito aos horários, trajar-se adequadamente de acordo com suas atividades, e se possível, buscar separar ao máximo o ambiente do resto da casa, evitando assim distrações que possam atrapalhar o desempenho e contribuir para a desorganização.

## 2.4. Expectativas para o futuro

Durante a pandemia, muitas empresas descobriram que o home office é muito interessante e passaram a adotar a ideia de manter o trabalho a distância, mesmo ao fim desse período em que vivemos. Aliás, isso já era uma tendência esperada muito antes do coronavírus surgir. Em 2017, uma pesquisa chamada “O Futuro do Trabalho” foi divulgada pelo site Transformação Digital e apresentou a intenção dos empregadores em promover a cultura do trabalho remoto, conforme o gráfico de dados mostrado abaixo:

GRÁFICO 2 – Nos próximos 12 meses, as empresas pretendem:



Fonte: Adaptado de “O Futuro do Trabalho” por Transformação Digital, 2017.

A pandemia, nesse contexto, apareceu somente para acelerar esse processo de mudança, e a tendência a partir de agora é que cada vez mais as pessoas tenham essa liberdade para trabalharem de onde for mais conveniente e produtivo, alinhando seus interesses aos da organização, visando assim a continuidade dos negócios e o crescimento profissional e empresarial.

Essa liberdade nos leva a acreditar que o futuro dos negócios tende a ser híbrido, onde empresas e pessoas terão mais opções de escolha, e poderão optar por ambientes físicos alinhados simultaneamente aos ambientes virtuais, ou estritamente o que lhes for mais oportuno.

### **3. SOLUÇÕES**

Com toda essa situação atual, boa parcela das empresas já está atuando, parcialmente ou integralmente, em regime home office, e por isso devem buscar entender e assim, se prepararem para os perigos embutidos nos ambientes virtuais. Para isso, algumas medidas devem ser tomadas e comportamentos devem ser levados em consideração, a fim de aumentar os níveis de cibersegurança e reduzir os riscos digitais, os quais só aumentam quando o local de trabalho se expande para fora do escritório.

#### **3.1. Principais ameaças**

Os perigos virtuais então presentes na internet durante anos, não é novidade para ninguém, e muito menos para as empresas. Por tratar de dados e informações de maior confiabilidade, os riscos e ameaças aumentam na mesma proporção que o nível de sigilo desejado.

Agora tratando da mudança para home office na pandemia, a situação fica ainda mais assustadora, pois muitas empresas não estavam completamente preparadas para lidar com essas ameaças e tiveram de se adaptar às pressas.

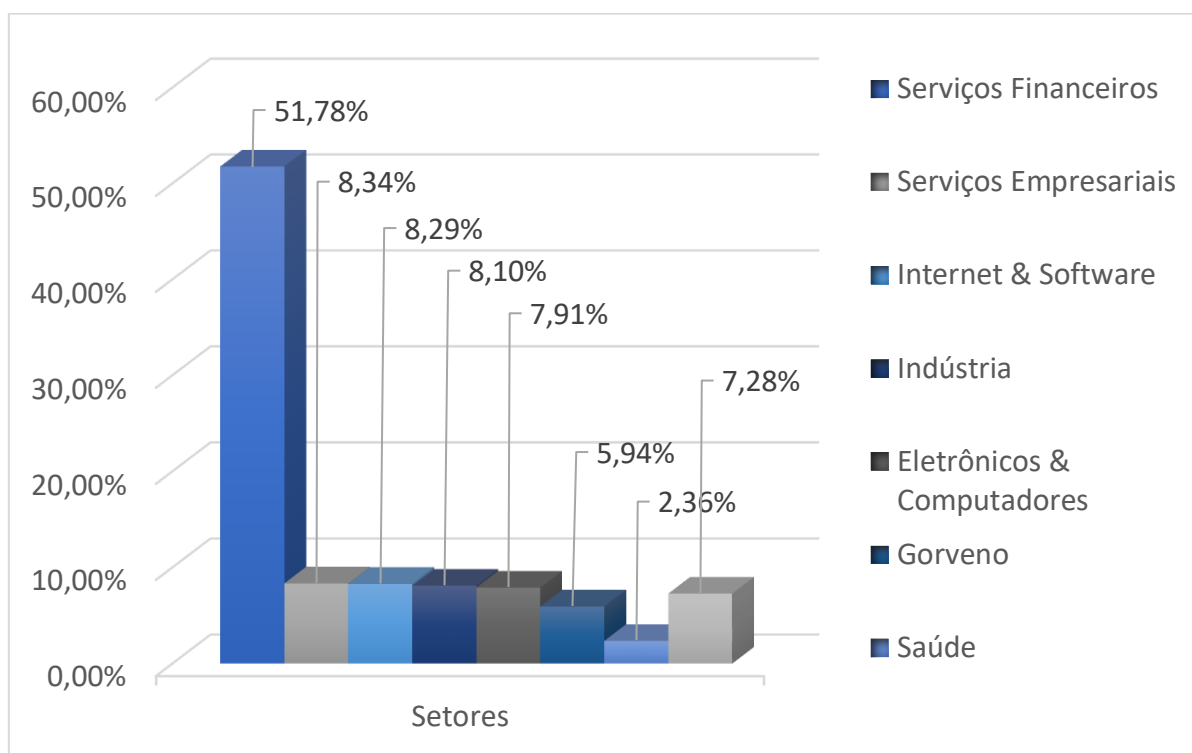
Para isso, algumas dessas medidas tomadas são aplicar antivírus nas máquinas, ter cópias de segurança do que está nos servidores, criptografar dados e oferecer uma tecnologia de assinatura digital. Essas não parecem soluções tão complexas para uma empresa comum, porém imagine esse cenário aplicado a rede doméstica de cada funcionário da empresa...

#### **3.2. Principais alvos**

O setor financeiro tem sido cada vez mais visado durante o alastramento da COVID-19. Somente entre fevereiro e março de 2020, observamos um aumento de 38% nos ataques cibernéticos contra instituições financeiras, de acordo com os dados da VMware Carbon Black.

Nesse mesmo período, os ataques relacionados à empresas do setor de serviços financeiros foram responsáveis por 52% de todos os ataques virtuais vistos no conjunto de dados VMware Carbon Black, uma anomalia sem precedentes em seus registros de rastreamento de dados, o que nos mostra uma diferença gritante para as demais áreas, conforme podemos conferir no gráfico abaixo:

GRÁFICO 3 - Distribuição de ataques empresariais



Fonte: Adaptado de VMware Carbon Black, 2020.

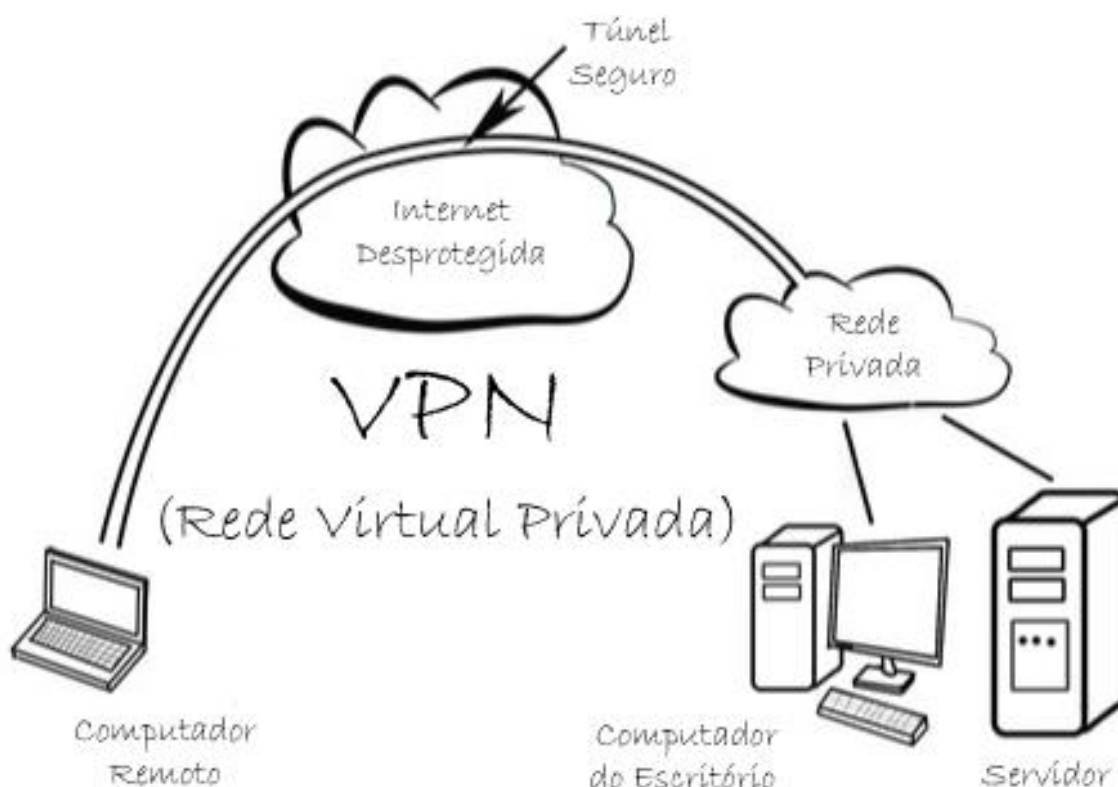
As equipes de segurança devem ser capazes de prever e prevenir não apenas ataques conhecidos, mas também ataques futuros. Processos inovadores aproveitam todos os dados disponíveis para fornecer a proteção mais abrangente possível. Com o poder da análise de dados, as equipes de segurança podem descobrir as táticas ocultas mais perturbadoras e prejudiciais, identificar as causas básicas e impedir as ameaças mal-intencionadas antes que sejam totalmente desenvolvidas, protegendo assim as informações sigilosas.



### 3.3. Rede Privada Virtual

*Virtual Private Network* ou simplesmente VPN, como conhecemos, protege os dados e informações por meio de criptografia e estabelece uma conexão segura através da internet, essa tecnologia cria uma espécie de túnel entre seu computador e o escritório da empresa, impedindo que eventuais invasores tenham acesso às informações trafegadas, conforme ilustrado abaixo:

FIGURA 1 – VPN Tunnel



Fonte: Adaptado de Adobe Stock, 2021.

A VPN serve para garantir uma conectividade confiável, permitindo a conexão segura de todos os dispositivos, mesmo quando acessados a partir de pontos públicos de acesso *Wi-Fi*, um recurso desejável para os empregadores que praticam o trabalho remoto e nem sempre sabem de onde seus colaboradores se conectam.

Mesmo aprimorando a segurança da rede doméstica, o uso de VPN ainda é a melhor forma de proteger dados da empresa ao trabalhar em casa. A solução é uma das mais indicadas para quem faz home office e precisa ter acesso a documentos que ficarão nos computadores e servidores da organização.

### 3.4. Criptografia

A criptografia é uma prática de cibersegurança onde os dados e informações são codificadas, de forma que somente um usuário com a chave correta poderá realizar o acesso ou remover a criptografia. Assim, o conteúdo criptografado aparecerá de maneira confusa, misturadamente disposto ou ilegível para quem estiver tentando acessá-lo sem que as devidas permissões sejam concedidas.

Usamos esse tipo de feramente na segurança da informação para tentar impedir que pessoas ou organizações mal-intencionadas consigam acesso a dados sigilosos da companhia. Trata-se de uma das mais importantes ferramentas nesse contexto pois dificulta muito o trabalho dos invasores.

### 3.5. Autenticação

Senhas são as chaves de acesso mais comuns para acesso a informações, por isso a importância de utilizar senhas fortes e não utilizar a mesma senha para mais de um acesso, assim diminuindo os riscos. Senhas fracas são uma das maiores brechas de cibersegurança que levam ao roubo de dados e informações sigilosas.

Porém, quando tratamos de informações sigilosas, é importante garantir outros métodos de autenticação. É o que chamamos MFA ou autenticação multifator, onde além da senha, o usuário terá que comprovar sua identidade através de um método extra de verificação. Quanto mais fatores de autenticação, mais proteção agregada.

### 3.6. Antivírus

O responsável por cuidar de um dos problemas mais comuns no ambiente virtual, os *malwares*. Esses incluem vírus, *spyware*, *ransomware*, *adware*, entre outras ameaças, onde todas tem como objetivo infectar um computador ou rede e causar algum mal.

Por ser facilmente disseminado através de e-mails e downloads, é importante manter seu antivírus atualizado para obter o melhor nível de proteção, detectando e removendo ameaças.

### 3.7. Conscientização

A preocupação com cibersegurança não envolve apenas ferramentas, mas também ações e medidas visando agregar a cultura de proteção de dados e conectar as pessoas aos objetivos da organização. Os dados a seguir apresentados, mostram que a falta de treinamento de cibersegurança aos colaboradores, têm levado as organizações a resultados muito negativos.

Segundo o relatório “The Rise Of The Business-Aligned Security Executive” desenvolvido pela Forrester e encomendado pela Tenable, realizado com 416 profissionais de segurança da informação e 425 líderes de negócios de diversos países, incluindo o Brasil, muitas empresas não estavam devidamente preparadas para o aumento de ataques cibernéticos. Aproximadamente 96% das organizações brasileiras, por exemplo, sofreram com algum tipo de ataque dessa natureza que tenha afetado o andamento de seus negócios, entre 2019 e 2020, conforme podemos conferir na tabela abaixo, onde os participantes da pesquisa responderam a seguinte pergunta: “Quantas vezes sua organização passou por um ataque cibernético ou comprometimento com impacto nos negócios nos últimos 12 meses?”

TABELA 1 – Additional data

	ALEMANHA (N = 103)	ARÁBIA SAUDITA (N = 52)	AUSTRÁLIA (N = 105)	BRASIL (N = 59)	ESTADOS UNIDOS (N = 106)	FRANÇA (N = 104)	ÍNDIA (N = 54)	JAPÃO (N = 51)	MÉXICO (N = 104)	REINO UNIDO (N = 103)
<b>NENHUM</b>	1%	4%	5%	2%	1%	5%	2%	0%	2%	3%
<b>1</b>	3%	0%	3%	5%	2%	1%	6%	2%	1%	3%
<b>2</b>	2%	8%	6%	3%	4%	5%	6%	6%	4%	8%
<b>3</b>	11%	10%	10%	10%	212%	17%	24%	18%	15%	16%
<b>4</b>	33%	33%	18%	39%	25%	27%	24%	18%	28%	22%
<b>5 OU MAIS</b>	47%	44%	55%	39%	44%	40%	37%	55%	47%	47%
<b>NÃO SOUBE RESPONDER</b>	4%	2%	4%	2%	3%	5%	2%	2%	3%	2%

Fonte: Adaptado de “The Rise Of The Business-Aligned Security Executive” por Forrester, 2020.

Através dos dados apresentados, podemos notar a necessidade do investimento das organizações em treinamentos e iniciativas que promovam a cultura de cibersegurança empresarial, alinhando assim as ferramentas e tecnologias disponíveis no mercado, ações realizadas na prática durante a rotina do dia a dia e pessoas conscientes, a fim de prospectar ambientes de trabalho mais seguros.

## CONCLUSÃO

O ano de 2020 apresentou diversos desafios para o cenário empresarial. Um deles é a dificuldade relacionada a proteção de dados sigilosos, e com isso, conseqüentemente veio à tona a importância da cibersegurança para a continuidade dos negócios.

Trabalhar em casa (ou levar seu escritório para casa) é a nossa realidade agora. Para muitas empresas, essa mudança para o trabalho remoto interrompeu os negócios. Outros estão adaptando e reavaliando sua estratégia de TI agora que veem o trabalho remoto como uma abordagem plausível que permite que os funcionários permaneçam produtivos.

Sim, o trabalho remoto apresenta novos desafios de segurança, mas a escolha da tecnologia certa pode manter seus dados protegidos e garantir um local seguro onde os funcionários possam continuar a ser produtivos.

Mantenha-se saudável, mantenha-se seguro.

## REFERÊNCIAS BIBLIOGRÁFICAS

ADOBE STOCK. VPN tunnel. Disponível em: <https://adobe.ly/2UgTpqP>. Acesso em 13 jun. 2021.

AGÊNCIA BRASIL. Em maio, 13,3% das pessoas ocupadas exerceram teletrabalho. Disponível em: <https://bit.ly/2RlrSDp>. Acesso em 27 maio 2021.

AGÊNCIA BRASIL. Home office foi adotado por 46% das empresas durante a pandemia. Disponível em: <https://bit.ly/3x2zyKd>. Acesso em 27 maio 2021.

AGÊNCIA BRASIL. Número de empresas com home office deve crescer 30% após pandemia. Disponível em: <https://bit.ly/34NIJmQ>. Acesso em 27 maio 2021.

AGÊNCIA BRASIL. Pesquisa mostra potencial para a expansão do home office. Disponível em: <https://bit.ly/3cgK4pd>. Acesso em 27 maio 2021.

AGÊNCIA BRASIL. Trabalho em home office tende a continuar após fim da pandemia. Disponível em: <https://bit.ly/2TH40Lr>. Acesso em 27 maio 2021.

BACKUP GARANTIDO. Autenticação Multifator (MFA): entenda o recurso de cibersegurança. Disponível em: <https://bit.ly/3iQeLFy>. Acesso em 13 jun. 2021.

BEER OR COFEE. Tudo sobre as diferenças entre Home Office e Trabalho Remoto. Disponível em: <https://bit.ly/3vcYJZ5>. Acesso em 10 jun. 2021.

BIOLOGIA NET. Doenças. Pandemia. O que é pandemia? Um breve histórico sobre pandemias. Disponível em: <https://bit.ly/2TqPA1K>. Acesso em 19 maio 2021.

CANALTECH. Ciberataques crescem 50% durante a migração para home office na pandemia. Disponível em: <https://bit.ly/2TwmMVv>. Acesso em 13 jun. 2021.

CANALTECH. Isolamento e home office levaram a aumento em ataques de ransomware no Brasil. Disponível em: <https://bit.ly/3zwDYuK>. Acesso em 13 jun. 2021.

CCM TECNOLOGIA. Saiba como funciona a criptografia na segurança de dados. Disponível em: <https://bit.ly/3zA4aVm>. Acesso em 13 jun. 2021.

CITRIX. Security challenges in the time of quarantine. Disponível em: <https://bit.ly/3zzCJLI>. Acesso em 13 jun. 2021.

COMPUGRAF. Campanhas de Conscientização: Por que são tão importantes em Cibersegurança. Disponível em: <https://bit.ly/3gCivsl>. Acesso em 13 jun. 2021.

CRYPTO ID. Autenticação de dois fatores está entre as medidas de cibersegurança que você deve aplicar em 2020. Disponível em: <https://bit.ly/2SHawSe>. Acesso em 13 jun. 2021.

CRYPTO ID. Tempest apresenta primeiro estudo do mercado brasileiro de cibersegurança. Disponível em: <https://bit.ly/3vjMGcE>. Acesso em 10 jun. 2021.

DNK. Cibersegurança é tendência em mundo pós-pandemia. Disponível em: <https://bit.ly/3xk9JFI>. Acesso em 13 jun. 2021.

ECONOMIA – UOL. Bancando o home office. Disponível em: <https://bit.ly/3wAG62w>. Acesso em 13 jun. 2021.

EDITORA JC. Home office e Segurança da Informação – Tendência e desafios. Disponível em: <https://bit.ly/3wtjjWw>. Acesso em 13 jun. 2021.

ENCONTRE UM NERD. Saiba o que é trabalho remoto e conheça 4 vantagens. Disponível em: <https://bit.ly/2TiwrPJ>. Acesso em 10 jun. 2021.

EVEO. Confira agora o guia para aumentar a segurança no home office. Disponível em: <https://bit.ly/3iKco7h>. Acesso em 13 jun. 2021.

FATEL. Trabalho remoto: Segurança da Informação ainda é um dos grandes desafios do home office. Disponível em: <https://bit.ly/35i3R3o>. Acesso em 13 jun. 2021.

FIA – FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO. Entenda mais sobre cibersegurança, seu potencial e oportunidades de carreira. Disponível em: <https://bit.ly/3cyN2oV>. Acesso em 03 jun. 2021.

FIRST TECH. Como evitar infrações à LGPD no home office. Disponível em: <https://bit.ly/3xlkirP>. Acesso em 13 jun. 2021.

FLOW TI. Segurança da informação ou Cibersegurança: o que é e qual é a sua importância? Disponível em: <https://bit.ly/3vRskbL>. Acesso em 03 jun. 2021.

FORRESTER. The Rise Of The Business-Aligned Security Executive. Disponível em: <https://bit.ly/35wlefX>. Acesso em 13 jun. 2021.

G1 – GLOBO. Home Office na pandemia. Disponível em: <https://glo.bo/3fRJVLla>. Acesso em 19 maio 2021.

G1 – GLOBO. Produtividade, conexão, flexibilidade: pesquisa aponta os principais desafios do home office após um ano de pandemia. Disponível em: <https://glo.bo/350PAs5>. Acesso em 19 maio 2021.

GRUPO RISOTOLÂNDIA. Entenda a diferença entre trabalho remoto e home office. Disponível em: <https://bit.ly/3xaZqU8>. Acesso em 10 jun. 2021.

JORNAL CONTÁBIL – R7. Home office: Confira dicas de segurança para o trabalho remoto. Disponível em: <https://bit.ly/3cG9VXJ>. Acesso em 13 jun. 2021.

KASPERSKY. Como desenvolver uma cultura de consciência cibernética no trabalho. Disponível em: <https://bit.ly/3gAAxvD>. Acesso em 13 jun. 2021.

KASPERSKY. O que é cibersegurança? Disponível em: <https://bit.ly/3vz3Jaz>. Acesso em 13 jun. 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de Metodologia Científica. 5ª edição. São Paulo: Atlas, 2003.

LUMIUN. 4 dicas de segurança na era do trabalho Home Office. Disponível em: <https://bit.ly/35mx2T0>. Acesso em 13 jun. 2021.

NA PRÁTICA. Qual a diferença entre trabalho remoto e home office? Disponível em: <https://bit.ly/3cyKOWV>. Acesso em 10 jun. 2021.

OI SOLUÇÕES. Segurança em tempos de pandemia. Disponível em: <https://bit.ly/3cC62mA>. Acesso em 13 jun. 2021.

REUTERS. CORRECTED-Hacking against corporations surges as workers take computers home. Disponível em: <https://reut.rs/2TFpfxg>. Acesso em 13 jun. 2021.

REVISTA SEGURANÇA ELETRÔNICA. Cinco dicas de cibersegurança para empresas com home office. Disponível em: <https://bit.ly/2UgvlEw>. Acesso em 13 jun. 2021.

SECURITY REPORT. Apenas 40% das empresas vítimas de ataques reforçam regras de cibersegurança. Disponível em: <https://bit.ly/3zvf1A1>. Acesso em 13 jun. 2021.

SEGINFO. Ataques contra empresas disparam com funcionários em home-office. Disponível em: <https://bit.ly/2SagHhs>. Acesso em 13 jun. 2021.

START TI. Cultura de Cibersegurança para empresas: entenda porque é importante! Disponível em: <https://bit.ly/3q5motl>. Acesso em 13 jun. 2021.

SYNNEX COMSTOR. O que é cultura de cibersegurança e como desenvolvê-la? Disponível em: <https://bit.ly/3gCiapW>. Acesso em 13 jun. 2021.

TECH TUDO. Dicas para trabalhar em home office: saiba proteger informações importantes. Disponível em: <https://glo.bo/3cPOqDL>. Acesso em 13 jun. 2021.

VMWARE. Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted. Disponível em: <https://bit.ly/3xt9E2j>. Acesso em 13 jun. 2021.

VMWARE. Technical Analysis: Hackers Leveraging COVID-19 Pandemic to Launch Phishing Attacks, Fake Apps/Maps, Trojans, Backdoors, Cryptominers, Botnets & Ransomware. Disponível em: <https://bit.ly/3q4G2FW>. Acesso em 13 jun. 2021.

WE LIVE SECURITY. Cibersegurança ou segurança da informação? Explicando a diferença. Disponível em: <https://bit.ly/3g9R4FI>. Acesso em 03 jun. 2021.

WE LIVE SECURITY. Como tornar o seu home office mais seguro em tempo de coronavírus (Covid-19). Disponível em: <https://bit.ly/3cDVoM0>. Acesso em 13 jun. 2021.