UNIVERSIDADE EVANGÉLICA DE GOIÁS - UNIEVANGÉLICA
ENGENHARIA DE COMPUTAÇÃO/ENGENHARIA DE SOFTWARE

ANDRÉ LUIS DA SILVA
JOÃO VICTOR DA SILVA

Ambientes Seguros para Trabalho Remoto

Anápolis – GO
Dezembro, 2021

UNIVERSIDADE EVANGÉLICA DE GOIÁS - UNIEVANGÉLICA
ENGENHARIA DE COMPUTAÇÃO/ENGENHARIA DE SOFTWARE

ANDRÉ LUIS DA SILVA
JOÃO VICTOR DA SILVA

Ambientes Seguro para Trabalho Remoto

Trabalho apresentado ao Curso de Engenharia de Software da Universidade Evangélica de Goiás – UniEVANGÉLICA, da cidade de Anápolis-GO como requisito parcial para obtenção do Grau de Bacharel em Engenharia de Software.

Orientador (a): Prof. Millys Fabrielle Araujo Cavalhaes

Anápolis - Go
Dezembro, 2021

RESUMO

O trabalho remoto, também chamado de *Home Office* ou teletrabalho tem ganhado cada vez mais adeptos ao longo dos últimos anos. A chegada da pandemia da COVID19 obrigou empresas e funcionários a repensarem os modos tradicionais de trabalho. O resultado foi um grande número de funcionários, movidos para ambientes remotos. O objetivo deste trabalho é criar um guia de boas práticas mostrando quais configurações são adequadas para reforçar a segurança da informação em home office.

Palavras-chave: Trabalho Remoto; Segurança da Informação; Hacker.

ABSTRACT

Remote work, also called Home Office or Telecommuting, has gained more and more followers over the past few years. The arrival of the COVID19 pandemic forced companies and employees to rethink their traditional ways of working. The result was a large number of employees, moved to remote environments. The objective of this work is to create a best practices guide showing which settings are suitable to reinforce information security in the home office.

Keywords: Remote Work; Information Security; Hacker.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

Siglas	Descrição
AES	Advanced Encryption Standard
Covid19	Corona Virus Disease 2019
EXE	Executable
FTP	File Transfer Protocol
HD	Hard Disk
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LTS	Long-term support
MSI	Microsoft Installer
OWASP	Open Web Application Security Project
RDP	Remote Desktop Protocol
SSD	Solid State Drive
TXT	Text
VPN	Virtual Private Network
RAT	Remote Access Trojan

SUMÁRIO

1. INTRODUÇÃO

Uma estatística feita pela Buffer (2020), aponta que grande parte dos trabalhadores gostariam de continuar executando o trabalho de forma remota. Além disso, 97% dos entrevistados disseram que recomendariam o trabalho remoto para outras pessoas.

Neste sentido, em meios aos problemas causados pelo momento pandêmico, no Brasil as empresas e trabalhadores foram forçados a utilizarem a internet e o Trabalho Remoto para exercerem seus trabalhos e não pararem a produção, sendo assim, aquelas empresas que não funcionavam neste regime, tiveram que se adaptar rapidamente. (ALVES e REZENDE, [2021]).

Ao mesmo tempo, com o aumento da demanda pelo trabalho remoto, também aumentou a necessidade de implementação de segurança da informação por parte da empresa e dos funcionários. Com o aumento do trabalho remoto, houve um aumento de 704% nos ataques aos chamados servidores RDP e esse tipo de ataque soma 29 bilhões de incidentes na américa latina. No geral, as empresas mais afetadas por *malwares* foram as brasileiras (19%), seguidas pelas empresas mexicanas (17,5%) e pelas argentinas (13,3%). O *phishing* também afetou o Brasil, com (24,6%) de incidentes. (Extra, 2021).

Nesse contexto, como as tecnologias atuais podem ser empregadas no trabalho remoto a fim de melhorar a segurança da informação?

Como objetivo geral, este trabalho propõe a elaboração de um guia de boas práticas para configuração adequada da segurança da informação em um ambiente para trabalho remoto. Para alcançar o objetivo proposto este trabalho possui os seguintes objetivos específicos: (a) identificar normas de segurança relacionadas ao trabalho remoto, (b) pesquisar as principais tecnologias de segurança e comunicação, (c) criar guia de boas práticas, (d) configurar um ambiente home office.

O site Indeed, mostra um crescimento de 215% na procura do trabalho remoto entre março e novembro. (G1, 2020). Porém, com este aumento houve uma alta também no índice de ciberataques.

Corroborando a necessidade de investimento em segurança da informação, dados do jornal Hoje em Dia mostram que os prejuízos com ciberataques podem chegar a 6 trilhões de dólares em 2021 (ÁVILA, 2021).

Como justificativa deste trabalho, quaisquer investimentos em melhores práticas para tornar o ambiente de trabalho remoto mais seguro, trarão benefícios às empresas que optarem por este tipo de trabalho e aos seus funcionários, ou seja para uma empresa ou pessoa que deseja desempenhar trabalhos de forma remota, o qual não tenha nenhum investimento ou nenhum conhecimento sobre segurança da informação, o trabalho visa proporcionar uma base simples pela qual os investimentos em segurança poderão se iniciar.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Trabalho Remoto

O Trabalho Remoto, é um meio de um profissional exercer o seu trabalho à distância através da internet dispensando a necessidade de presença física. A SOBRATT - Sociedade Brasileira de Teletrabalho e Teleatividades define teletrabalho como:

> O teletrabalho é a modalidade de trabalho, que utilizando as tecnologias da informação e das comunicações (TIC), pode ser realizada à distância, fora do âmbito onde se encontra o contratante, de maneira total ou parcial, podendo realizar-se em relação de dependência (empregado) ou de maneira autônoma (freelance), executando atividades que podem ser desenvolvidas pelos equipamentos móveis, tais como computadores, smartphones, tablets etc. (SOBRATT, [s.d.]).

No Brasil, a modalidade do trabalho remoto é relativamente recente e foi reconhecido por Lei em 2011, lei 12.551 de 15 de dezembro de 2011 (Brasil, 2011). Com a chegada da pandemia do Covid19, muitas empresas tiveram que adaptar o seu modo de trabalho utilizando o trabalho remoto. Devido ao aumento do trabalho remoto, houve também o aumento da necessidade da segurança da informação, problemas causados por hackers e pessoas mal intencionadas. (BAPTISTA JUNIOR e DIAN, 2021).

2.2. Hacker

Hacker é o profissional que utilizar os seus conhecimentos para proteger a si mesmo ou a terceiros. “Para os fãs de Guerra nas Estrelas, pensem no *hacker* como o cavaleiro *jedi* bonzinho. Ele possui os mesmos poderes que o *jedi* do lado negro da força (*cracker*) mas os utiliza para proteção” (ASSUNÇÃO, 2020).

Belcic (2020) também afirma que existe diferentes tipos de *hacker* “*Hacker* é alguém que aplica habilidades de computação para resolver um problema”. Muitos quando ouvem a palavra *hacker* já associam, por engano, às pessoas que utilizam do conhecimento de computação para cometer um crime. Todavia, desmentindo o senso comum, existem 3 tipos de *hackers*: o chapéu preto (B*lack Hat*), o chapéu branco (*White Hat*) e o chapéu cinza (*Gray hat*) (BELCIC, 2020).

2.2.1. Chapéu Preto

Um hacker chapéu preto é um cibercriminoso que procura falhas em sistemas e aproveita essas vulnerabilidades para invadir e/ou roubar informações de pessoas e empresas.

> Um chapéu preto é quem viola os sistemas de segurança cibernética para obter acesso ilícito a um computador ou uma rede. Se um *hacker* chapéu preto descobre uma vulnerabilidade de segurança, ele fará a exploração sozinho ou alertará outros *hackers* sobre a oportunidade, normalmente em troca de dinheiro (BELCIC, 2020).

Segundo Ivan (2020) "Os *hackers black hat* podem ser tanto amadores iniciantes na disseminação de *malware*, quanto hackers muito mais habilidosos e experientes que visam roubar informações pessoais, credenciais de login, ou dados bancários".

Segundo Silva (2013) "*crackers* possuem o pseudônimo de *Black hat*, também podendo ser chamados de — *hackers* do mau ou — *hacker* chapéu negro".

2.2.2. Chapéu Branco

Um *hacker* chapéu branco é uma pessoa que utiliza de seu conhecimento para tentar invadir um sistema e reportar falhas de segurança à empresa ou pessoa. Muitos desses *hackers* são contratados por empresas para manter os seus sistemas ou redes seguras.

> *Hackers* chapéu branco são o oposto dos *hackers* de chapéu preto. Eles têm os mesmos talentos, mas em vez de usá-los para fins criminosos, eles aplicam esses talentos para ajudar as empresas a fortalecer suas defesas digitais. Um *hacker* chapéu branco tentará intencionalmente violar um sistema, com permissão do proprietário, para identificar pontos fracos a serem corrigidos. Esse tipo de trabalho também é conhecido como "*hacking* ético" (BELCIC, 2020).

O termo *White Hat* é intitulado á aqueles que possuem conhecimento sobre vulnerabilidades e falhas de segurança de um sistema e mesmo assim não cometem crime aproveitando destes problemas de segurança (SILVA, 2013).

2.2.3. Chapéu Cinza

Um hacker chapéu cinza é um *hacker* que fica "em cima do muro", ele atua *como White hat* porém em alguns momentos atua como *Black hat*, mas sem causar danos muito sérios à empresas ou pessoas.

> [...]Eles não são exatamente o modelo de altruísmo, como os *hackers* chapéu branco, nem se dedicam a atos criminosos. Enquanto os *hackers* chapéus branco obtêm permissão antes de sondar as vulnerabilidades de um sistema, os chapéus cinzas pulam essa parte e vão direto ao *hacking* (BELCIC, 2020).

Aqueles profissionais que se dizem *White Hat*, porém tem suas ações reconhecidas como as de *Black Hat*, são intitulados de *Gray Hat* (ALENCAR; QUEIROZ; DE QUEIROZ 2013).

Para que um hacker consiga realizar um ataque, seja tanto profissional como criminoso, ele busca vulnerabilidades que estão presentes em sistemas ou redes e aplicam técnicas de invasão.

2.3. Vulnerabilidades

Quando um *hacker* encontra uma vulnerabilidade, ele estuda como utilizá-la para invadir este ambiente. “Uma vulnerabilidade de segurança pode ser vista como qualquer fator que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a recursos” (IT.EAM, 2020).

Para Fernandes (2013):

> Podemos entender por vulnerabilidades as falhas que um sistema possui, podendo provocar a indisponibilidade das informações, ou até mesmo a quebra do sigilo e alteração sem autorização, podendo ser decorrente de uma série de fatores, como falta de treinamento, falta de manutenção, falha nos controles de acesso, ausência de proteção de uma determinada área ameaçada.

Estando dentro de um sistema já invadido, os *hackers* estão atentos a buscar novas vulnerabilidades para deixarem uma nova “porta de entrada” facilitada para invasões futuras.

Entretanto, a segurança da informação está aí para evitar esses tipos de cenários com suas propriedades de segurança.

2.4. Segurança da Informação

Segurança da informação ou cibersegurança é a área computacional que foca em guardar e manter os dados de empresas e pessoas seguros sem que terceiros tenham acessos a eles.

Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas.[...] (KASPERSKY, [s.d.]).

Segundo autores como Mello ([s.d.]) e Fernandes (2013), a segurança da informação é composta pelos pilares da trilogia CID: Confidencialidade, Integridade, Disponibilidade.

2.4.1. Confidencialidade

A confidencialidade está relacionada à privacidade dos dados, de maneira que ações maliciosas como ataques *hackers* não liberam informações confidenciais. Uma maneira de reforçá-la é colocando medidas de prevenção, de modo que o acesso só é permitido por pessoas autorizadas (MELLO, [s.d.]).

Fernandes (2013) descreve confidencialidade como: “Garante que somente pessoas autorizadas poderão acessar as informações. Trata-se da não permissão da divulgação de uma informação sem prévia autorização.”

2.4.2. Integridade

A integridade está associada a confiabilidade dos dados, onde o objetivo é manter os dados da maneira que foram criados (MELLO, [s.d.]).

Fernandes (2013) descreve integridade como garantia de que as informações não serão alteradas ou violadas.

2.4.3. Disponibilidade

A disponibilidade tem o objetivo de manter os dados sempre acessíveis (MELLO, [s.d.]).

Fernandes (2013) descreve a disponibilidade como: “Garante acesso a uma informação no momento desejado. Isso implica no perfeito funcionamento da rede e do sistema. Imagine você necessitando de umas informações para concluir um relatório e o sistema não está funcionando!”.

A segurança da informação utiliza técnicas e ferramentas para que mantenha as informações seguras, entre elas estão VPN, senhas, criptografia, antivírus, backup utilizando armazenamento na nuvem.

2.5. VPN

Uma VPN é uma rede privada criada dentro de uma rede pública utilizando protocolosde criptografia. Para ter acesso à essa rede, é necessário possuir as credenciais corretas, caso contrário não será possível conectar a ela. “Uma VPN cria um "túnel" pelo qual você pode enviar dados com segurança, usando ferramentas de criptografia e autenticação[...].” (CISCO, [s.d.]).

Borges, Fagundes e Da Cunha (2019) afirmam que:

> A VPN deve dispor de ferramentas para permitir o acesso de clientes remotos autorizados aos recursos da rede corporativa e viabilizar a interconexão de redes geograficamente distantes, de forma a possibilitar acesso de filiais a matriz. Em geral, uma VPN, deve estar sempre possibilitando o compartilhamento de recursos e informações além de assegurar privacidade e integridade dos dados que trafegam pela Internet.

2.6. Criptografia

A criptografia protege um conjunto de informações, alterando o texto original para impossibilitar a leitura por aqueles que não possuem a chave de decriptografia a informação.

Segundo Ciriaco (2015) "[...]a criptografia é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas emissor e receptor consigam compreendê-la[...]".

2.6.1. Criptografia Simétrica

O modelo mais antigo de criptografia é a simétrica. O elemento que dá acesso à mensagem que foi criptografada, é igual para ambas as partes e deve ser mantida em segredo (privado). Muita das vezes, esta chave é representada por uma senha, onde é utilizada pelo remetente para codificar uma ponta, e pelo destinatário para decodificá-la de outra. A principal vantagem deste tipo de criptografia é a simplicidade. Esta técnica resume em facilidade de uso e rapidez para executar os processos criptográficos. A desvantagem é quando a chave de ciframento é a mesma para o deciframento, onde a esta ultima pode ser facilmente descoberta a partir da primeira, como ambas precisam ser compartilhadas entre origem e destino, elas podem ser interceptadas (OLIVEIRA, 2012).

2.6.2. Criptografia Assimétrica

A chave assimétrica, ou também conhecida como chave pública, na qual cada parte envolvida na comunicação, utiliza duas chaves diferentes, por isso o nome assimétrica. Uma chave é privada e a outra é pública, e neste caso não é utilizado apenas senhas, mas arquivos digitais mais complexos. A chave pública pode ficar disponível para qualquer usuário que desejar se comunicar com outra de modo seguro, porém a chave privada deverá ser secreta e apenas o titular ter acesso a ela. É utilizando a chave privado que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua chave pública (OLIVEIRA, 2012).

2.7. Antivírus

Os antivírus são *softwares* desenvolvidos para agir contra vírus em meios digitais, podendo eliminar a ameaça ou colocar as mesmas em quarentena onde pode realizar alguma

ação posteriormente. Os antivírus são mantidos por empresas da área de segurança da informação (PAULA, 2018).

Segundo Paula (2018):

> Não existe computador imune a vírus, pois a cada dia surgem novos vírus, e leva-se um certo tempo para detectar que o código de um determinado arquivo é destrutivo e seja considerado vírus. Sendo assim, é necessário sempre atualizar o antivírus e evitar a ocorrência de sérios danos ao sistema operacional.

2.8. *Backup* em Nuvem

Como afirma Goodrich (2019) "O *backup* na nuvem, também conhecido como *backup* do computador na nuvem, refere-se ao backup de dados para um servidor remoto baseado na nuvem". A empresa e/ou usuário que realizar um *backup* na nuvem pode acessar os dados remotamente a partir de um login de cliente, geralmente por um navegador web.

Segundo Ferreira e Da Silva (2019):

> O *backup* em nuvem é uma estratégia da empresa onde quaisquer tipos de cópias de segurança das informações possam ser mantidas, como por exemplo, dados da rede ou pessoais obtidos por meio de uma locação remota, baseando-se também na nuvem.

3. METODOLOGIA

Inicialmente, o tema deste trabalho foi escolhido devido ao aumento do trabalho remoto e a demanda pela segurança da informação, além do interesse pessoal para maior aprendizagem sobre a segurança da informação.

Após a escolha do tema, foi realizada uma pesquisa bibliográfica sobre trabalho remoto e segurança da informação e seus princípios básicos através de sites, documentos e trabalhos relacionados ao tema encontrados na internet.

Também, foi realizado na norma ISO/IEC 27002 um estudo sobre as diretrizes de como uma organização deve implementar políticas que definam condições, restrições, tecnologias e boas práticas de segurança da informação em ambientes para trabalho remoto.

Na sequência, foi realizada uma pesquisa na internet para entender e definir quais são as principais configurações e tecnologias utilizadas em um ambiente para trabalho remoto seguindo indicações propostas pela ISO/IEC 27002.

Em seguida, com todos os dados obtidos, foi criada uma seção onde o propósito é mostrar quais são as indicações da norma ISO/IEC 27002 em relação ao trabalho remoto e quais tecnologias e configurações podem suprir as necessidades dessas indicações.

Por fim, foi montado e testado a simulação de um ambiente destinado ao trabalho remoto aplicando todas tecnologias e configurações propostas.

4. DESENVOLVIMENTO

Este capítulo é destinado a apresentar cada etapa realizada para o desenvolvimento do guia de boas práticas e a simulação do ambiente para trabalho remoto utilizando as configurações propostas. Foram escolhidos os sistemas operacionais Windows 10 para o cliente e Linux (Ubuntu 20.10) baseado nas estatísticas da W3 TECH (W3 TECH, 2021).

4.1. Definição das principais configurações e tecnologias utilizadas em um ambiente para trabalho remoto

No contexto de trabalho remoto, as principais configurações e tecnologias utilizadas são:

4.1.1. Acesso Remoto

A ISO/IEC 27002 na seção 6.2.2 - Trabalho Remoto, recomenda os requisitos de segurança que uma organização deve ter, levando em consideração o acesso remoto aos sistemas internos e a sensibilidade tanto das informações acessadas e trafegadas quanto do próprio sistema interno.

Para realizar o acesso remoto de forma segura, a forma mais simples é utilizar uma VPN. Segundo (HARA, 2015), “A segurança é a primeira e mais importante função da VPN”.

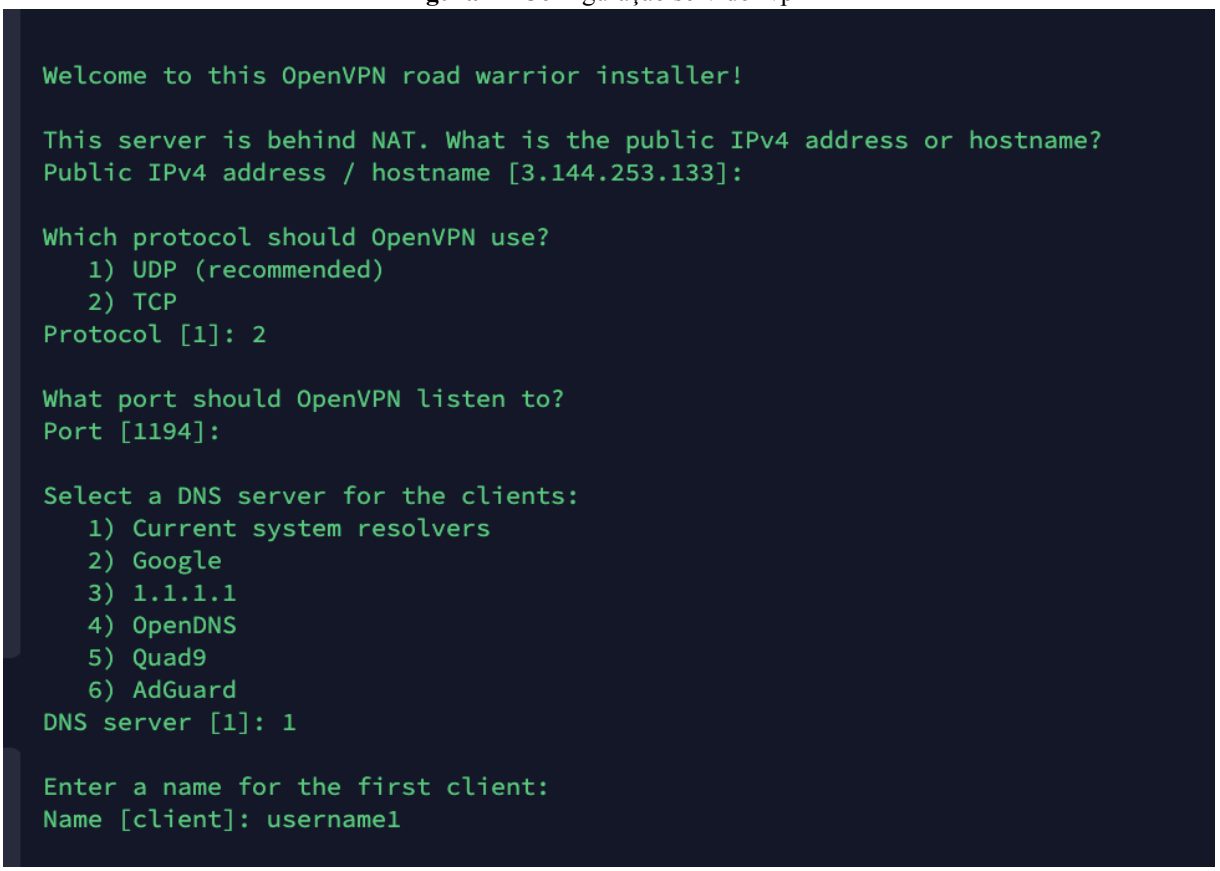
4.1.1.1. Como configurar e utilizar uma VPN

Como parte das configurações essenciais a VPN cumpre o papel de "tunelar" os dados trafegados apenas por uma rede privada, permitindo um maior controle por parte dos administradores.

4.1.1.1.1. Como configurar o servidor VPN

Para o servidor foi utilizado uma máquina virtual Ubuntu 20.04.2 LTS e a aplicação servidor escolhida foi o OpenVPN.

Figura 1 - Configuração servidor vpn



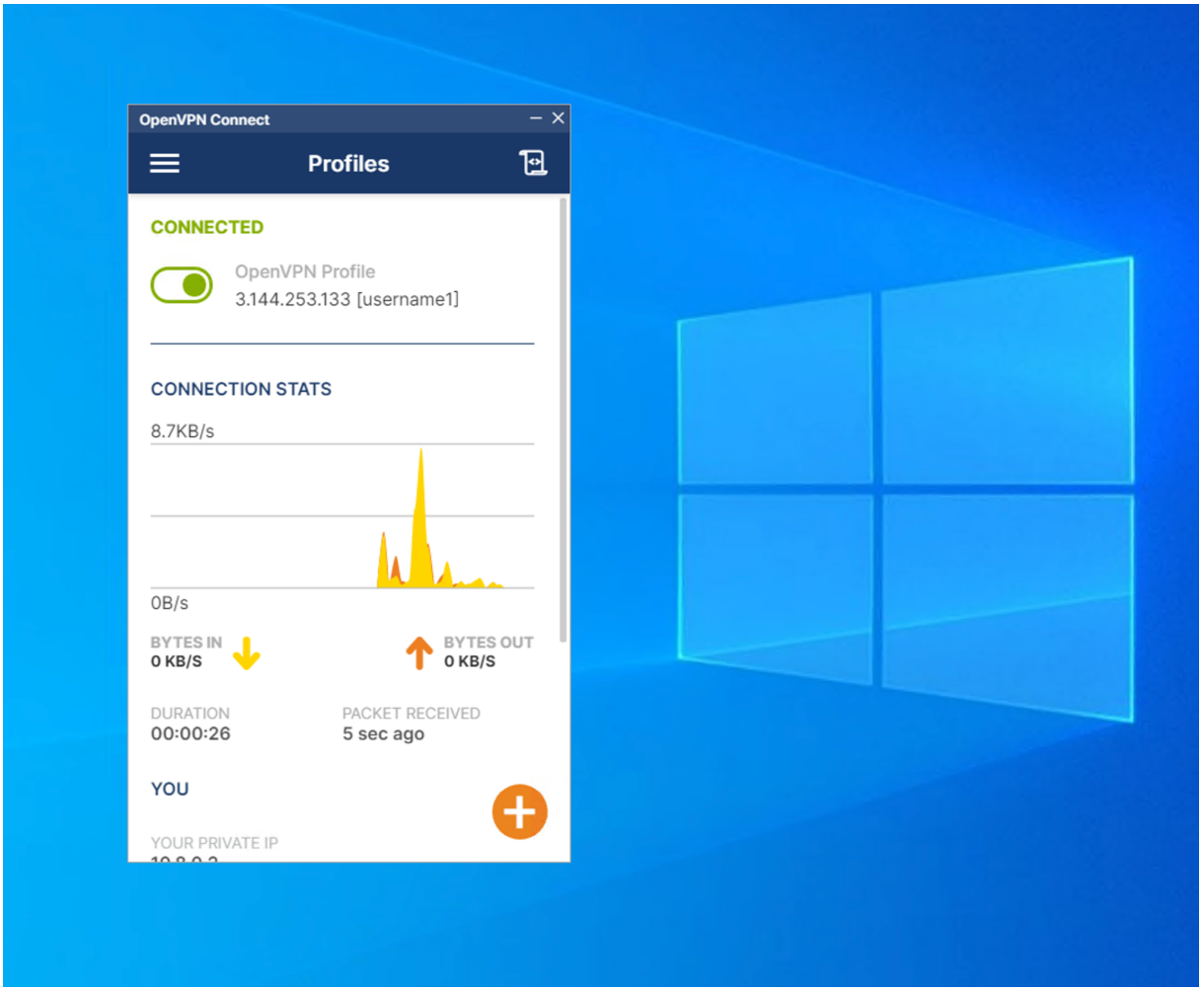
Fonte: Print screen server do OpenVPN no Ubuntu.

Ao final do processo foi gerado um certificado para o usuário especificado, aqui chamado de 'username1', o arquivo então foi compartilhado através da pasta do backup em nuvem com o cliente para configuração do ambiente.

4.1.1.1.2. Como configurar o cliente VPN

No Windows foi baixado a aplicação cliente do OpenVPN e com o certificado compartilhado na etapa anterior foi criado o perfil para a conexão segura do cliente ao servidor.

Figura 2 – Conexão com o client vpn



Fonte: Print screen cliente OpenVPN no windows10

Após a conexão com a VPN todos os dados trafegados foram primeiramente passados pela vpn, evitando-se assim o tráfego de dados privados em redes públicas.

4.1.2. Criptografia de dados

Para manter seus arquivos seguros longe de pessoas que não possuem permissão para obtê-los, a ISO/IEC 27002 recomenda a utilização de criptografia, sendo assim é possível proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Para realizar a criptografia, alguns softwares podem ser utilizados, tais como:

- AESCrypt
- AxCrypt
- DiskCryptor
- DMCrypt
- Minilock

- VeraCrypt

Para este guia de boas práticas foi utilizado o AESCrypt devido ser uma ferramenta *OpenSorce* e compatível com diversos sistemas operacionais.

4.1.2.1. Como instalar e utilizar o AESCrypt

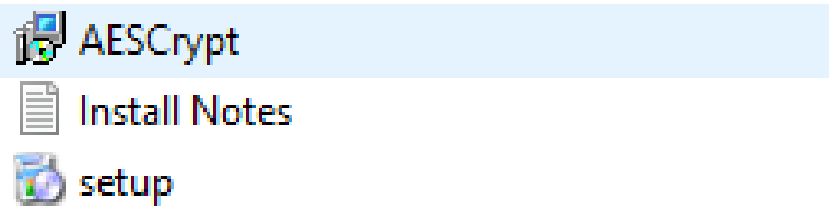
Primeiramente, foi preciso entrar no site oficial do AESCrypt na página de download (https://www.aescrypt.com/download/) e escolher o link de download de acordo com o sistema operacional e arquitetura do ambiente para trabalho remoto como mostra a Figura 16.

Figura 16 – Download AESCrypt

Fonte: Site AESCrypt

Em seguida, foi aberto o arquivo zip baixado. Como foi baixado para o sistema operacional Windows10 x64, nele continha 3 arquivos: AESCrypt.msi, Install Notes.txt e setup.exe como mostra a Figura 17.

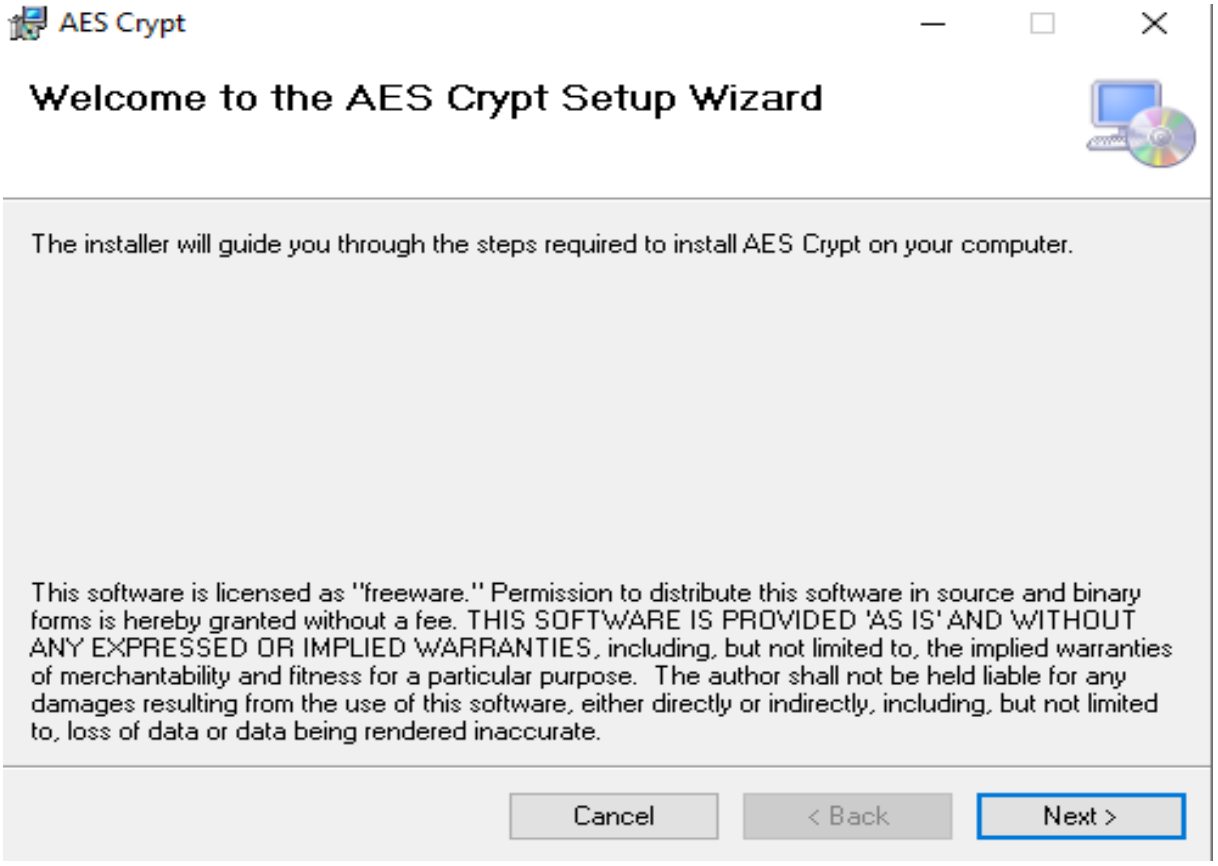
Figura 17 - Arquivo zip AESCrypt



Fonte: Print screen arquivos no Windows 10

Primeiro, foi executado o AESCrypt.msi e como mostra a Figura 18, foi apresentado a seguinte tela e realizado o clique no botão "*next*".

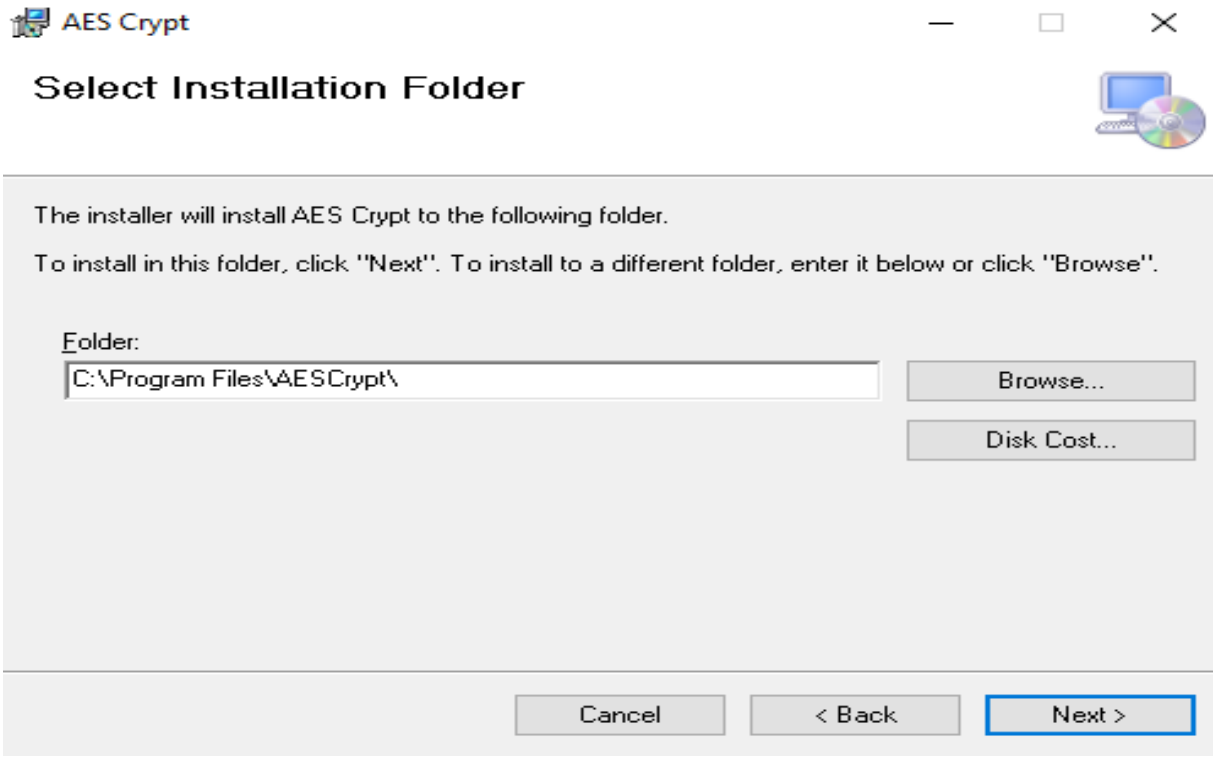
Figura 18 – Passo 1 Instalação AESCrypt



Fonte: Print screen instalação AESCrypt no Windows 10

Em seguida, o instalador do AESCrypt pediu para selecionar o local de instalação. Neste guia, foi deixado o caminho padrão, mas caso queira mudar é só clicar no botão "*browse...*" e selecionar o novo caminho. Quando estiver com o local selecionado, clique no botão "*next*" como mostra a Figura 19.

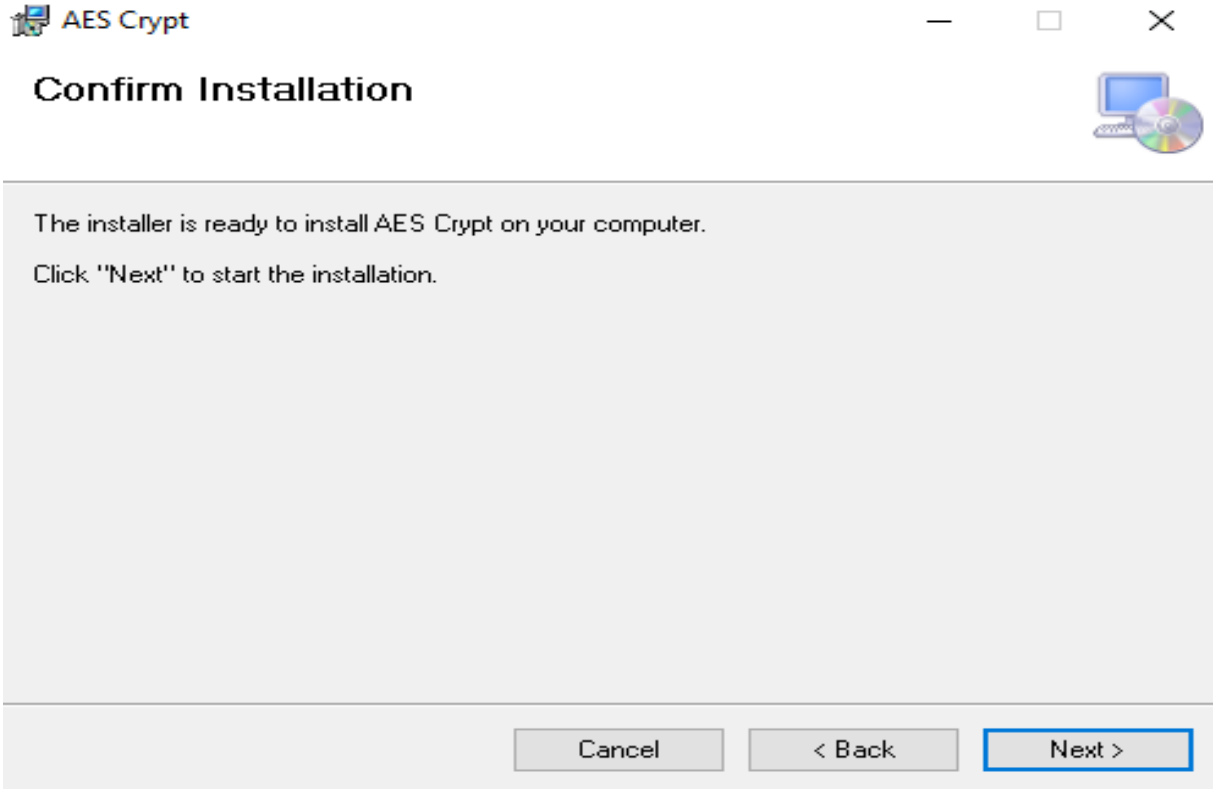
Figura 19 – Passo 2 Instalação AESCrypt



Fonte: Print screen instalação AESCrypt no Windows 10

Logo após, foi clicado no botão "*next*" novamente para começar a instalar os arquivos no caminho escolhido anteriormente como mostra a Figura 20.

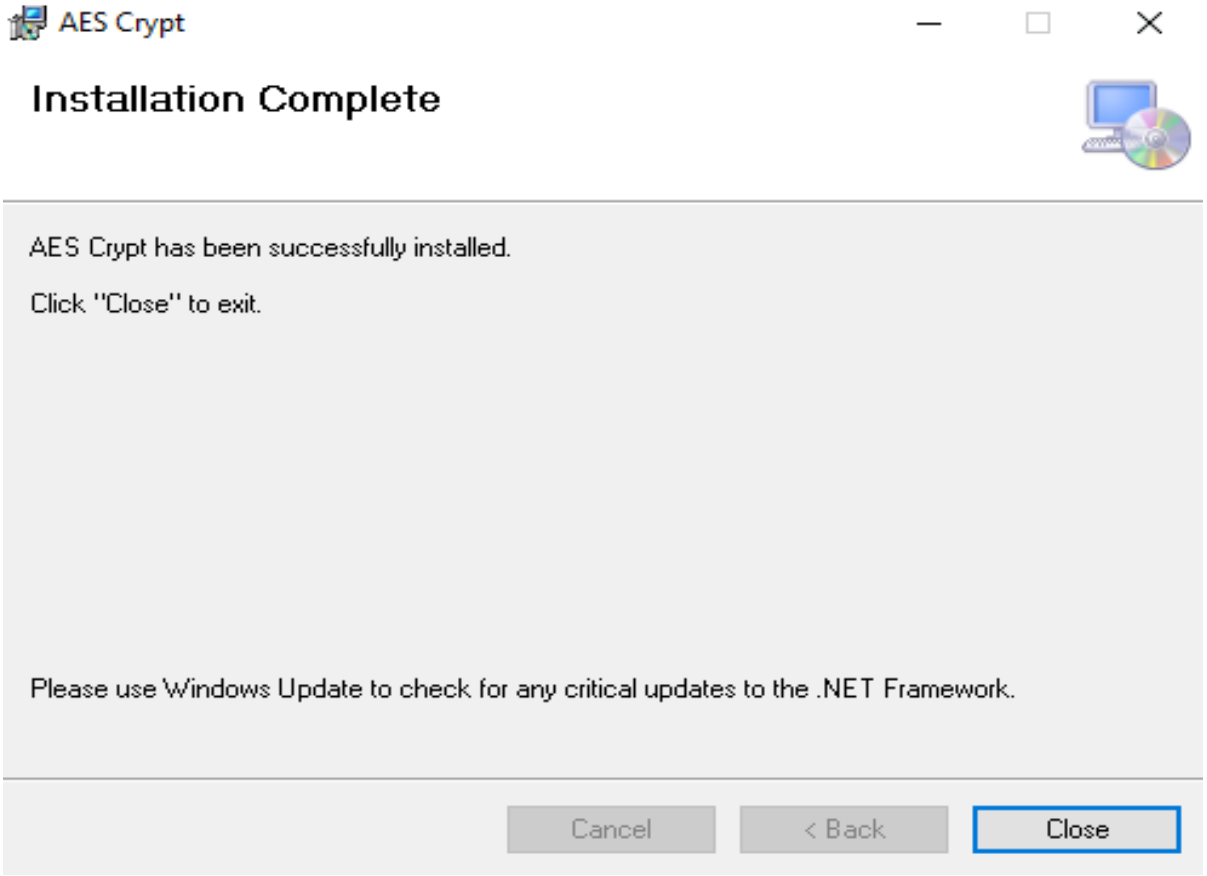
Figura 20 – Passo 3 Instalação AESCrypt



Fonte: Print screen instalação AESCrypt no Windows 10

Por fim, o AESCrypt foi instalado. Para fechar o assistente de instalação, foi clicado no botão “Close” como mostra a Figura 21.

Figura 21 – Passo 4 Instalação AESCrypt

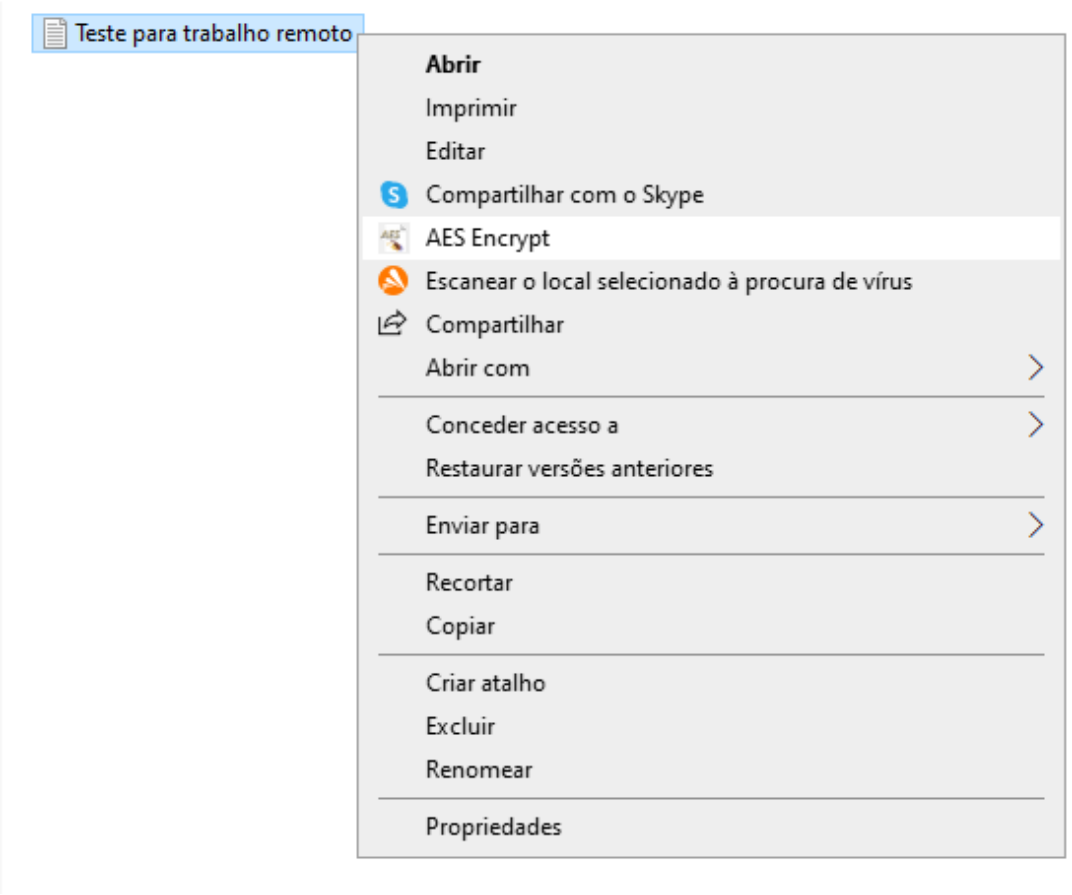


Fonte: Print screen instalação AESCrypt no Windows 10

Como foi mostrado na figura 17, ainda restam 2 arquivos, o *Install Notes*.txt e o setup.exe. O *Install Notes* é um arquivo de texto explicando alguns passos de como instalar o AESCrypt, e o *setup*.exe é um software para detectar se no sistema operacional está faltando algum programa que auxilia no funcionamento do AESCrypt.

Para utilizar o AESCrypt e criptografar arquivos foi necessário navegar até o arquivo desejado e clicar com o botão auxiliar do mouse e escolher a opção AES Crypt como mostra a Figura 22.

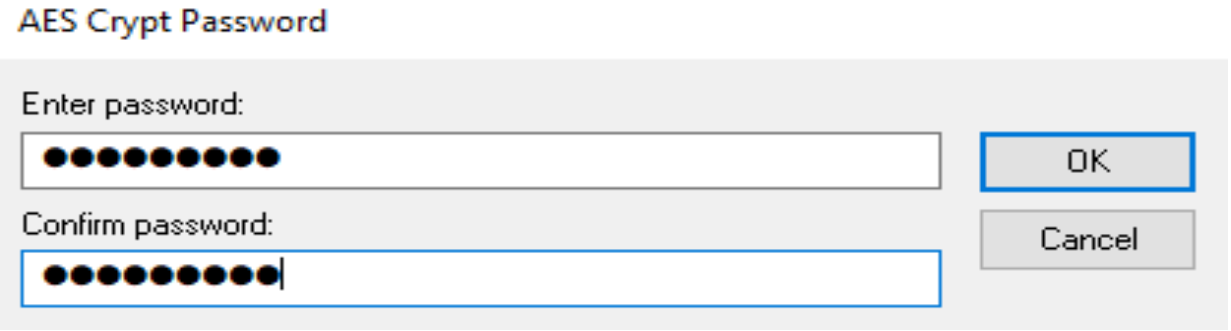
Figura 22 – Passo 1 Utilizando AESCrypt



Fonte: Print screen utilizando aplicação AESCrypt no Windows 10

Por fim, foi escolhido uma senha para poder criptografar o arquivo como mostra a Figura 23.

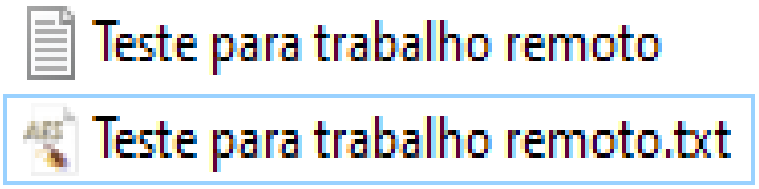
Figura 23 *– Passo 2 Utilizando o AESCrypt*



Fonte: Print screen aplicação AESCrypt

O AESCrypt gerou um arquivo do tipo .aes como mostra a Figura 24. Foi necessário destruir o arquivo que não possuía criptografia para manter a segurança.

Figura 24 – Passo 3 Utilizando o AESCrypt



Fonte: Print screen arquivo criptografado no Windows 10

Por fim, para descriptografar o arquivo, foi necessário clicar duas vezes nele e inserir a senha definida anteriormente.

4.1.3. Senhas

A ISO/IEC 27002 na seção 9.3.1 - Uso da informação de autenticação secreta, indica cinco propriedades para se obter uma senha de qualidade:

- fáceis de lembrar;
- não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;
- não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras incluídas no dicionário);
- isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;
- caso a senha seja temporária, ela deve ser mudada no primeiro acesso;

Já a OWASP (Open Web Application Security Project), comunidade de segurança da informação para aplicações web, possui uma implementação de controle adequado de força para senhas que são:

- Senhas com menos de 8 caracteres são consideradas fracas;
- A quantidade de caracteres do campo da senha de uma aplicação não pode ser muito baixo, pois impede ao usuário que utilize softwares para criação de senhas;
- Permitir todos os caracteres incluindo unicode e espaços em branco;

- Mostrar a barra de força para o usuário saber se a senha é forte ou não;

Uma forma de se obter senhas seguras, rápidas e fáceis é utilizando o 1password, que faz a geração e armazenamento de senhas.

4.1.3.1. Como utilizar o 1Password

O 1Password gera as suas senhas com algumas opções escolhida pelo usuário. É possível gerar senhas aleatórias, senhas fáceis de ser lembradas e senhas utilizando apenas números também de forma aleatória, onde as senhas com alfas numéricos podem ter tamanhos de até 64 caracteres e senhas com apenas números com tamanhos de 12 caracteres. Para isso, os seguintes passos mostram como utilizar o 1Password.

Primeiramente foi conectado no site oficial do 1Password (www.1password.com) e criado uma nova conta no sistema para autenticação.

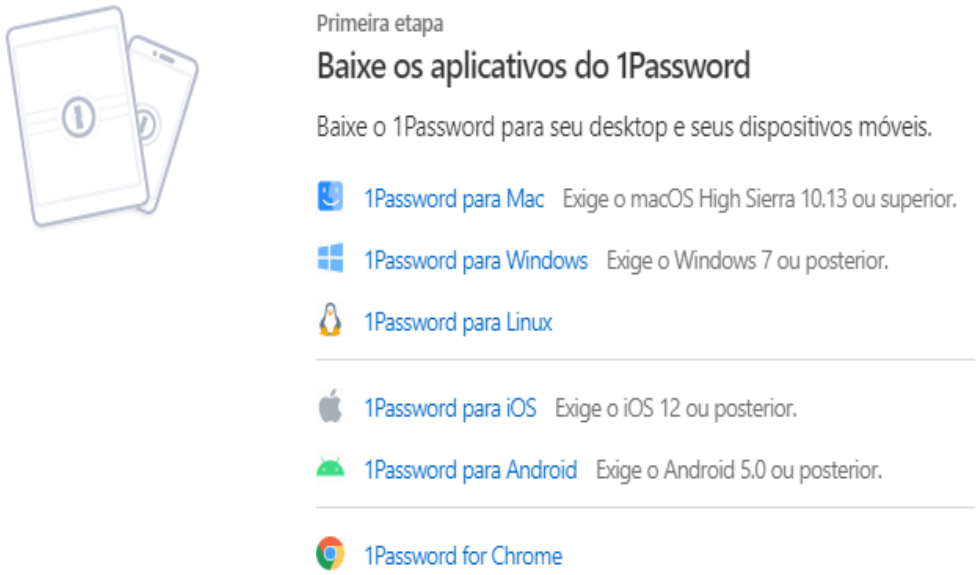
Logo após estar autenticado, foi clicado em “baixe os aplicativos” como mostra a Figura 3.

Figura 3 - Download dos aplicativos de gerenciamento de senhas

Fonte: Print screen site 1password

Em seguida foi escolhido o arquivo para download de acordo com seu sistema operacional como mostra a Figura 4.

Figura 4 - Escolha do sistema operacional para download do aplicativo

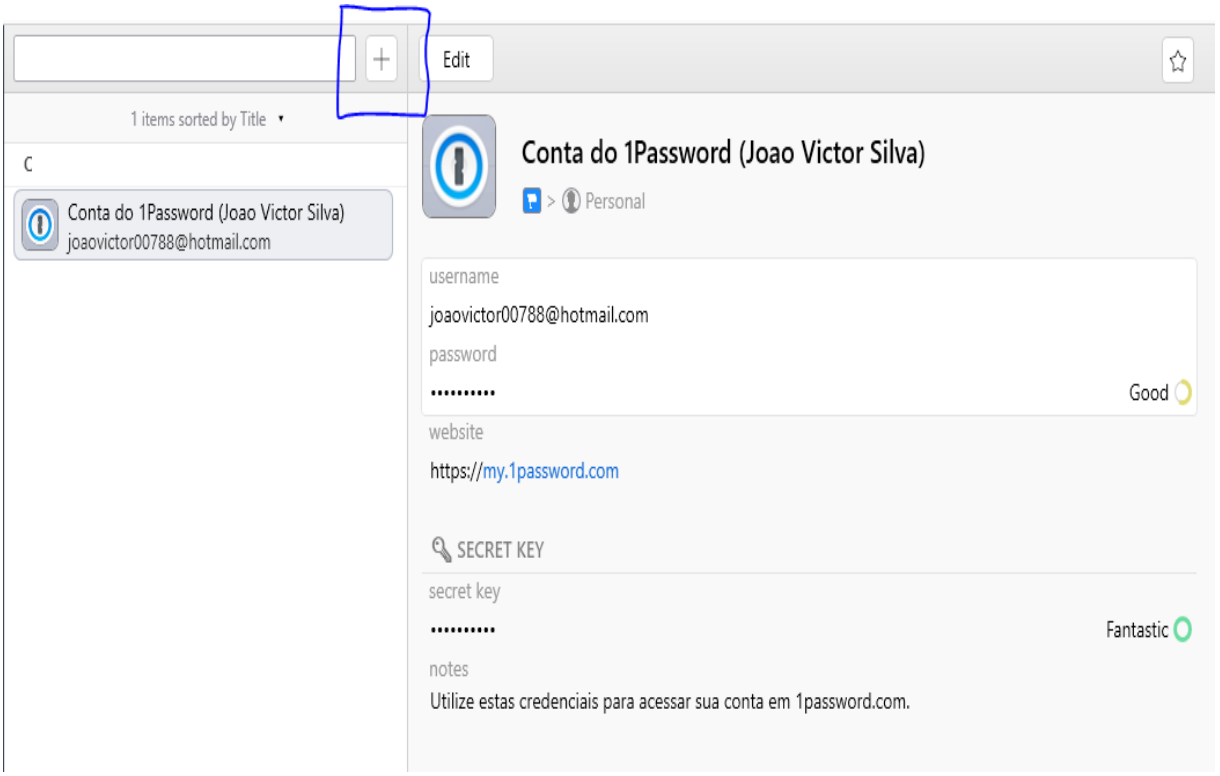


Fonte: Print screen site 1password

Foi instalado o software no sistema operacional e realizado a autenticação.

Na sequência foi clicado no botão "*New Item*" como mostra a Figura 5, também é possível utilizar o atalho (Ctrl+ N).

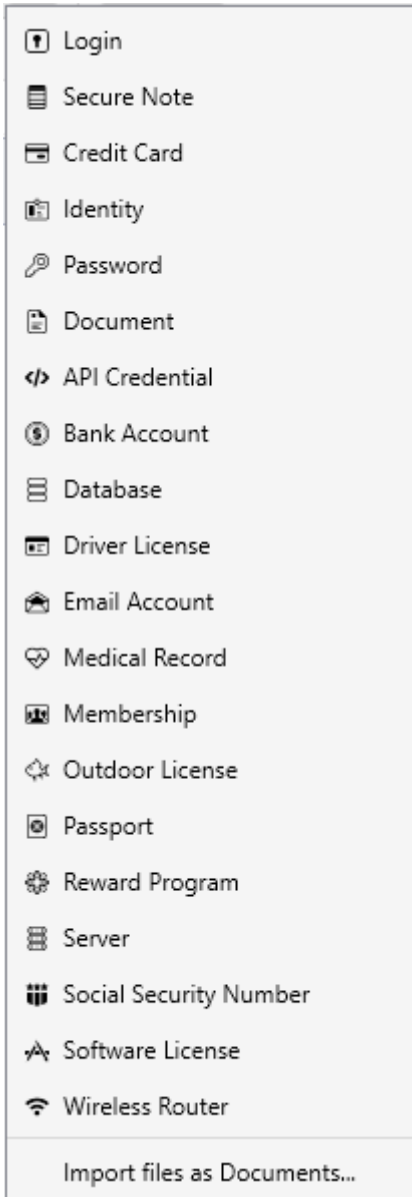
Figura 5 - Botão para adicionar novo item.



Fonte: Print screen aplicação 1password

E foi escolhido o tipo de serviço utilizado para se autenticação como mostra a Figura 6.

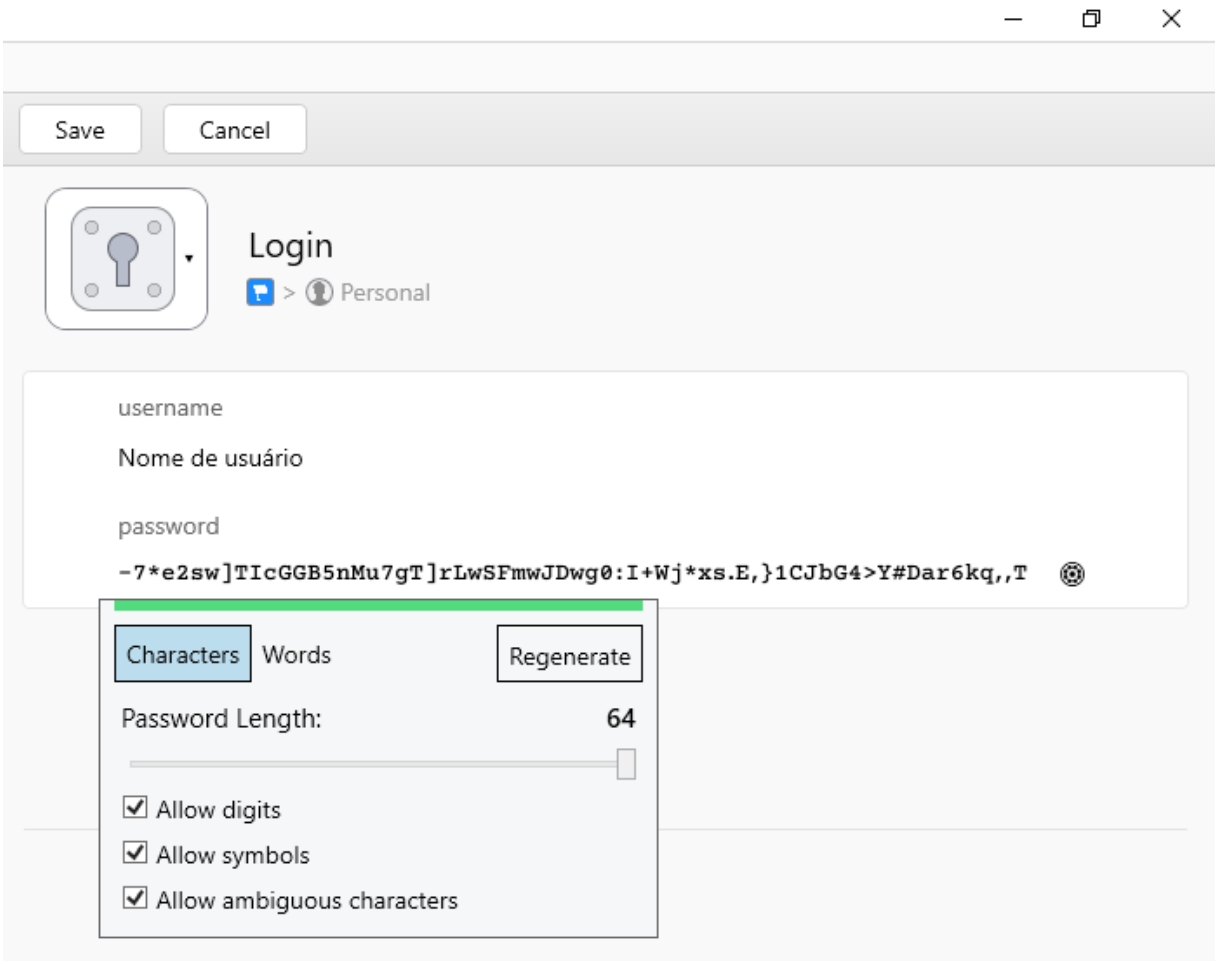
Figura 6 - Serviços para realizar autenticação.



Fonte: Print screen aplicação 1password.

Em seguida foi preenchido o campo de *username* e clicado no ícone no campo *password*, e foi marcado todas as opções apresentadas e escolhido a quantidade de caracteres para sua senha. Logo após, foi clicado no botão "*Save*" como mostra a Figura 7.

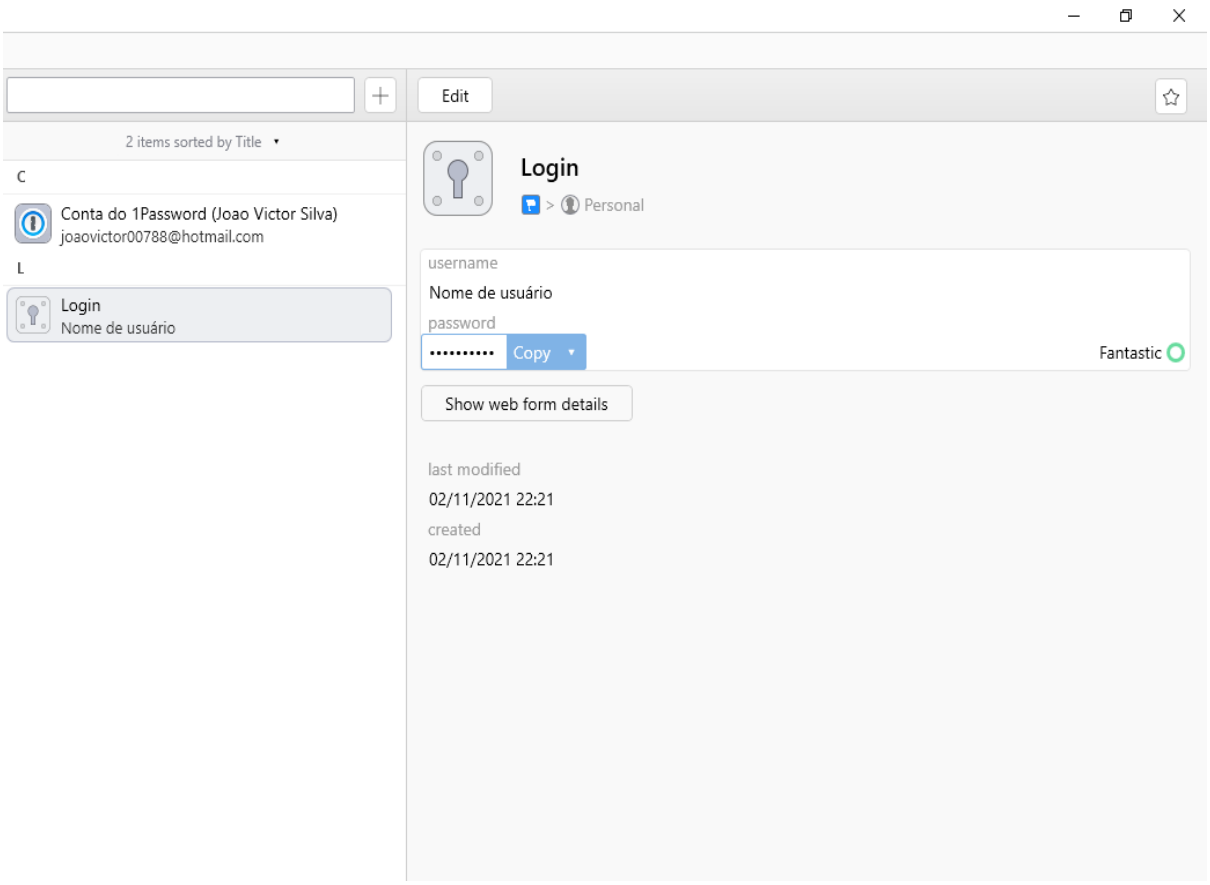
Figura 7 - Geração de senhas.



Fonte: Print screen aplicação 1password.

Na sequência, a senha para autenticação foi armazenada no software e para acessá-la, foi preciso clicar no serviço escolhido anteriormente e clicar no botão "*copy*" como mostra a Figura 8.

Figura 8 - Armazenamento de senhas.



Fonte: Print screen aplicação 1password.

4.1.4. Antivírus

Como diretriz para implementação do modelo de trabalho remoto, a ISSO/IEC 27002, indica também o uso de antivírus.

O antivírus é uma ferramenta que possui a utilidade de detectar, interromper e combater softwares e arquivos potencialmente maliciosos e indesejáveis (OBERHEIDE, COOKE, JAHANIAN, 2008).

Existem vários tipos de antivírus que pode ser encontrado em diversos locais de distribuições e vendas, como na internet e lojas de tecnologias, sendo alguns eles:

- Avast Antivírus
- AVG Antivírus
- Kaspersky Antivírus
- McAfee Antivírus
- Norton Antivírus
- Panda Antivírus

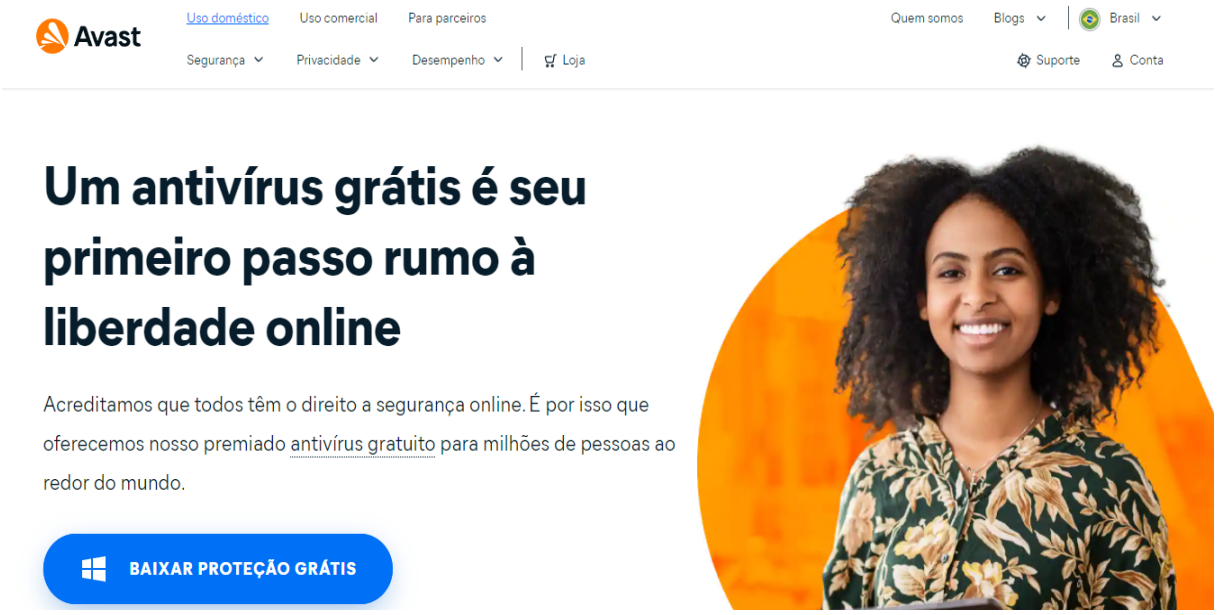
Para este guia de boas práticas, foi utilizado o Avast Antivírus devido a sua versão gratuita, compatível com diversos sistemas operacionais e apresentar dados sobre detecção e bloqueio de ataques. O Avast em 2021, detectou e bloqueou cerca de 500.000 golpes de sextorsão, onde os criminosos aproveitaram o aumento do uso de serviços que utilizam câmeras para videoconferências durante a pandemia do Covid-19. Como mostra o relatório de Ameaças Digitais da Avast no 3° trimestre de 2021, houve um grande aumento de vítimas envolvendo ataques de ransomwares, Trojans de Acesso Remoto (RATs), rootkits, ladrões de dados, malwares bancários para celulares (AVAST, 2021).

Para utilizar o Avast Antivírus, siga os seguintes passos.

4.1.4.1. Como instalar e utilizar o Avast Antivírus

Primeiramente foi preciso entrar no site oficial do Avast, (www.avast.com) e clicar no botão “baixar proteção grátis” como mostra a Figura 9.

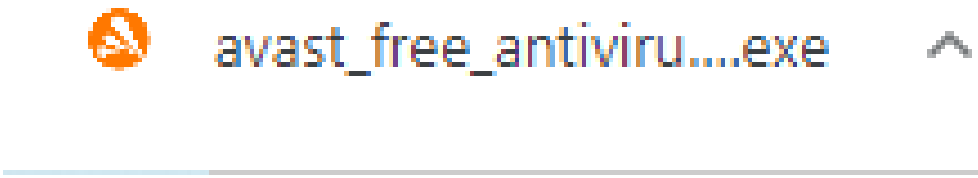
Figura 9 – Botão download Avast



Fonte: Print screen site Avast.

Em seguida foi executado o arquivo .exe de instalação do Avast como mostra a Figura 10.

Figura 10 – Arquivo .exe Avast



Fonte: Print screen executável no Windows 10

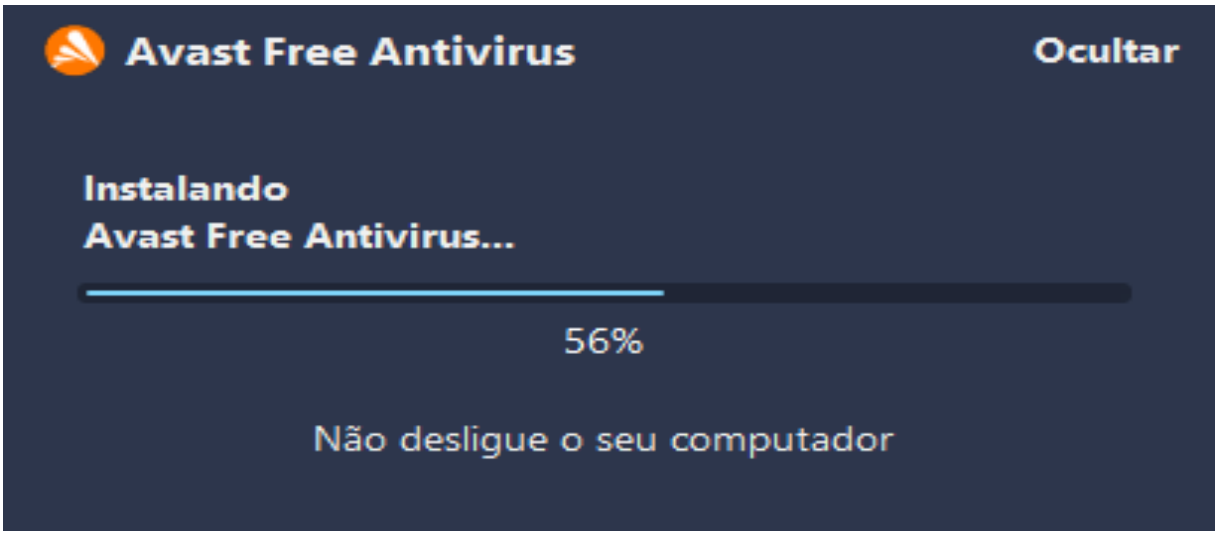
Logo após, na tela de execução do instalador do Avast, foi clicado no botão "INSTALAR" como mostra a Figura 11.

Figura 11 – Instalar Avast

Fonte: Print screen aplicação Avast

Em seguida, foi aguardado todo o carregamento da instalação como mostra a Figura 12.

Figura 12 – Carregando instalação Avast



Fonte: Print screen aplicação Avast

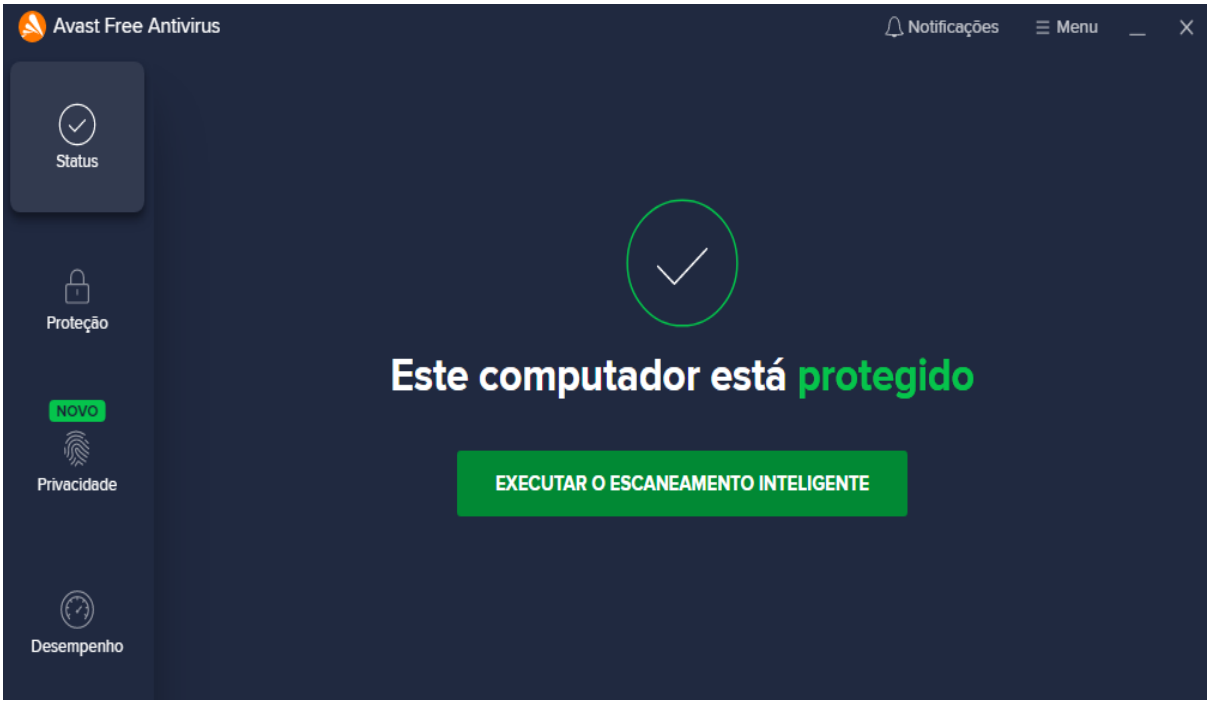
Logo após carregar a instalação, foi informado uma tela de aviso dizendo que a instalação foi concluída e com um botão que foi clicado com o nome de “CONTINUAR” como mostra a Figura 13.

Figura 13 – Instalação Avast concluída

Fonte: Print screen aplicação Avast

Em seguida, foi aberto a tela principal do Avast, com as informações sobre o estado do computador. Para fazer uma varredura e escaneamento do sistema, foi necessário clicar no botão “EXECUTAR O ESCANEAMENTO INTELIGENTE” como mostra a Figura 14.

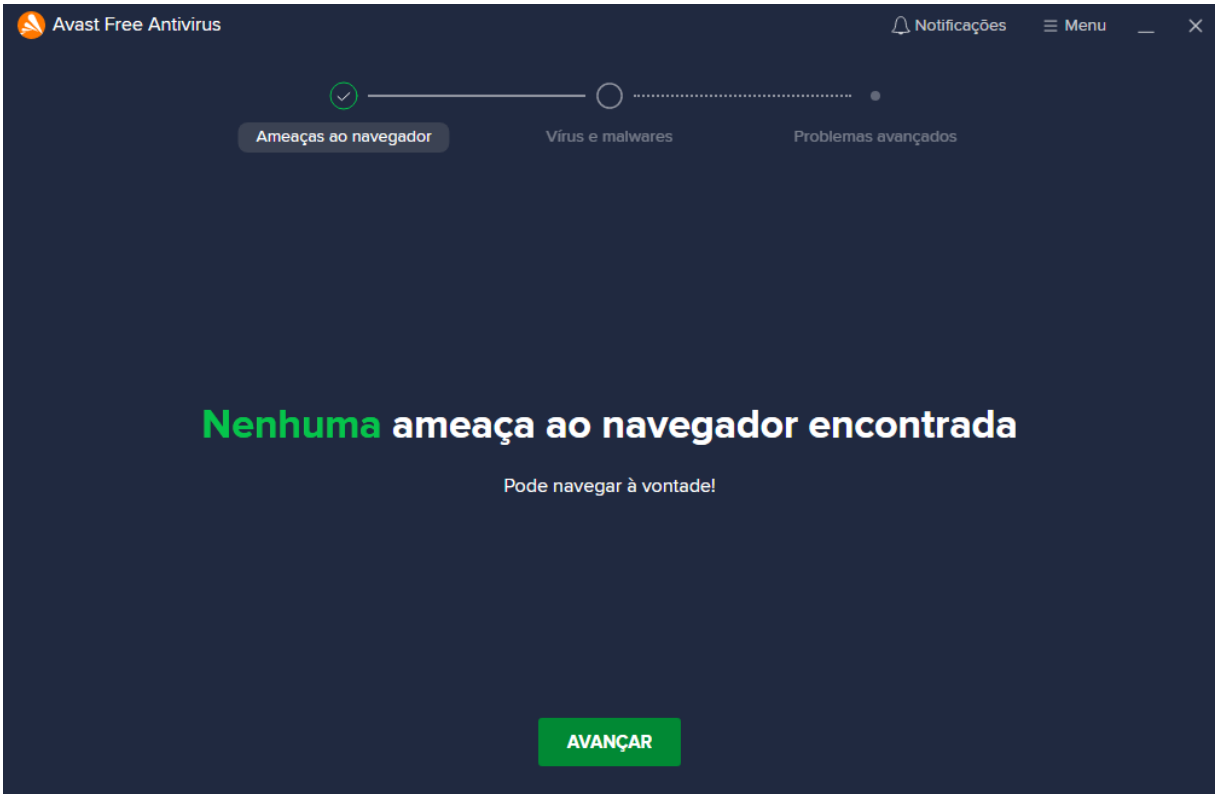
Figura 14 – Tela principal Avast.



Fonte: Print screen aplicação Avast

Na sequência foi mostrado uma tela com 3 níveis: Ameaças ao navegador, Vírus e malwares e Problemas avançados. Onde foi verificado cada um deles em busca de ameaças e softwares indesejáveis e problemas que possam facilitar a entrada de novos programas maliciosos como mostra a Figura 15.

Figura 15 – Escaneamento Inteligente



Fonte: Print screen aplicação Avast

4.1.5. *Backup* em nuvem

Para manter cópias de seguranças e não ocorrer perda de dados, a ISO/IEC 27002 recomenda a utilização de backups.

O backup em nuvem possui algumas vantagens em relação ao backup feito em armazenamentos físico (HDs, SSDs e *Pendrives*) como: o acesso à informação em qualquer lugar que possua acesso à internet e diminuição de custos (AMADO, 2015).

Existem diversos serviços que possibilitam o backup em nuvem, como:

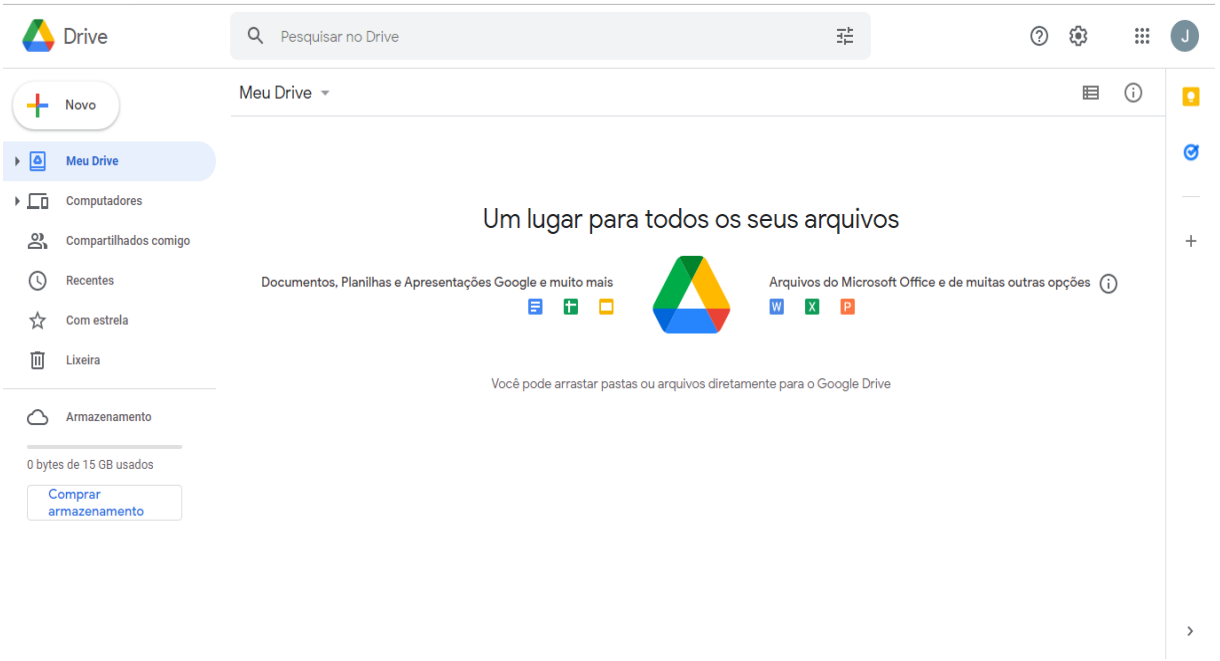
- Dropbox
- Google Drive
- iCloud
- One Drive

O serviço que foi utilizado para realizar o *backup* em nuvem neste guia de boas práticas foi o Google Drive devido ser um serviços que fornece até 15 GB de armamento gratuito e pode-se armazenar qualquer tipo de arquivo, além de fornecer boa disponibilidade do serviço oferecido.

4.1.5.1. Como Utilizar o Google Drive

Primeiramente foi necessário acessar o site oficial do Google Drive (https://drive.google.com) e realizar a autenticação da conta Google. Caso não possua uma conta Google, basta criar uma. Ao autenticar, foi apresentado a página inicial do Google Drive como mostra a Figura 25.

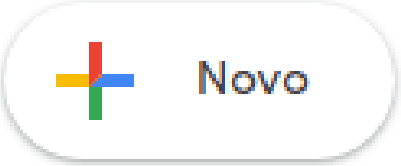
Figura 25 – Passo 1 Utilizando Google Drive



Fonte: Print screen site Google Drive

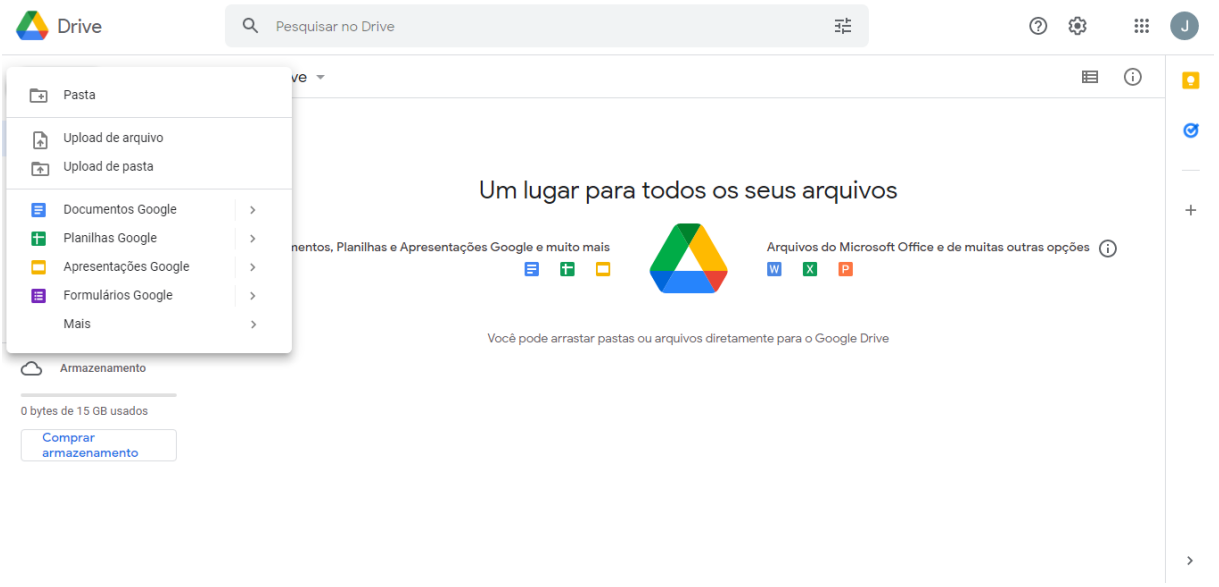
Para criar uma pasta ou fazer upload de um arquivo ou pasta, foi necessário clicar no botão “Novo” e escolhido a opção desejado como mostra as Figuras 26 e 27 respectivamente.

Figura 26 – Passo 2 Utilizando Google Drive



Fonte: Print screen aplicação Google Drive

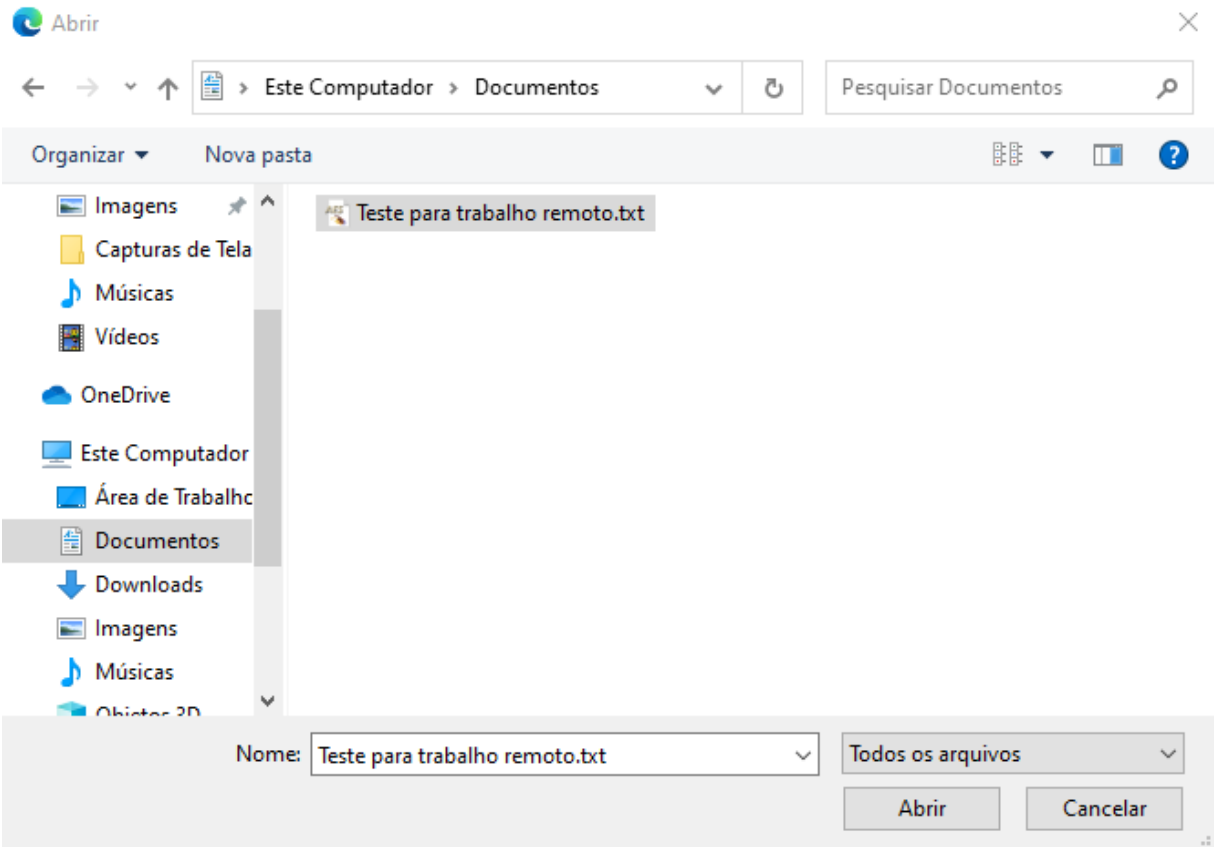
Figura 27 – Passo 3 Utilizando Google Drive



Fonte: Print screen site Google Drive

Em seguida foi aberto o gerenciador para buscar o arquivo para *upload* como mostra a Figura 28.

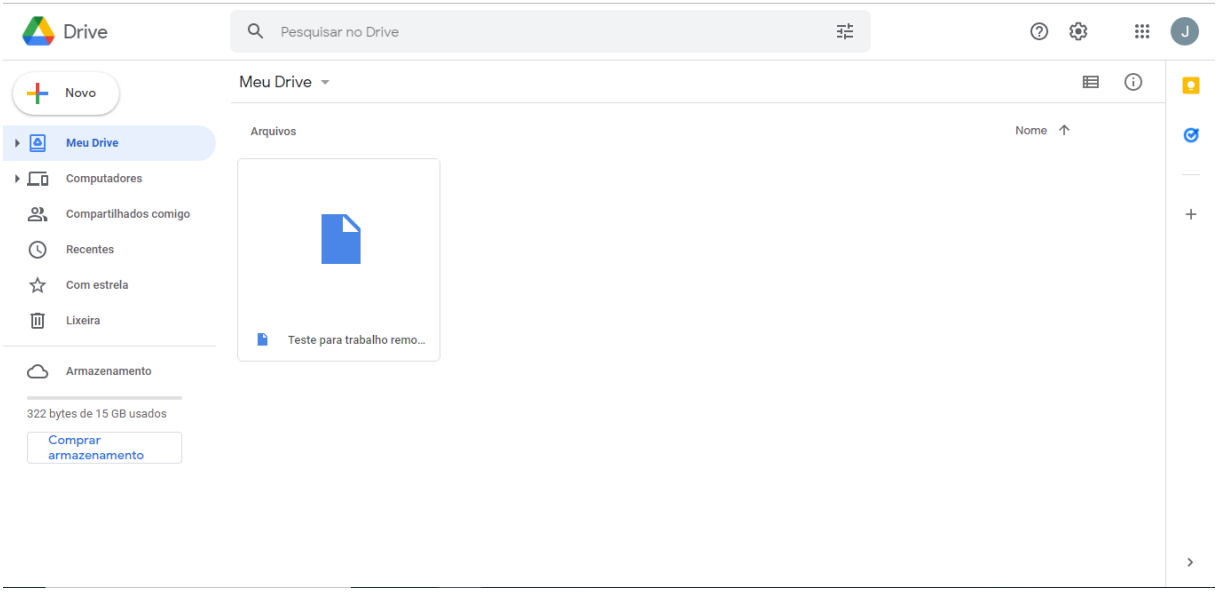
Figura 28 – Passo 4 Utilizando o Google Drive



Fonte: Print screen seletor de arquivos do Windows 10

Por fim, foi realizado o *upload* do arquivo, sendo assim foi realizado o *backup* em nuvem como mostra a Figura 29.

Figura 29 – Passo 5 Utilizando o Google Drive



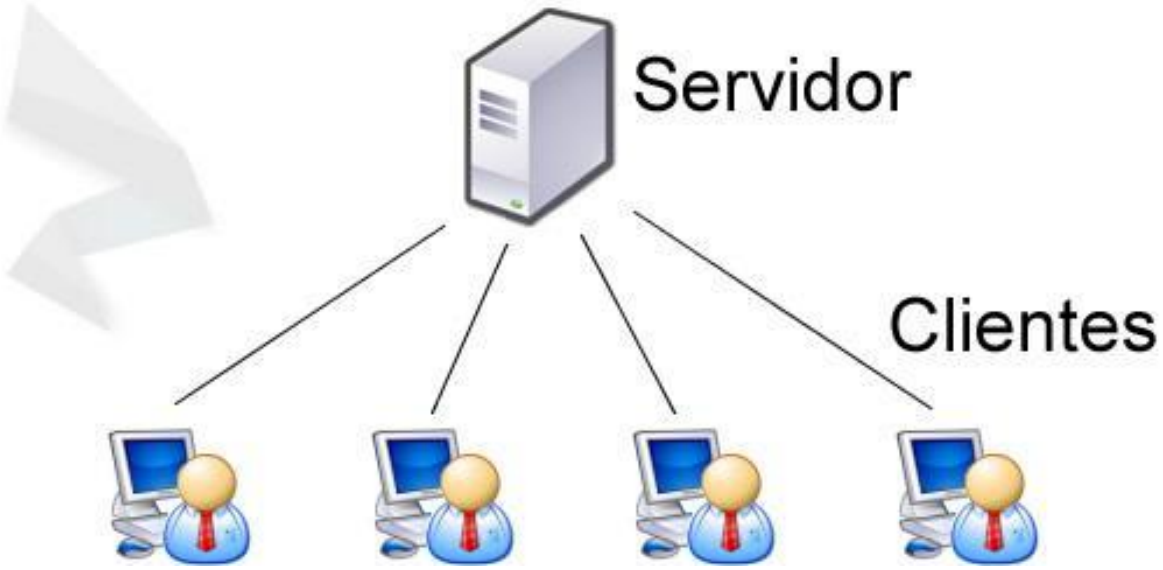
5. Fonte: Print screen site Google Drive

5.1. Simulação do ambiente para Trabalho Remoto

Foi configurada uma máquina virtual com o sistema operacional Windows 10 e com as configurações propostas pelo guia de boas práticas para simular o ambiente de Trabalho Remoto, onde o ambiente realizou, com sucesso, a conexão um servidor FTP simulando uma conexão do ambiente do funcionário à empresa em que trabalha.

Para isso foi utilizado o modelo de arquitetura cliente/servidor como mostra a Figura 30.

Figura 30 - Arquitetura cliente/servidor



Fonte: Site ctrlzeta

6. CONSIDERAÇÕES FINAIS

Este trabalho apresentou um guia de boas práticas para melhorar o nível de segurança de um ambiente de trabalho na modalidade de teletrabalho. Um conjunto de passos foi seguido para montagem do ambiente de trabalho com as diretrizes estabelecidas pela ISO/IEC 27002.

Foram realizadas análises na finalidade e nos requisitos dos sistemas aqui utilizados, além da montagem do ambiente de trabalho seguindo as diretrizes estabelecidas pela ISO/IEC 27002 e a documentação dos passos seguidos.

Fica como sugestão submeter as configurações propostas aqui à uma bateria de testes de penetração utilizando-se de técnicas mais conhecidas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT/CB-21. **Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos.** 2013.

ALENCAR, Gliner Dias; QUEIROZ, Anderson Apolonio Lira; DE QUEIROZ, Ruy José Guerra Barretto. Insiders: análise e possibilidades de mitigação de ameaças internas. **Revista Eletrônica de Sistemas de Informação**, v. 12, n. 3, 2013.

ALVES, Amabily A.; REZENDE, Camila A. **O TRABALHO HOME OFFICE E SUAS REPERCURSSÕES NAS RELAÇÕES DE EMPREGO.** Artigo (Direito) - Centro Universitário Una. Bom Despacho [2021].

AMADO, Wesley Ricardo; MARCONDES, Cesar Augusto Cavalheiro. Análise do Software BSN para a Realização de Backups na Nuvem. **Revista TIS**, v. 3, n. 3, 2015.

ASSUNÇÃO, Marcos Flávio Araújo. **Guia do hacker brasileiro**. Marcos Flávio Araújo Assunção, 2002.

ÁVILA, Maria Amélia. **Prejuízo global com ataques cibernéticos a empresas deve chegar a US$ 6 trilhões em 2021.** Hoje em Dia. 24 set. 2021. Disponível em: <https://www.hojeemdia.com.br/primeiro-plano/preju%C3%ADzo-global-com-ataques-cibern%C3%A9ticos-a-empresas-deve-chegar-a-us-6-trilh%C3%B5es-em-2021-1.855562>. Acesso em: 20 out. 2021.

BAPTISTA JUNIOR, J. H.; DIAN, M. de O. A CRESCENTE IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO, SOBRETUDO DURANTE A PANDEMIA. **Revista Interface Tecnológica**, *[S. l.]*, v. 18, n. 1, p. 56-67, 2021. DOI: 10.31510/infa.v18i1.1109. Disponível em: https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/view/1109. Acesso em: 19 nov. 2021.

BELCIC, I. **O que é hacking?** Disponível em: <https://www.avast.com/pt-br/c-hacker>. Acesso em: 17 nov. 2020.

BORGES, Fábio; FAGUNDES, Bruno Alves; DA CUNHA, Gerson Nunes. **Vpn: Protocolos e segurança.** Artigo – Universidade Católica de Petrópolis, 2019. Disponível em: <https://www.lncc.br/~borges/doc/VPN%20Protocolos%20e%20Seguranca.pdf>. Acesso em: 15 nov. 2021.

CIRIACO, D. **O que é criptografia e por que você deveria usá-la Por Douglas Ciriaco | 19 de Novembro de 2015 às 09h21**. Disponível em: <https://canaltech.com.br/seguranca/o-que-e-criptografia-e-por-que-voce-deveria-usa-la/>. Acesso em: 26 mar. 2021.

CISCO. **Como configurar uma VPN**. Disponível em: <https://www.cisco.com/c/pt_br/solutions/small-business/resource-center/security/how-to-set up-a-vpn.html>. Acesso em: 18 nov. 2020.

Com home office, ataques hackers sobem 700% na América Latina. **Extra**. 18 mai. 2021. Disponível em <https://extra.globo.com/economia/com-home-office-ataques-hackers-sobem-700-na-america -latina-25023033.html>. Acesso em: 12 out. 2021.

Comparison of the usage statistics of Linux vs. Windows for websites. **W3 Tech.** Disponível em: <https://w3techs.com/technologies/comparison/os-linux,os-windows>. Acesso em: 12 dez. 2021.

DEMARTINI, Felipe. **Ciberataques crescem 50% durante a migração para home office na pandemia.** Canaltech. 18 mar. 2021. Disponível em: <https://canaltech.com.br/seguranca/ciberataques-crescem-50-durante-a-migracao-para-home-office-na-pandemia-180898/>. Acesso em 15 out. 2021.

FERNANDES, Nélia O. Campo. **Segurança da informação**. Rede e-Tec Brasil/UFMT. 2013.

FERREIRA, Bárbara Gonçalves; DA SILVA, Fábio Henrique Batista. Segurança da Informação: Backup em Nuvem. **Revista Agroveterinária, Negócios e Tecnologias**, v. 4, n. 2, p. 25-41, 2019.

G1. **Vagas de trabalho remoto crescem 215% entre março e novembro; veja cargos com maior demanda.** 6 dez. 2020. Disponível em: <https://g1.globo.com/economia/concursos-e-emprego/noticia/2020/12/06/vagas-de-trabalho-remoto-crescem-215percent-entre-marco-e-novembro-veja-cargos-com-maior-demanda.ghtml >. Acesso em: 15 out. 2021.

GOODRICH, R. **What Is Cloud Backup?** Disponível em: <https://www.businessnewsdaily.com/5018-what-is-cloud-backup.html>. Acesso em: 3 maio. 2021.

HARA, CAROLINE L. **Home Office e as Tecnologias de Acesso Remoto.** Monografia (Tecnólogo em Processamento de Dados) - FATEC. São Paulo, 2015.

IT.EAM. **Entenda o que é vulnerabilidade de segurança e quais são as mais comuns**. Disponível em: <https://it-eam.com/entenda-o-que-e-vulnerabilidade-de-seguranca-e-quais-sao-as-mais-comuns/>. Acesso em: 15 dez. 2020.

IVAN, G. **Cada hacker com o seu chapéu: o bom, o mau e o feio**. Disponível em: <https://www.avira.com/pt-br/blog/hacker-e-chapeus-black-white-gray-hat>. Acesso em: 10 maio. 2021.

KASPERSKY. **O que é cibersegurança?** Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security>. Acesso em: 19 nov. 2020.

MELLO, A. **Os três pilares da segurança da informação**. Disponível em: <https://ead.catolica.edu.br/blog/pilares-da-seguranca-da-informacao>. Acesso em: 13 maio. 2021.

OBERHEIDE, Jon; COOKE, Evan; JAHANIAN, Farnam. CloudAV: N-Version Antivirus in the Network Cloud. In: **USENIX Security Symposium.** 2008. p. 91-106

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital [Revista online]**, v. 31, p. 11-15, 2012.

PAULA, D. P. DE. OFICINA – ANTIVÍRUS. **Instituto Federal Sudeste de Minas Gerais**, 2018.

Relatório de Ameaças Digitais da Avast – 3º trimestre de 2021, **AVAST**. 17 nov. 2021. Disponível em:< https://blog.avast.com/pt-br/avast-threat-labs-q3-report-avast>. Acesso em: 10 dez. 2021

SILVA, Fernando Moreira da. **Os ataques de hackers contra a segurança da informação: estudo de caso-Kevin Mitnick**. Orientadora: Acácia de Fátima Ventura. 58 f. 2013. TCC (Graduação) – Segurança da Informação, Faculdade de Tecnologia de Americana Curso de Análise de Sistemas e Tecnologia da Informação, Americana, SP 2019. Disponível em:< http://ric.cps.sp.gov.br/bitstream/123456789/1206/1/20132S_SILVAFernandoMoreirada_CD1710.pdf>. Acesso em: 12 nov. 2021.

SOBRATT. **Questões**. Disponível em: <http://www.sobratt.org.br/index.php/certificacao/questoes/>. Acesso em: 16 nov. 2020.

The 2020 State of Remote Work. **BUFFER**, 2020. Disponível em: < https://lp.buffer.com/state-of-remote-work-2020>. Acesso em: 06 nov. 2021.