PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

UTILIZAÇÃO DA VPN NO CENÁRIO DE TELETRABALHO

ISABELLA ALVES CARVALHO

GOIÂNIA
2023

ISABELLA ALVES CARVALHO

UTILIZAÇÃO DA VPN NO CENÁRIO DE TELETRABALHO

Trabalho de Conclusão de Curso II apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientadora: Profa. Ma. Angélica da Silva Nunes

GOIÂNIA
2023

ISABELLA ALVES CARVALHO

UTILIZAÇÃO DA VPN NO CENÁRIO DE TELETRABALHO

Trabalho de Conclusão de Curso II apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação, em 12/12/2023.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orientadora: Profa. Ma. Angélica da Silva Nunes

_____

Prof. Me. Wilmar Oliveira de Queiroz

_____

Prof. Me. Rafael Leal Martins

GOIÂNIA
2023

RESUMO

Este estudo aborda de maneira abrangente o conceito e as características das *Virtual Private Networks*, Redes Privadas Virtuais (VPNs), destacando a importância de sua aplicação no contexto do teletrabalho. O trabalho explicita os fundamentos relacionados à segurança em redes de computadores, evidenciando os requisitos essenciais para estabelecer comunicações seguras e apresentando o funcionamento de algoritmos de criptografia. É destacado também, que as VPNs são amplamente adotadas devido à sua relação custo-benefício, sendo analisada sua operacionalidade no ambiente da *Internet*, com ênfase no protocolo de segurança *Internet Protocol Security*, Protocolo de Segurança da *Internet* (IPsec). O presente estudo mostra o funcionamento do IPsec, explorando sua estrutura e sua aplicabilidade no cenário de teletrabalho. Para complementar, são apresentados detalhes sobre a implementação da VPN, mostrando o ambiente de testes utilizado para simular o teletrabalho. O cenário de simulação envolve a configuração de um cliente e um servidor VPN em máquina virtual, incorporando serviços de *Domain Name System*, Sistema de Nomes de Domínio (DNS) e Active Directory para configuração da VPN no Windows Server.

Palavras-chave: VPN, IPsec, Segurança, Teletrabalho

ABSTRACT

This study comprehensively addresses the concept and characteristics of Virtual Private Networks (VPNs), highlighting the importance of their application in the context of teleworking. The work explains the fundamentals related to security in computer networks, highlighting the essential requirements for establishing secure communications and presenting the functioning of encryption algorithms. It is also highlighted that VPNs are widely adopted due to their cost-benefit ratio, and their operability in the internet environment is analyzed, with an emphasis on the Internet Security Protocol (IPsec). The present study shows how IPsec works, exploring its structure and its applicability in the teleworking scenario. To complement this, details are presented about the implementation of the VPN, showing the tests environment used to simulate teleworking. The simulation scenario involves configuring a client and a VPN server in a virtual machine, incorporating Domain Name System (DNS) and Active Directory services for VPN configuration on Windows Server.

Keywords: VPN, IPsec, Security, Teleworking

LISTA DE FIGURAS

LISTA DE SIGLAS

AD DS	Active Directory *Domain Services*, Serviços de Domínio do Active Directory
AES	*Advanced Encryption Standard*, Padrão de Criptografia Avançada
AH	*Authentication Header,* Cabeçalho de Autenticação
CA	*Certification Authority*, Autoridade Certificadora
DES	*Data Encryption Standard*, Padrão de Criptografia de Dados
DHCP	*Dynamic Host Configuration Protocol*, Protocolo de Configuração Dinâmica de Hosts
DNS	*Domain Name System*, Sistema de Nomes de Domínio
ESP	*Encapsulating Security Payload*, Encapsulamento de Segurança de Carga Útil
GB	Gigabyte
GHz	Gigahertz
GPO	*Group Policy Object*, Objeto de Política de Grupo
HMAC	*Hash-based Message Authentication Code*, Código de Autenticação de Mensagem Baseado em *Hash*
IBGE	Instituto Brasileiro de Geografia e Estatística
ICMPv4	*Internet Control Message Protocol version 4*, Protocolo de Mensagem de Controle da *Internet* versão 4
IKE	*Internet Key Exchange*, Troca de Chaves de *Internet*
IP	*Internet Protocol*, Protocolo de *Internet*
IPSec	*Internet Protocol Security*, Protocolo de Segurança da *Internet*
IPv4	*Internet Protocol version 4*, Protocolo da *Internet* versão 4
ISO	*International Organization for Standardization*, Organização Internacional de Padronização
MAC	*Message Authentication Code*, Código de Autenticação da Mensagem
MB	Megabyte
RAM	*Random Access Memory*, Memória de Acesso Aleatório
SA	*Security Association*, Associação de Segurança
SHA-1	*Secure Hash Algorithm* 1, Algoritmo de *Hash* Seguro 1
SPI	*Security Parameter Index*, Índice de Parâmetro de Segurança

SSL	*Secure Sockets Layer*, Camada Segura de Soquetes
TCP	*Transmission Control Protocol,* Protocolo de Controle de Transmissão
TLS	*Transport Layer Security*, Segurança na Camada de Transporte
VPN	*Virtual Private Network*, Rede Privada Virtual

SUMÁRIO

1 INTRODUÇÃO

As redes de computadores são sistemas interconectados que permitem a troca de informações. A *Internet* é uma dessas redes e, como mostrado na Figura 1, conecta diversos dispositivos, como computadores, servidores, *smartphones*, *tablets* e roteadores, proporcionando acesso imediato a informações de todo o mundo.

Figura 1: Sistemas interconectados através da *Internet*

Fonte: Viraliza mídia, 2023.

A velocidade de acesso às informações e a capacidade de troca de dados, aliadas à possibilidade de cada usuário possuir um computador pessoal, contribuem para o desenvolvimento de empresas, indústrias, ciência e educação.

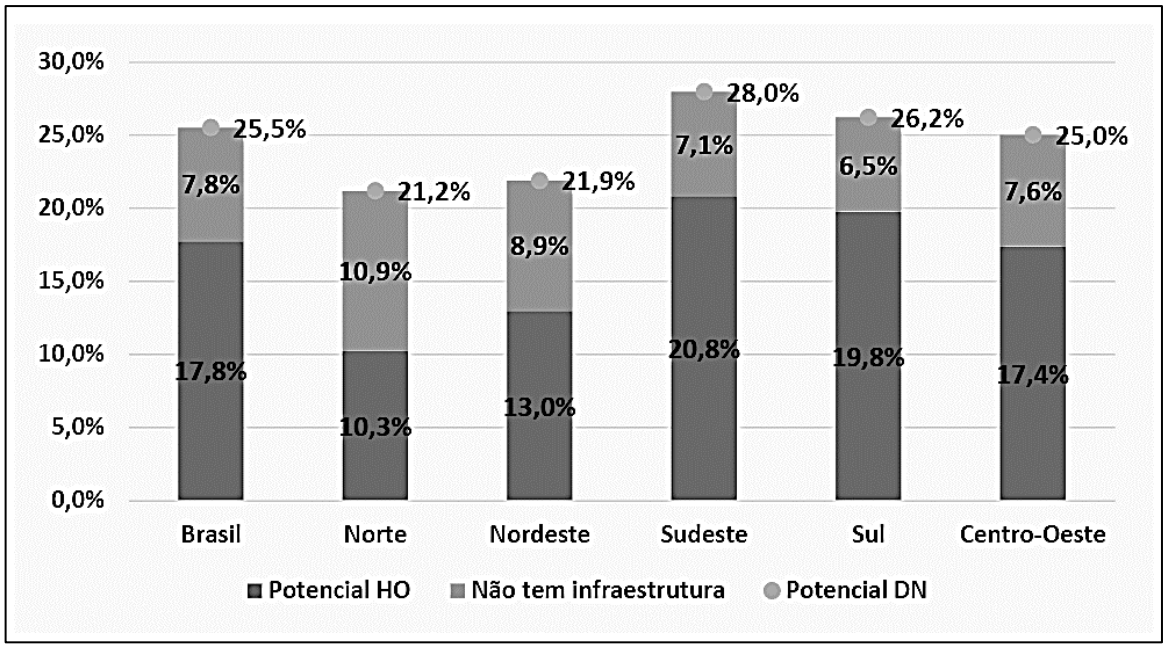
No trabalho, o uso da rede de computadores permitiu a comunicação e a colaboração entre empresas e colegas de trabalho de todo o mundo, além de automatizar tarefas repetitivas e proporcionar maior flexibilidade aos profissionais de várias áreas, permitindo o trabalho remoto.

No Brasil, o Tribunal Superior do Trabalho foi pioneiro em todo o Judiciário ao adotar o teletrabalho desde 2012. O trabalho a distância foi oficialmente inserido na legislação trabalhista brasileira em 2011 e, com a popularização e a adoção do

teletrabalho, houve uma reforma trabalhista em 2017 que regulamentou a forma de adesão e indicou os meios tecnológicos envolvidos no processo (TRIBUNAL SUPERIOR DO TRABALHO, 2020).

A Figura 2 mostra um gráfico com o percentual de pessoas em teletrabalho potencial no Brasil em 2019. A barra mais escura representa as pessoas que possuem uma infraestrutura mínima para o potencial de trabalho remoto, indicada pela legenda "Potencial HO". A barra mais clara representa as pessoas que possuem potencial de trabalho remoto sem a exigência de uma infraestrutura mínima. A soma total das duas barras é representada pelo potencial DN (FILHO et al., 2022).

Figura 2: Percentual de pessoas em teletrabalho



Fonte: Filho et. al., 2022.

De acordo com a pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) em 2020, mais de 7,9 milhões de pessoas trabalharam remotamente no Brasil devido à pandemia do coronavírus (TRIBUNAL SUPERIOR DO TRABALHO, 2020).

Porém, a troca de informações na rede requer uma comunicação segura, uma vez que a *Internet* é pública e muitas mensagens são transmitidas em texto claro. Isso pode possibilitar vários ataques aos sistemas, resultando em roubo de dados, fraudes, falsificação de identidade dos usuários, dentre outros problemas.

Por anos, a comunicação segura entre empresas exigiu alto investimento para interligar suas redes por meio de uma conexão direta. Com o objetivo de reduzir custos e conectar empresas e trabalhadores ao redor do mundo de forma segura, surgiu a abordagem de rede privada dentro da rede pública, chamada *Virtual Private Network*, Rede Privada Virtual (VPN).

A VPN utiliza criptografia e autenticação para fornecer segurança da comunicação. Dessa forma, os trabalhadores a distância podem ter acesso completo aos dados da empresa.

É relevante estudar este tema porque o teletrabalho tem sido adotado por muitas organizações, e a principal rede de computadores utilizada para troca de dados é a *Internet* pública. Isso gera preocupações nos clientes e nas empresas, ao saberem que existem vulnerabilidades e ameaças que podem comprometer seus dados na rede. No entanto, as VPNs podem manter a segurança da rede que conecta a empresa aos profissionais de trabalho, o que torna o conhecimento sobre seu funcionamento importante.

Diante deste contexto, este projeto visa responder a seguinte questão de pesquisa: **Como manter uma comunicação segura entre o usuário e a empresa, utilizando a VPN no teletrabalho?**

1.1 Objetivo geral

Apresentar como a VPN pode manter uma comunicação segura em teletrabalho.

1.2 Objetivos específicos

- Explorar os estudos feitos sobre segurança de redes e VPN;
- Analisar como a VPN pode oferecer segurança na comunicação no trabalho remoto;
- Identificar as melhores abordagens na implementação de uma solução VPN para teletrabalho;
- Implementar um cenário de testes da VPN no Windows Server;
- Simular o cenário de teletrabalho em um ambiente de testes.

1.3 Metodologia

Esta pesquisa, segundo sua natureza é um resumo de assunto que busca estruturar a área de conhecimento abordada no projeto, mostrando sua progressão histórica e seu estado atual de desenvolvimento (WAZLAWICK, 2014).

Segundo os objetivos é uma pesquisa descritiva buscando obter informações mais precisas sobre determinado assunto, sem interferência do pesquisador ou a tentativa de elaboração de teorias que expliquem os fenômenos, mas sim descrevendo os fatos como eles são (WAZLAWICK, 2014).

E segundo seus procedimentos técnicos é uma pesquisa bibliográfica e experimental. A pesquisa bibliográfica envolve o estudo de artigos, teses, livros e outros. A pesquisa experimental envolve manipulação de uma ou mais variáveis para chegar a uma conclusão (WAZLAWICK, 2014).

Segundo Gil (2017) a pesquisa experimental deve seguir as seguintes etapas:

a) Formulação do problema: Como manter uma comunicação segura entre o usuário e a empresa, utilizando a VPN no teletrabalho?
b) Construção das hipóteses: é descrito como utilizar a VPN para manter uma comunicação segura no trabalho remoto;
c) Definição do plano experimental: são descritas as principais características da VPN e, em seguida, é simulado uma comunicação segura;
d) Determinação do ambiente: a rede VPN é implementada entre uma máquina virtual e uma máquina física para simular e testar o desempenho e a segurança na comunicação;
e) Coleta de dados: são realizadas pesquisas em livros e artigos para descrever a segurança de rede utilizando VPN, e mostrar sua importância no teletrabalho;
f) Análise e interpretação dos dados: realizada a coleta dos dados obtidos na experiência com o propósito de aprimorar a compreensão do tema;
g) Redação do relatório: o trabalho é registrado em forma de monografia.

1.4 Estrutura da monografia

O capítulo 2 descreve o que é necessário para manter uma comunicação segura na rede, utilizando técnicas como criptografia e autenticação de mensagem.

No capítulo 3 é definido a VPN, detalhando seu funcionamento com relação aos modos e protocolos utilizados.

No capítulo 4 é mostrado a implementação da VPN, assim como outros serviços que devem ser instalados juntos a VPN e a configuração do IPsec.

No capítulo 5 são mostrados os testes feitos após a instalação da VPN, para se conectar ao servidor, e também os resultados obtidos.

No capítulo 6 são feitas as considerações finais, ressaltando a importância do uso da VPN no cenário de teletrabalho e oferecndo sugestões de trabalhos futuros.

2 CONCEITOS DE SEGURANÇA EM REDES DE COMPUTADORES

A *Internet* é uma realidade na sociedade contemporânea e faz parte do dia-a-dia das pessoas. Contudo, muitas mensagens são transmitidas em texto claro. Assim, um intruso pode ter acesso e monitorar a comunicação, executando ações de roubar, inserir, modificar ou eliminar informações ou conteúdo das mensagens. Além disso, o intruso pode sobrecarregar a rede. Para certificar que a rede forneça uma comunicação segura, é desejável que se tenha confidencialidade, integridade da mensagem e autenticação do ponto final (KUROSE, 2013).

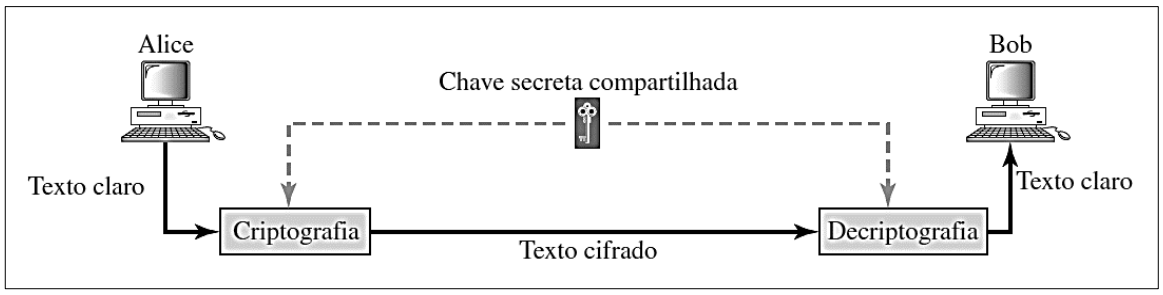
2.1 Confidencialidade

A confidencialidade assegura que, ao enviar uma mensagem, somente o remetente e o destinatário tenham conhecimento do seu conteúdo. Mesmo que a mensagem seja interceptada por intrusos, estes não devem ser capazes de compreendê-la, já que ela deve estar criptografada (KUROSE, 2013).

As técnicas criptográficas são padronizadas, publicadas e disponíveis para conhecimento público, por isso, não são suficientes para manter a segurança da mensagem. Portanto, o remetente usa uma chave para criptografar a mensagem a ser enviada, e somente o destinatário, que também possui a chave, está habilitado para decifrar a mensagem (KUROSE, 2013).

A criptografia de chaves simétricas envolve chaves secretas e idênticas que são usadas pelo remetente e pelo destinatário. Assim como mostra a Figura 3, sendo Alice o remetente e Bob o destinatário. Uma das técnicas usadas para a criptografia simétricas é a cifra de blocos (KUROSE, 2013).

Figura 3: Criptografia de chave simétrica



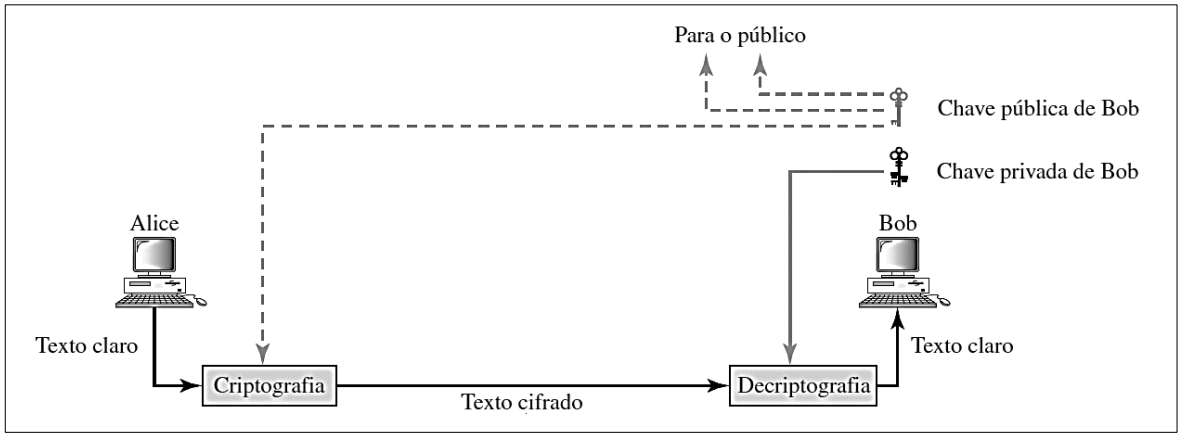
Fonte: Forouzan, 2010.

Alguns exemplos de cifras de blocos são o *Data Encryption Standard*, Padrão de Criptografia de Dados (DES) e o *Advanced Encryption Standard*, Padrão de Criptografia Avançada (AES), que criptografam o texto claro dividindo-o em blocos (FOROUZAN, 2010).

A criptografia de chave assimétrica, também conhecida como criptografia de chave pública, é composta por duas chaves, sendo uma privada, que apenas o proprietário da chave tem o conhecimento, e outra pública, que pode ser conhecida por qualquer um (KUROSE, 2013).

A Figura 4 mostra a criptografia de chave pública, composta por uma estrutura que inclui o texto claro, que é a mensagem original, um algoritmo de cifração usado pelo remetente da mensagem para cifrar o texto claro com a chave pública, o texto cifrado, uma mensagem embaralhada e ilegível, que é enviado ao destinatário, e um algoritmo de decifração utilizado pelo destinatário para decifrar a mensagem criptografada, aplicando a chave privada (STALLINGS, 2014).

Figura 4: Criptografia de chave pública ou assimétrica



Fonte: Forouzan, 2010.

Um algoritmo utilizado na criptografia de chaves assimétricas é o RSA. Nesse algoritmo, o proprietário das chaves, pública e privada, deve escolher dois números primos grandes, *p* e *q*, pois quanto maior os números escolhidos, mais difícil é para quebrar a criptografia. Esses números passam por cálculos, formando um par de números que compõem a chave pública e um par de números que compõem a chave privada (KUROSE, 2013).

2.2 Integridade da mensagem

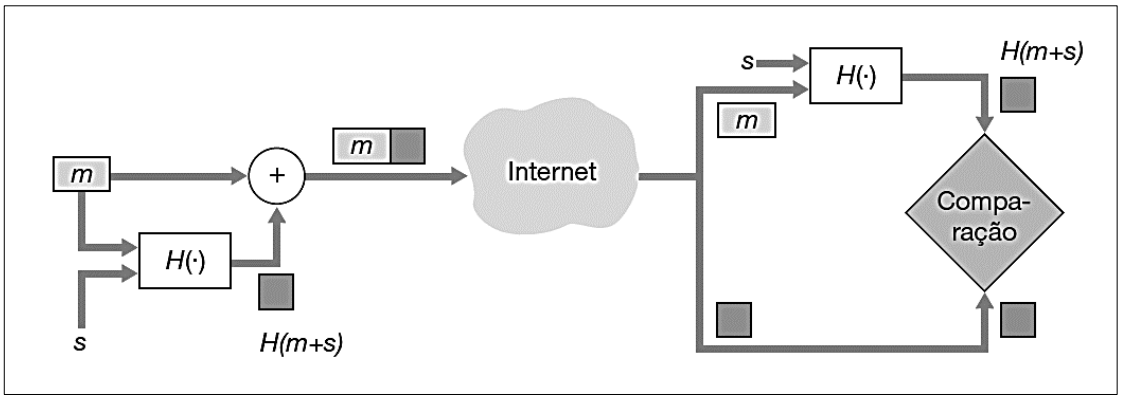
A integridade ou autenticação da mensagem consiste em certificar que o envio de uma mensagem foi realmente feito pelo remetente original e que não teve seu conteúdo alterado no caminho para o destinatário. Para assegurar a integridade é usado um algoritmo de criptografia, a função *hash* (KUROSE, 2013).

A função *hash* recebe como entrada uma mensagem *m,* e calcula um resumo criptográfico *H(m)*, prevenindo que a mensagem original não seja substituída e nem tenha o mesmo valor *hash* de outra (STALLINGS, 2014).

Um algoritmo utilizado na função *hash* é o *Secure Hash Algorithm* 1, Algoritmo de *Hash* Seguro 1 (SHA-1) que atua com os dados de entrada divididos em blocos de 512 *bits* de comprimento gerando um resumo de mensagem de 160 *bits* (FOROUZAN, 2010).

A função *hash* provê que a mensagem não seja modificada no caminho, mas para confirmar que esta foi enviada pelo remetente original, é necessária a chave de autenticação. A Figura 5 mostra como a função *hash*, juntamente com a chave de autenticação, autenticam a mensagem. O remetente envia a mensagem *m*, que é concatenada com a chave secreta *s,* e em seguida, é calculada o *hash* da junção *H(m+s)* denominada *Message Authentication Code*, Código de Autenticação da Mensagem (MAC). O MAC é anexado a mensagem original e o conjunto é enviado para o destinatário, que, ao receber, gera uma nova função *hash*, usando a chave de seu conhecimento, *s*, e compara com o MAC recebido. Ao verificar que os MACs são iguais, tem-se a confirmação que a mensagem não teve seu conteúdo alterado e pertence ao remetente original (KUROSE, 2013).

Figura 5: Processo de autenticação de mensagem



Fonte: Kurose, 2013.

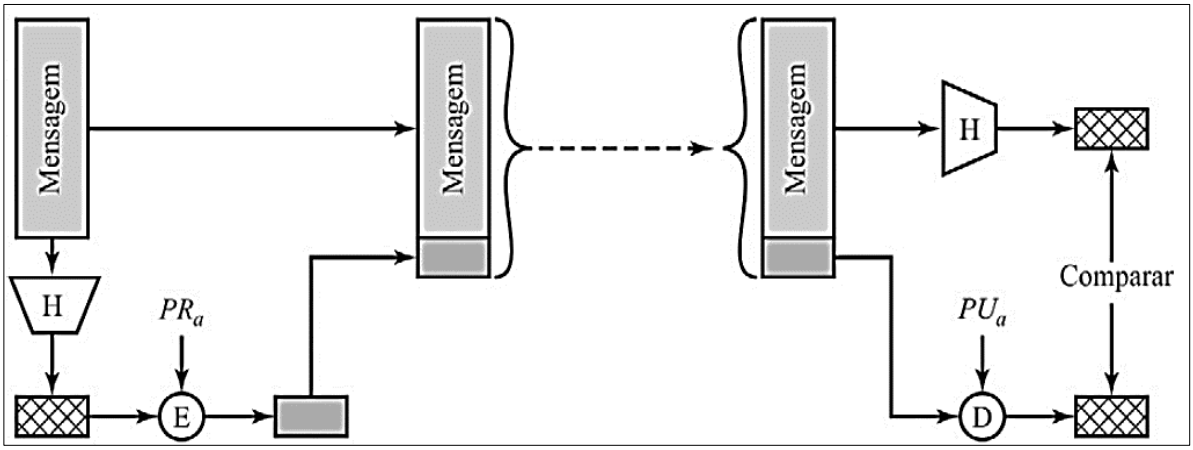
O algoritmo SHA-1 não foi projetado para usar a função *hash* com o MAC. Diante disso uma nova abordagem foi criada, o *Hash-based Message Authentication Code*, Código de Autenticação de Mensagem Baseado em *Hash* (HMAC) que pode ser usado com algoritmos como o SHA-1 (STALLINGS, 2014).

O MAC faz uso de chaves simétricas para prover integridade e autenticação, porém a assinatura digital utiliza um par de chaves assimétricas para atingir os mesmos objetivos (FOROUZAN, 2010).

A assinatura digital é a técnica criptográfica que indica o dono, o criador ou alguém que concorda com o conteúdo de um documento. Ela deve ser verificável e não falsificável (KUROSE, 2013).

A Figura 6 mostra como ocorre a geração da assinatura digital. O remetente deve gerar um *hash* da mensagem que é enviada e cifrar esse *hash* com sua chave privada. O destinatário, ao receber a mensagem assinada, também calcula o *hash* da mensagem e faz a decifração usando a chave pública do remetente. Dessa forma, ele compara o valor que obteve com o valor de *hash* da mensagem que recebeu. Se ambos os valores forem idênticos, o destinatário tem a certeza de que a mensagem é do remetente original (STALLINGS, 2014).

Figura 6: Assinatura Digital



Fonte: Stallings, 2014.

Mesmo com a assinatura digital, qualquer intruso pode se passar por outra pessoa e enviar uma mensagem para o destinatário. Para que isso não ocorra, foi criada uma organização para certificar as chaves públicas, chamada de *Certification Authority*, Autoridade Certificadora (CA). O proprietário da chave pública pode solicitar à CA uma certificação para poder se comunicar com segurança. As principais funções

da CA são autenticar a identidade do remetente e criar um certificado vinculando a chave pública ao remetente (FOROUZAN, 2010).

2.3 Autenticação do ponto final

A autenticação do ponto final consiste em verificar a identidade de uma entidade para outra em tempo real. Existem três tipos de autenticação, eles consistem em algo que o indivíduo conhece, possui e/ou é (FOROUZAN, 2010).

O método mais conhecido é o de senhas, algo que o usuário conhece. Porém, as senhas fixas podem apresentar vulnerabilidades por serem utilizadas repetidamente para acessar sistemas. Isso torna o método suscetível a ataques de intrusos, que podem interceptar a mensagem na rede e capturar a senha, tentar entrar no sistema fazendo várias combinações dos caracteres ou invadir o sistema e acessar o local de armazenamento de senhas. Uma solução para armazenar a senha de forma segura é guardar o *hash* da senha em vez do seu formato em texto claro, impedindo que um invasor consiga descobrir a senha (FOROUZAN, 2010).

Outro método é baseado em algo que o usuário possui, os *tokens*. Por exemplo, cartões de memória, frequentemente utilizados em acessos físicos a quartos de hotéis, podem ser combinados com senhas, o que proporciona maior segurança para o usuário. No entanto, esse tipo de *token* possui alto custo e pode ser roubado ou falsificado por adversários (STALLINGS, 2014).

O último método está relacionado às características físicas do usuário. A biometria pode autenticar o usuário por meio de suas características faciais, impressões digitais, estrutura da íris, voz e outros (STALLINGS, 2014).

3 REDE PRIVADA VIRTUAL

As organizações que operam em várias regiões geográficas, buscam ter suas próprias redes de sigilo e segurança durante a troca de dados e podem optar por redes físicas privadas. Mas, esse tipo de rede possui um alto custo para adquirir, instalar e manter. Por isso, em vez de escolher a rede privada, muitas instituições utilizam a VPN que usa a *Internet* pública como meio de tráfego de dados (KUROSE, 2013).

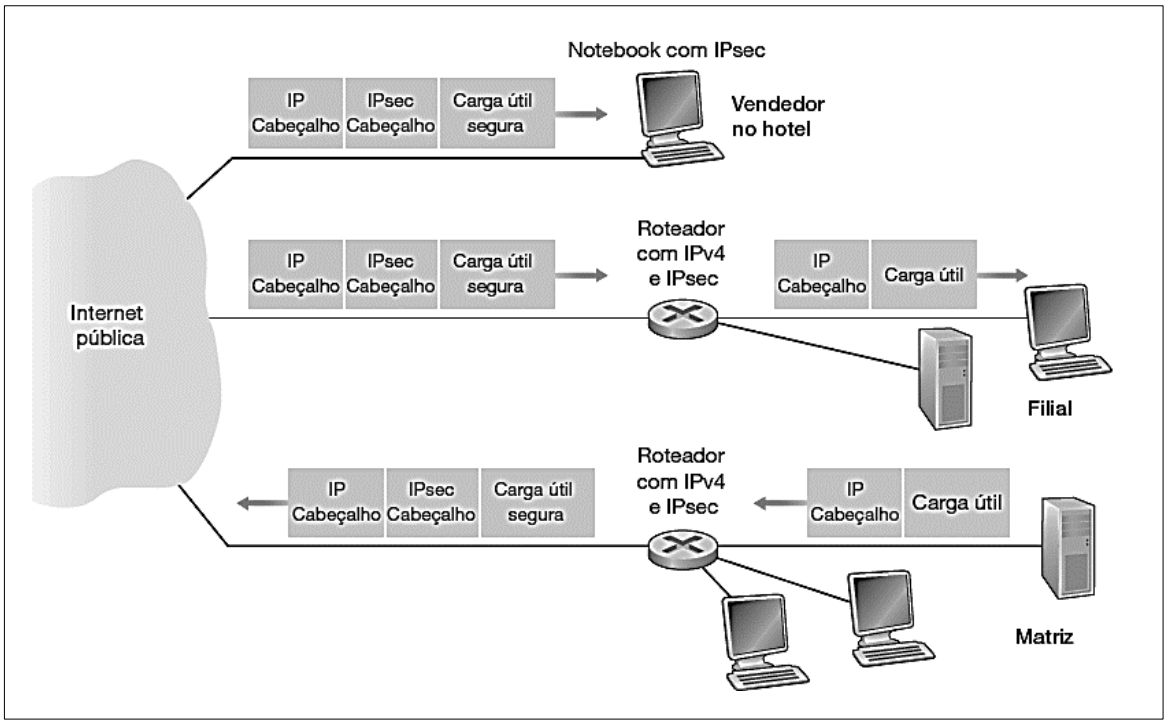
3.1 Introdução

Para fornecer segurança de rede na VPN é possível implementar medidas de autenticação e criptografia na transmissão de pacotes *Internet Protocol*, Protocolo da *Internet* (IP). Essas medidas de segurança requerem a conversão do datagrama em *Internet Protocol Security*, Protocolo de Segurança da *Internet* (IPsec) (STALLINGS, 2014).

Como mostrado na Figura 7, se a comunicação ocorre apenas dentro de uma empresa, não é necessário converter o datagrama em IPsec. Porém, a partir do momento em que o pacote sai da rede local e vai para a *Internet* pública, o datagrama *Internet Protocol version 4*, Protocolo da *Internet* versão 4 (IPv4) é convertido em IPsec. Quando a comunicação é feita entre empresas, utiliza-se o modo túnel, no qual a VPN é estabelecida entre os roteadores e o IPsec protege o pacote inteiro. Ainda na Figura 7, é mostrado uma comunicação entre a empresa e o vendedor no hotel, que utiliza um *notebook*. Neste caso, é utilizado o modo túnel do lado da matriz, a partir do roteador, e o modo transporte no notebook, que utiliza a proteção apenas na carga útil do datagrama, estabelecendo uma VPN híbrida (FOROUZAN, 2013).

O IPsec pode ser utilizado por empresas para fornecer a segurança na troca de dados entre matriz e filiais, bem como para acesso remoto seguro pela *Internet*. Com o IPsec, o usuário com um sistema equipado com protocolos de segurança pode ter acesso seguro à rede da empresa, promovendo acessibilidade e facilidade para pessoas que trabalham em casa ou viajando. Além disso, o IPsec também pode melhorar a segurança no comércio eletrônico, pois ele é capaz de cifrar e/ou autenticar todo o tráfego no nível do IP (STALLINGS, 2014).

Figura 7: Uso do IPsec em uma Rede Privada Virtual



Fonte: Kurose, 2013.

Os serviços do IPsec são utilizados quando o datagrama IP é enviado pela *Internet* pública. Por outro lado, se o envio de datagramas IP for realizado dentro da própria empresa, são utilizados apenas os datagramas, sem o IPsec (KUROSE, 2013).

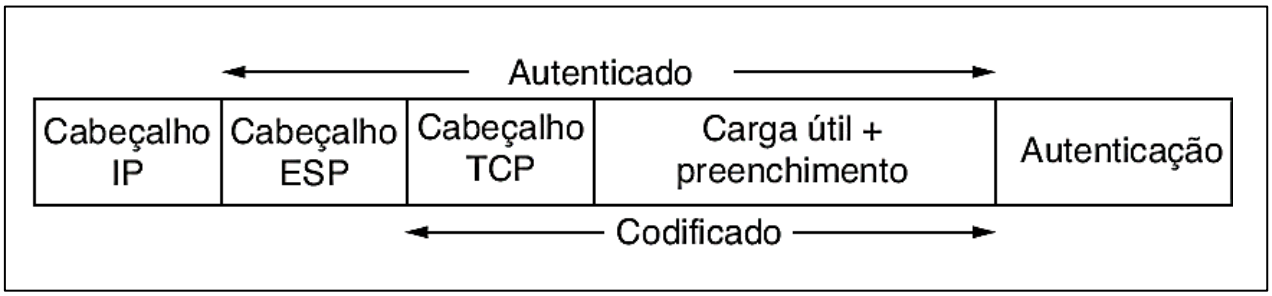
3.2 Protocolos usados na VPN

O IPSec é um conjunto de protocolos que provê a segurança de datagramas e possui dois protocolos, o *Authentication Header,* Cabeçalho de Autenticação (AH) e o *Encapsulating Security Payload*, Encapsulamento de Segurança de Carga Útil (ESP). Ambos proveem a autenticação da origem e a integridade dos dados, além de suportarem dois modos de uso: o modo de transporte e o modo túnel. Porém, o ESP é o mais utilizado por prover o essencial nas VPNs, que é o sigilo, ao contrário do AH, que não oferece sigilo (KUROSE, 2013).

No modo de transporte, o protocolo ESP tem seu cabeçalho inserido após o cabeçalho IP, criptografando os dados da carga útil e o cabeçalho *Transmission Control Protocol,* Protocolo de Controle de Transmissão (TCP). Também é feita a autenticação, mas, nesse modo, o cabeçalho IP não é protegido. Dessa forma,

assegura a privacidade e a segurança dos dados transmitidos entre duas estações finais. O ESP no modo transporte é mostrado na Figura 8 (FOROUZAN, 2010).

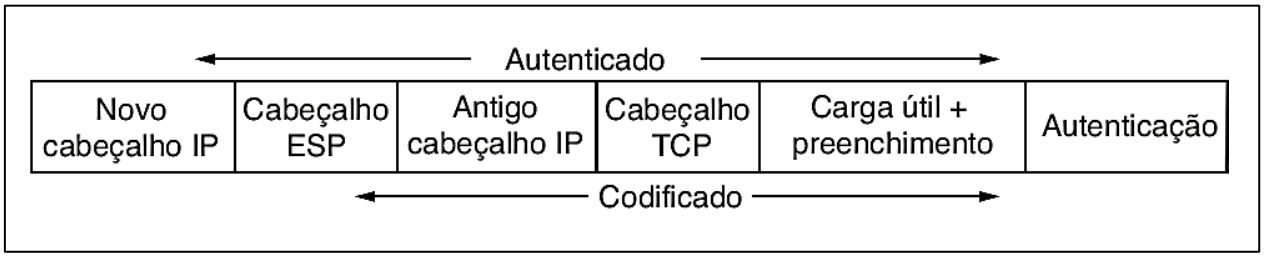
Figura 8: Protocolo ESP no modo transporte



Fonte: Tanenbaum, 2011.

No modo de túnel a proteção é feita para todo o pacote IP, encapsulando-o com novos cabeçalhos externos que ocultam o cabeçalho original. Dessa forma nenhum roteador examina o cabeçalho interno e o pacote original é enviado através de um túnel de um ponto de rede para outro de forma mais segura. Na Figura 9 é mostrado o protocolo ESP no modo túnel, no qual todo o pacote IP é protegido, acrescentando um novo cabeçalho IP (STALLINGS, 2014).

Figura 9: Protocolo ESP no modo túnel



Fonte: Tanenbaum, 2011.

3.3 Associação de segurança

Para enviar os datagramas IPsec é preciso estabelecer a conexão lógica simples na camada de rede, chamada *Security Association*, Associação de Segurança (SA). Essa conexão é feita antes do envio de datagramas e é unidirecional do remetente ao destinatário. Portanto, para haver troca de dados é necessário estabelecer duas conexões lógicas, uma em cada direção (KUROSE, 2013).

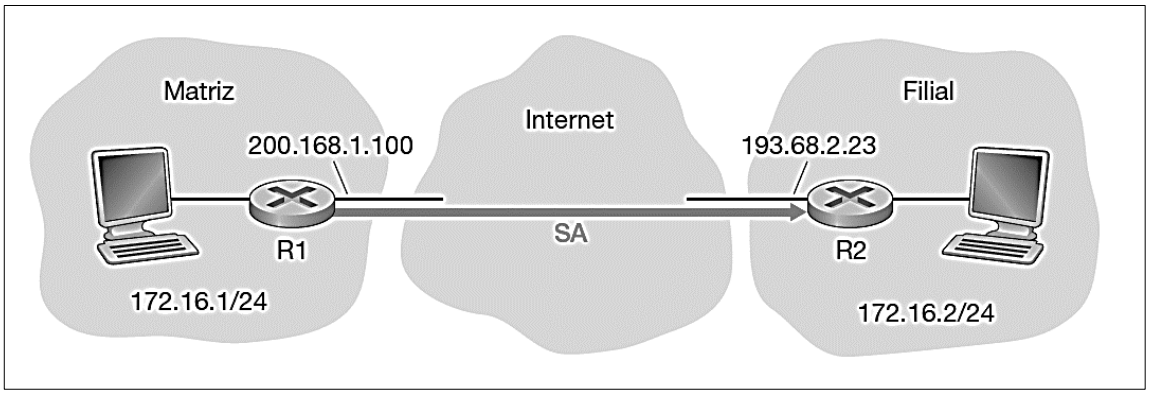
As SAs possuem um conjunto de parâmetros de segurança, para o envio do IPsec, que:

> […] pode ser estabelecido entre um emissor e determinado receptor na primeira vez que o emissor tiver um datagrama a ser enviado para esse receptor em particular. O conjunto pode ser salvo para transmissão futura de pacotes IP para o mesmo receptor (Forouzan, 2010, p. 1002).

Esses parâmetros incluem o *Security Parameter Index*, Índice de Parâmetro de Segurança (SPI), que identifica a SA, o endereço de IP de destino, que indica o sistema final, e o identificador de protocolo, que mostra se é um protocolo AH ou ESP. Todas as informações das SAs são armazenadas no banco de dados, gerado pelo IPsec (STALLINGS, 2014).

Na Figura 10, é mostrado um exemplo da VPN estabelecida entre o roteador R1 e o roteador R2 que possui a SA do R1 para o R2. Nesse caso, quando o datagrama IPsec é enviado, é necessário acessar os parâmetros da SA no banco de dados do roteador R1, para a criação do IPsec. Da mesma forma o roteador R2 acessa as informações necessárias para autenticar e decodificar o IPsec (KUROSE, 2013).

Figura 10: Associação de Segurança (SA)



Fonte: Kurose, 2013.

Quando a rede VPN é pequena essas informações podem ser incluídas manualmente pelo administrador de rede, porém se a rede for grande é necessário um mecanismo automático para a criação de SAs, utilizando o *Internet Key Exchange*, Troca de Chaves na *Internet* (IKE). (KUROSE, 2013).

O IKE é um protocolo utilizado pelo IPsec para criar chaves de sessão seguras nas SAs. Ele utiliza duas fases para estabelecer as chaves de sessão e negociar os

algoritmos de criptografia e autenticação. A primeira fase é utilizada para criar um canal seguro entre os roteadores e a segunda fase é usada para estabelecer as SAs em ambas as direções. O protocolo IKE usa certificados para autenticar as entidades IPsec e trocar informações de chave com segurança (KUROSE, 2013).

3.4 Opções de implementação da VPN

É utilizado a implementação da VPN IPsec nessa pesquisa, porém existe outro tipo de implementação, a OpenVPN. A tecnologia VPN IPsec é implementada através das configurações embutidas nos sistemas operacionais e possui suporte nativo no Windows. Entretanto, a tecnologia OpenVPN necessita da instalação de um software na máquina do cliente e no servidor, para realizar as configurações da VPN e possui pacotes nativos no Linux (FEILNER, 2006).

A OpenVPN opera na camada de aplicação enquanto a VPN IPsec opera na camada de rede. Apesar das abordagens diferentes, ambas as tecnologias proveêm a segurança necessária para a comunicação entre cliente e servidor VPN. Porém a OpenVPN utiliza o protocolo *Secure Sockets Layer*, Camada Segura de Soquetes (SSL) ou *Transport Layer Security*, Segurança na Camada de Transporte (TLS) para fornecer autenticação, confidencialidade e integridade dos dados transmitidos pela *Internet* (FEILNER, 2006).

Nesse trabalho optou-se pela utilização da VPN IPsec por oferecer melhor desempenho, quando implementado em hardware, em comparação com a OpenVPN, e o sistema operacional Windows Server por ser mais utilizado em ambientes corporativos.

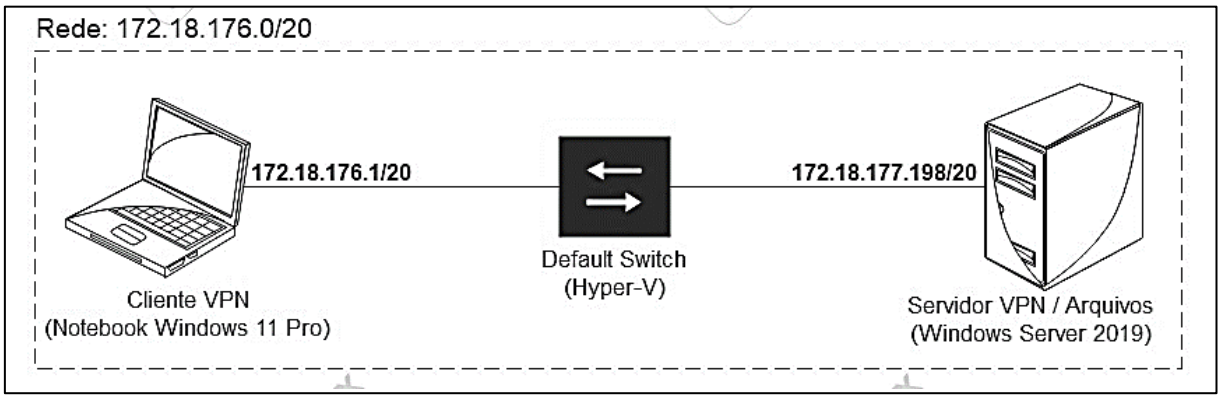
4 IMPLEMENTAÇÃO DA VPN

Neste capítulo, são detalhados os elementos utilizados no ambiente de testes para a realização deste trabalho, simulando o cenário de teletrabalho, compreendendo um cliente VPN e um servidor VPN. É apresentada a descrição do processo de instalação do servidor VPN na máquina virtual e as ferramentas utilizadas no servidor, abrangendo todas as configurações efetuadas com o intuito de configurar o acesso dos usuários e estabelecer a conexão remota possibilitando ao usuário acessar as informações necessárias da empresa, de forma segura, independente de sua localização.

4.1 Ambiente de testes

Para a configuração do ambiente de testes, foi utilizado um dispositivo de computação portátil (*notebook*) que virtualizou uma máquina com o sistema operacional Windows Server 2019 Datacenter, destinada a atuar como servidor VPN. Essa mesma máquina foi designada para desempenhar a função de cliente VPN, estabelecendo conexão com o servidor. A representação da infraestrutura gerada, é mostrada na Figura 11.

Figura 11: Topologia da Rede



Fonte: Elaborada pela autora desse trabalho.

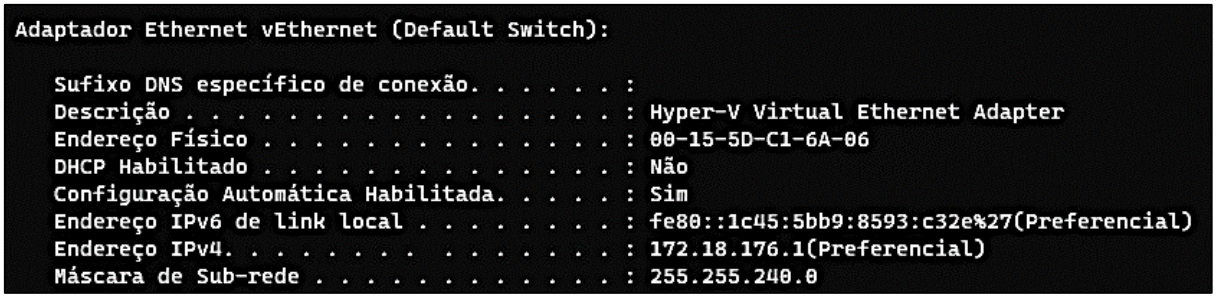
A rede 172.18.176.0/20 foi criada por meio da aplicação do Hyper-V, um recurso do sistema operacional Windows que possibilita a virtualização de máquinas.

Essa rede hospeda: o cliente VPN, que opera por meio do *Notebook* Windows 11 Pro, com o endereço IP 172.18.176.1/20; o Servidor VPN, desempenhando

simultaneamente o papel de servidor de compartilhamento de arquivos, utiliza o sistema operacional Windows Server 2019 Datacenter e possui o endereço IP 172.18.177.198/20; e o Hyper-V, que instaura o Default Switch, viabilizando a comunicação de informações entre o cliente e o servidor.

Os endereços IP, tanto do cliente VPN quanto do servidor VPN, podem ser verificados por meio do *prompt* de comando de cada máquina. Ao executar o comando *ipconfig*, os dados pertinentes, como o endereço IPv4 e a máscara de sub-rede, são exibidos, como mostrado na Figura 12 a saída desse comando no Cliente VPN.

Figura 12: Endereço IP do cliente VPN



Fonte: Imagem capturada pela autora desse trabalho em MICROSOFT, 2023c.

No contexto externo ao ambiente de teste, em substituição ao dispositivo roteador, faz-se uso do *Default Switch* com o propósito de estabelecer a conexão de rede externa, viabilizando a simultânea conexão de diversos clientes VPNs ao servidor.

A configuração para a VPN de acesso remoto utiliza o modo túnel do lado do servidor VPN, e o modo transporte do lado do cliente VPN, que faz o uso do *notebook*, assim como abordado no capítulo 3, seção 3.1.

4.2 Instalação e configuração do Hiper-V e Máquina Virtual

O Hyper-V é um recurso oferecido pelo Windows, que suporta vários sistemas operacionais diferentes, para criação de máquinas virtuais (MICROSOFT, 2023a).

Para determinar a compatibilidade da máquina com o Hyper-V, executa-se o comando *systeminfo* na janela do *prompt* de comando. Nessa janela, são exibidos os requisitos do Hyper-V, se todos estiverem marcados como "Sim", o sistema atende aos requisitos para a utilização do Hyper-V, como mostrado na Figura 13. No entanto,

caso algum requisito não esteja de acordo, é necessário efetuar as devidas modificações no sistema para habilitar esse recurso (MICROSOFT, 2023a).

Figura 13: Requisitos do Hyper-V

Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

O Hyper-V pode ser habilitado por meio da *interface* de ativação de recursos do Windows, acessível na seção "Programas e Recursos" no Painel de Controle da máquina. Informações detalhadas sobre esse processo podem ser consultadas no Apêndice I. Após a ativação desse recurso, a *interface* do gerenciador do Hyper-V é disponibilizada, permitindo a criação de máquinas virtuais.

A máquina virtual requer os requisitos mínimos: processador de 1,4 Gigahertz (GHz) de 64 *bits*, 512 Megabytes (MB) de *Random Access Memory*, Memória de Acesso Aleatório (RAM) e disco rígido com pelo menos 32 Gigabytes (GB). Esses requisitos podem ser consultados no menu Iniciar do Windows, pesquisando “Exibir nome do computador” na máquina (BATTISTI, 2022).

A máquina utilizada nesse trabalho possui um processador de 2,10 GHz de 64 *bits*, 12 GB de memória RAM, como mostrado na Figura 14. Além disso conta com um disco rígido de 446 GB e executa o sistema operacional da Microsoft edição Windows 11 Pro (MICROSOFT, 2023c).

Figura 14: Verificando processador e memória RAM

Nome do dispositivo	Isabella-Alves	
Processador	AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx	2.10 GHz
RAM instalada	12,0 GB (utilizável: 9,88 GB)	

Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

No Gerenciador do Hyper-V, ocorre o processo de criação da máquina virtual, definindo o nome da máquina virtual, a alocação de memória para otimização do desempenho do sistema operacional, a seleção da rede à qual a máquina virtual é conectada, a alocação de memória para a inclusão de um disco rígido virtual e, por fim, a instalação do sistema operacional desejado (BATTISTI, 2022).

As configurações relacionadas à memória e ao disco rígido durante a criação da máquina virtual são inicialmente estabelecidas com valores padrões, os quais são automaticamente definidos pela própria máquina virtual. Neste trabalho, foram utilizados os valores padrões estabelecidos, entretanto, é possível modificar essas configurações de acordo com as preferências e requisitos do usuário.

A instalação do sistema opercaional Windows Server 2019 foi realizada através da utilização do arquivo da *International Organization for Standardization*, Organização Internacional de Padronização (ISO) disponibilizado oficialmente no portal da Microsoft. Este procedimento permite uma avaliação gratuita com duração de 180 dias (MICROSOFT, 2023b).

Na Figura 15 é mostrado o nome e as configurações de processador, memória RAM e sistema operacional instalados na máquina virtual.

Figura 15: Configurações atribuídas para a Máquina Virtual

Nome do dispositivo	WIN-3SCT3F98GK3
Processador	AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx 2.10 GHz
RAM instalada	3,00 GB

Edição	Windows Server 2019 Datacenter Evaluation
Versão	1809
Instalado em	26/08/2023
Compilação do SO	17763.4737

Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

4.3 Configuração do Active Directory

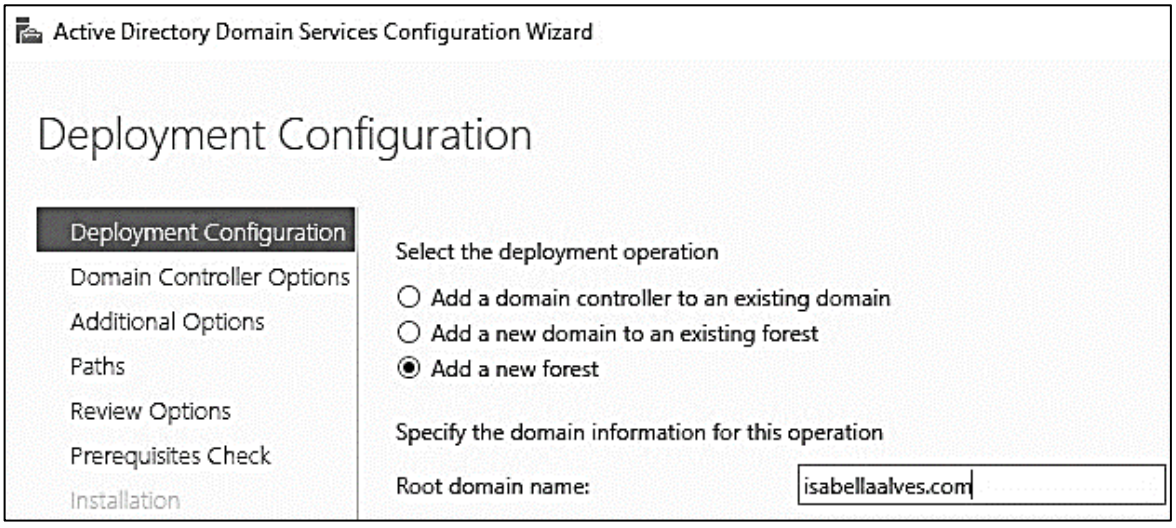
Após a conclusão da instalação do sistema operacional Windows Server 2019 Datacenter, foram implementadas as configurações remotas, acessíveis por meio das propriedades do sistema, para viabilizar o acesso remoto à máquina virtual.

Um servidor foi instalado automaticamente, sendo necessário realizar configurações para que se torne um servidor VPN. Adicionalmente, foram feitas a instalação do *Active Directory Domain Services*, Serviços de Domínio do Active Directory (AD DS) e do *Domain Name System*, Sistema de Nome de Domínios (DNS) (BATTISTI, 2022).

O AD DS desempenha a função de um controlador de domínio, com o objetivo de fornecer métodos de autenticação e autorização para que os usuários acessem o servidor, além de armazenar informações sobre usuários, computadores e outros dispositivos da rede, disponibilizando essas informações gerenciamento aos administradores de rede (MCDONALD et al., 2022).

Ao final da instalação do AD DS é necessário promover o servidor a um controlador de domínio, adicionando uma nova floresta e registrando a raiz. Os detalhes dessa instalação podem ser verificados no Apêndice II. Neste ambiente de testes foi inserido como nome de domínio “isabellaalves.com”, como mostrado na Figura 16 (MCDONALD et al., 2022).

Figura 16: Configuração do nome de domínio



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

Por meio das identificações dos usuários que permitem o acesso ao servidor, pode-se fazer a utilização do *Group Policy Object*, Objeto de Política de Grupo (GPO), com a finalidade de alocar usuários em grupos e determinar os privilégios de compartilhamento a eles concedidos (MCDONALD et al., 2022).

4.4 Configuração do Servidor VPN

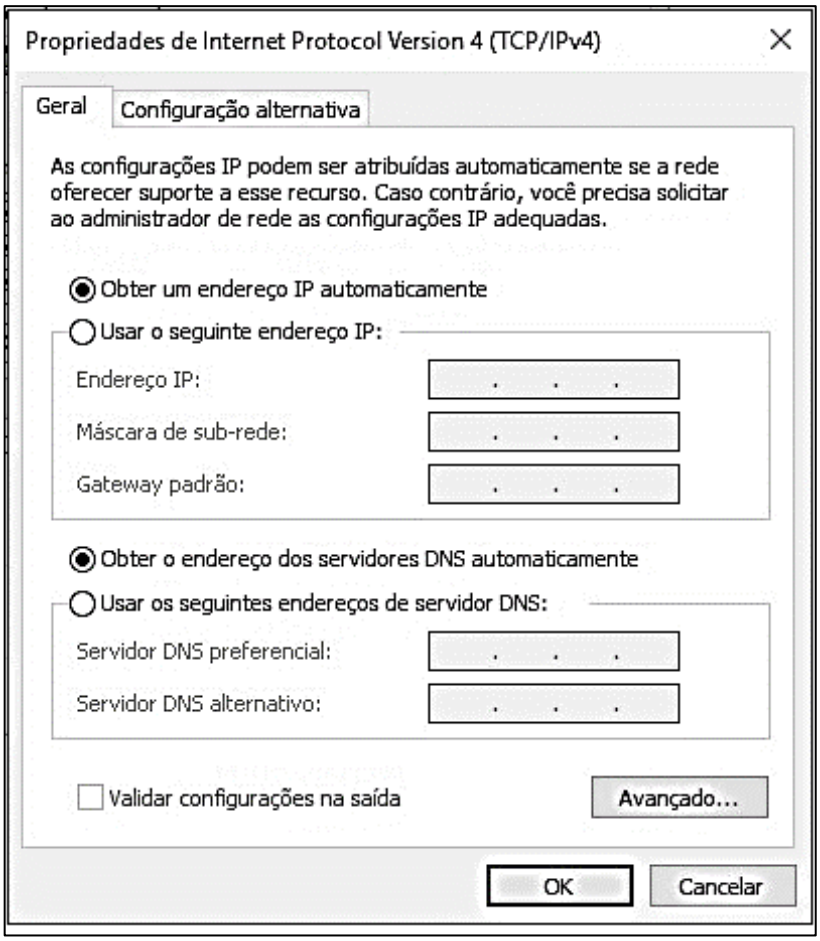
A implementação da VPN no servidor foi realizada por meio da funcionalidade do acesso remoto, que viabiliza a conectividade por meio da VPN, possibilitando que os usuários estabeleçam conexões remotas com redes corporativas. A VPN utiliza a infraestrutura da *Internet*, empregando uma combinação de técnicas de

encapsulamento e criptografia de dados para facilitar a comunicação segura com os usuários remotos, conforme abordado no capítulo 3, seção 3.2 (MICROSOFT, 2019).

Junto à implementação da VPN, procedeu-se à instalação da função de roteamento, para prover suporte aos dispositivos roteadores. Após a instalação, foi executado o assistente do guia de introdução, realizando as configurações de clientes remotos de acordo com todos os computadores alocados nos grupos de segurança no computador de domínio (MICROSOFT, 2019).

No contexto da instalação da VPN, destaca-se a necessidade de selecionar os tipos de atribuição de IP para clientes remotos. Neste trabalho, foi escolhido a atribuição automática, como mostrado na Figura 17, resultando na alocação de endereços aos clientes VPN diretamente do servidor *Dynamic Host Configuration Protocol*, Protocolo de Configuração Dinâmica de Hosts (DHCP). Sob esta abordagem, o próprio servidor é responsável por gerar os endereços de forma automática (BATTISTI, 2022).

Figura 17: Configuração da atribuição de IP automática

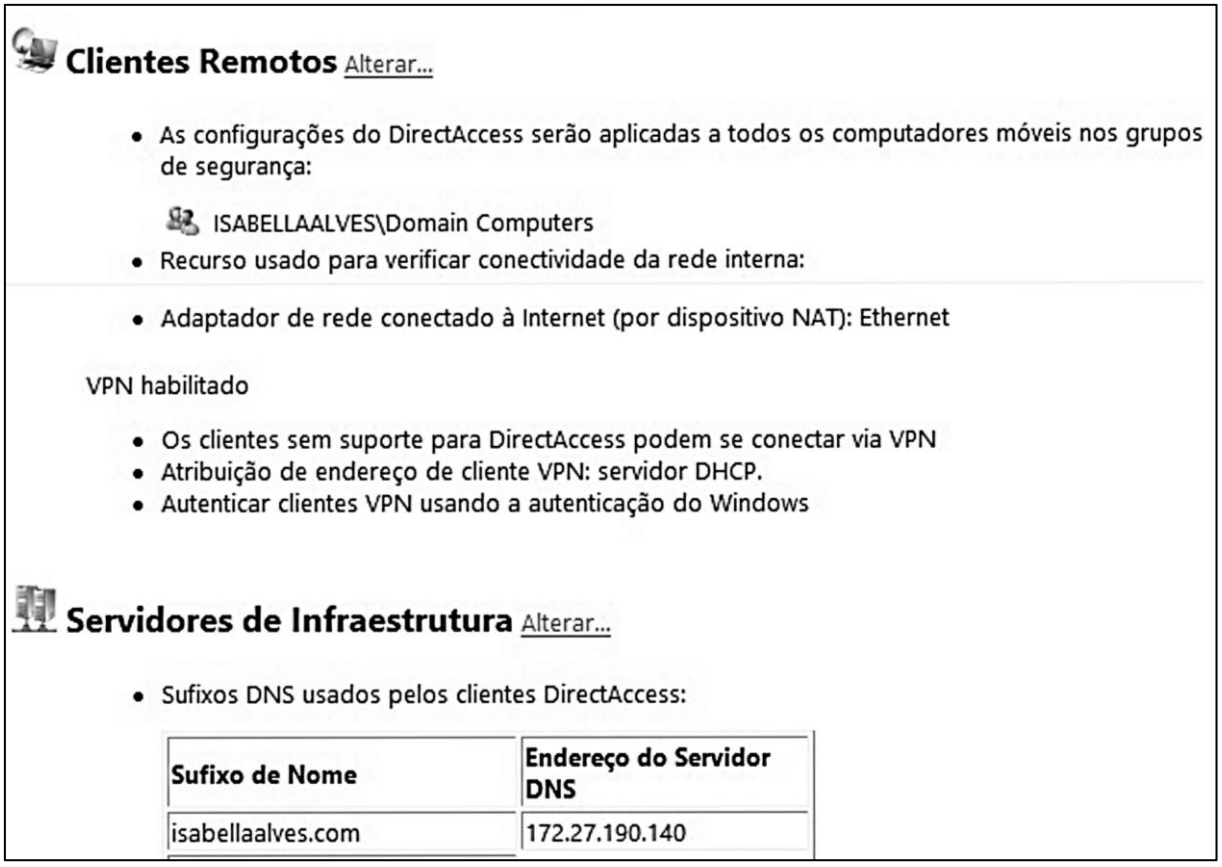


Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

Outra opção, seria optar pela atribuição de endereços IP escolhendo um intervalo de endereços específicos. A escolha da forma de atribuição dos endereços IP, pode ser realizada pelo usuário de acordo com as necessidades específicas do ambiente em questão (BATTISTI, 2022).

Este processo habilitou a VPN para a autenticação dos clientes mediante o emprego da autenticação do Windows. Além disso, foram configuradas as definições relativas ao endereço do servidor DNS e ao sufixo de nome. O resumo dessas configurações são mostradas na Figura 18 (MICROSOFT, 2019).

Figura 18: Resumo das configurações realizadas para a VPN

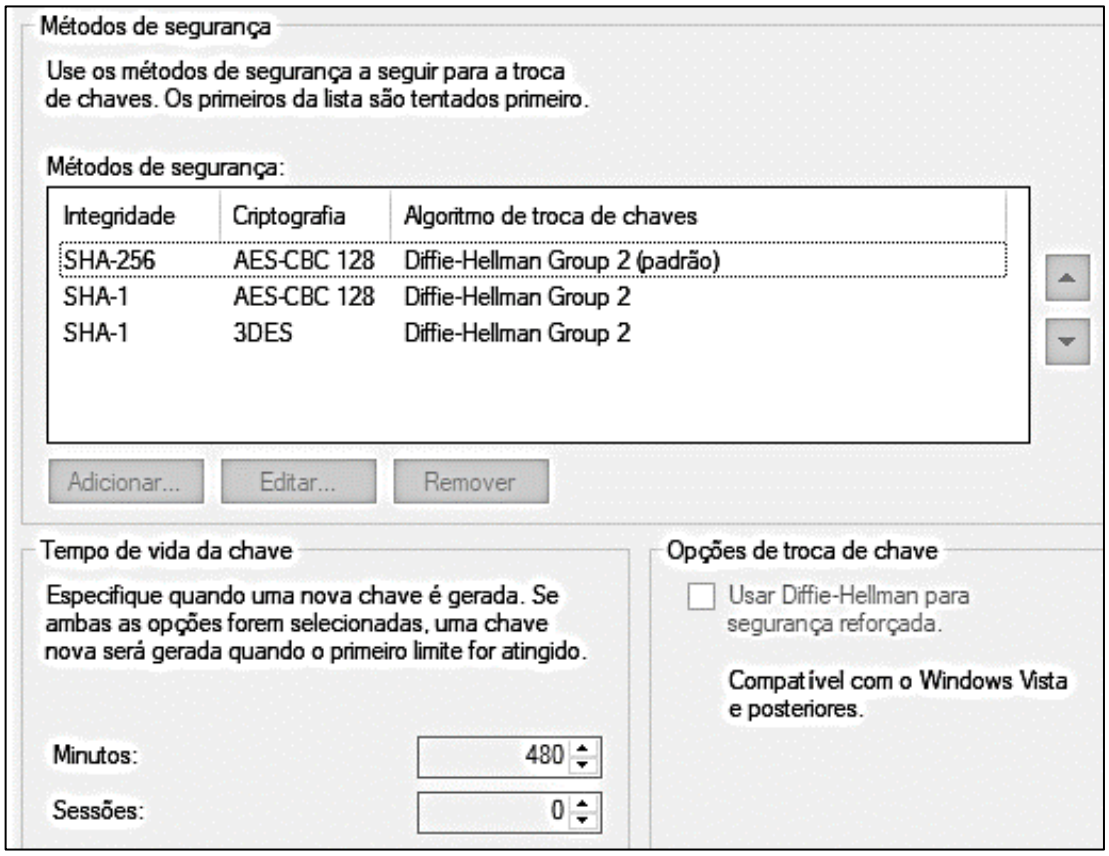


Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

Com a instalação da VPN, procedeu-se à configuração do IPSec no *firewall* do servidor. Esta etapa envolveu a criação de uma nova regra de segurança de conexão, estabelecendo critérios de autenticação mediante a utilização de métodos específicos configurados nas definições do IPSec. Esses métodos de autenticação foram estipulados para abranger conexões de um domínio corporativo, uma rede privada local ou uma rede pública local (BATTISTI, 2022).

As configurações dos métodos de autenticação foram especificadas nas "Propriedades do Windows Defender *Firewall* com Segurança Avançada", onde se encontram as definições relativas ao tipo de troca de chaves aplicado ao IPSec. Neste trabalho, foi aplicado o algoritmo SHA-256 e da criptografia AES, conforme mostrado na Figura 19. Estes parâmetros de algoritmo e criptografia foram abordados de maneira detalhada no capítulo 2, seção 2.2 (MICROSOFT, 2019).

Figura 19: Métodos de Segurança utilizados no IPSec



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

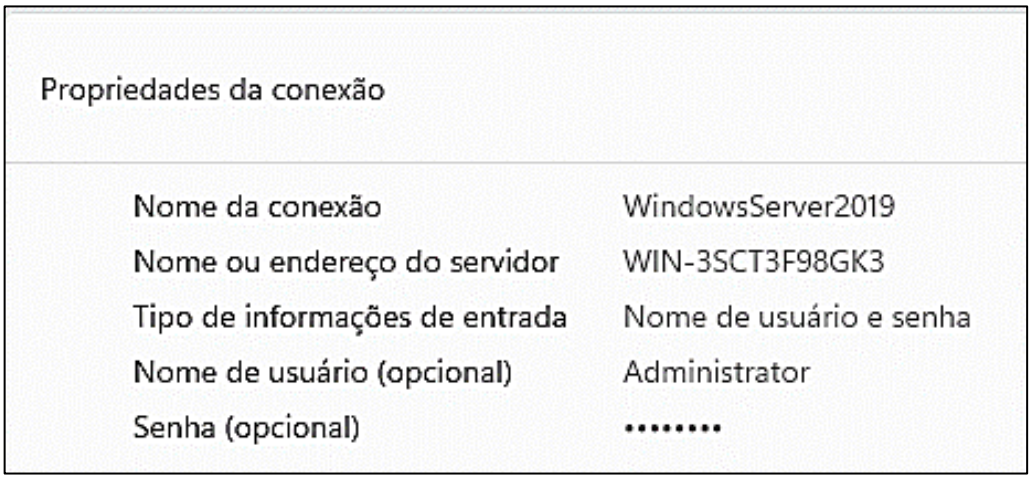
4.5 Configuração do Cliente VPN

Na máquina do usuário remoto, a configuração realizada consistiu na ativação das portas do *firewall* destinadas ao compartilhamento de arquivos de *Internet Control Message Protocol version 4*, Protocolo de Mensagem de Controle da *Internet* versão 4 (ICMPv4), tanto nas portas de entrada quanto nas de saída. Este procedimento foi realizado para estabelecer a conectividade VPN de maneira eficaz.

Neste trabalho, a máquina física utilizada possui o sistema operacional Windows 11 Pro, que incorpora, em suas opções de conectividade, a capacidade de

estabelecer conexões VPN. Para efetuar a conexão, foi necessário acessar as configurações da conexão VPN na máquina, atribuir um nome à conexão, especificar o nome do servidor e, ao realizar a conexão, fornecer as credenciais de usuário e senha. Os detalhes de como foi realizado essa conexão podem ser consultados no Apêndice IV. As propriedades detalhadas da conexão VPN podem ser visualizadas na Figura 20.

Figura 20: Propriedades da conexão do cliente VPN



Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

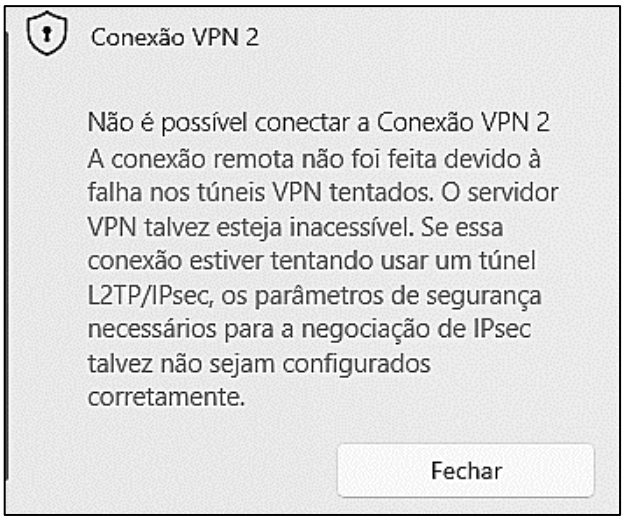
5 TESTES REALIZADOS

Neste capítulo, são descritos os testes efetuados no intuito de estabelecer a conexão do cliente com o servidor VPN. Também são abordadas as dificuldades enfrentadas ao longo da implementação deste trabalho.

5.1 Autenticação

Na conexão do cliente ao servidor VPN, foram realizadas tentativas de autenticação. Inicialmente, ao efetuar a conexão, houve a apresentação de uma mensagem de erro, que indicava a inacessibilidade da VPN, conforme mostra na Figura 21.

Figura 21: Erro de conexão VPN



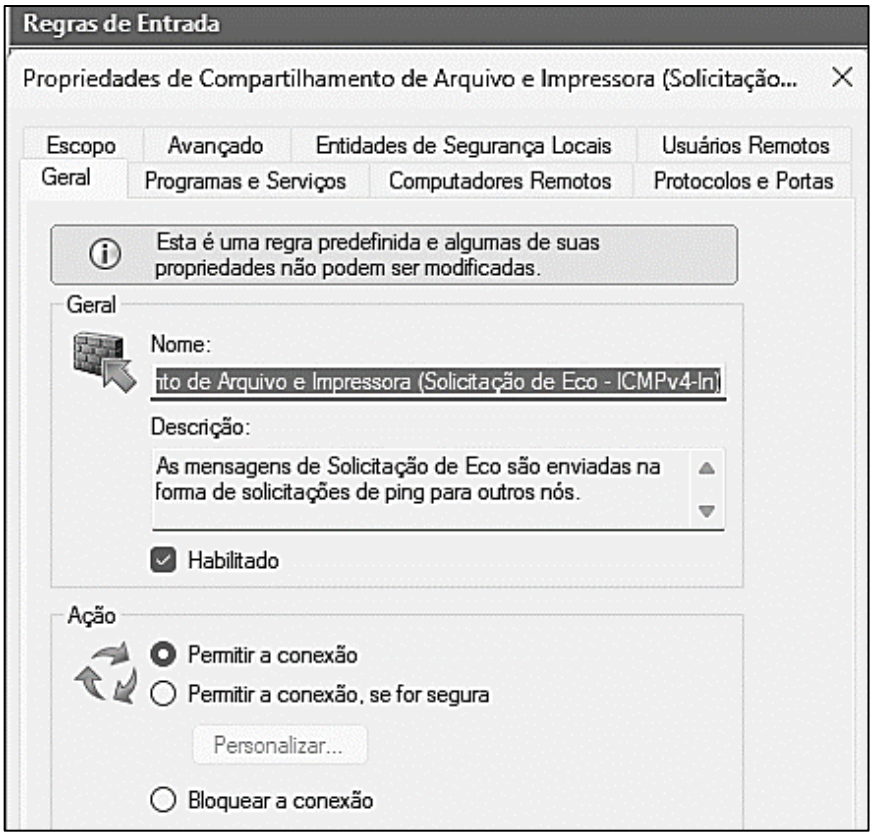
Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

Após a manifestação do referido erro, foi realizado a verificação da configuração do IPsec e das suas regras de criptografia no servidor VPN. Contudo, não foram identificadas pendências de configuração, e o IPsec estava devidamente configurado. Uma segunda tentativa de conexão foi feita, na qual todos os dados da VPN foram novamente fornecidos. Porém o erro persistiu. O próximo passo consistiu na verificação das portas do *firewall* no cliente VPN.

As portas de compartilhamento ICMPv4 estavam desabilitadas no cliente VPN. Estas portas podem ser ativadas através do menu iniciar da máquina, acessando o Windows Defender Firewall com Segurança Avançada. Posteriormente, nas regras de

entrada, é possível localizar a opção "Compartilhamento de Arquivo e Impressora (Solicitação de Eco - ICMPv4 - In)". Duas regras correspondentes são identificadas, é necessário acessá-las, habilitar, aplicar as alterações e clicar em "Ok". A Figura 22 mostra a tela de ativação da regra.

Figura 22: Habilitando porta no *firewall* para a conexão VPN



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

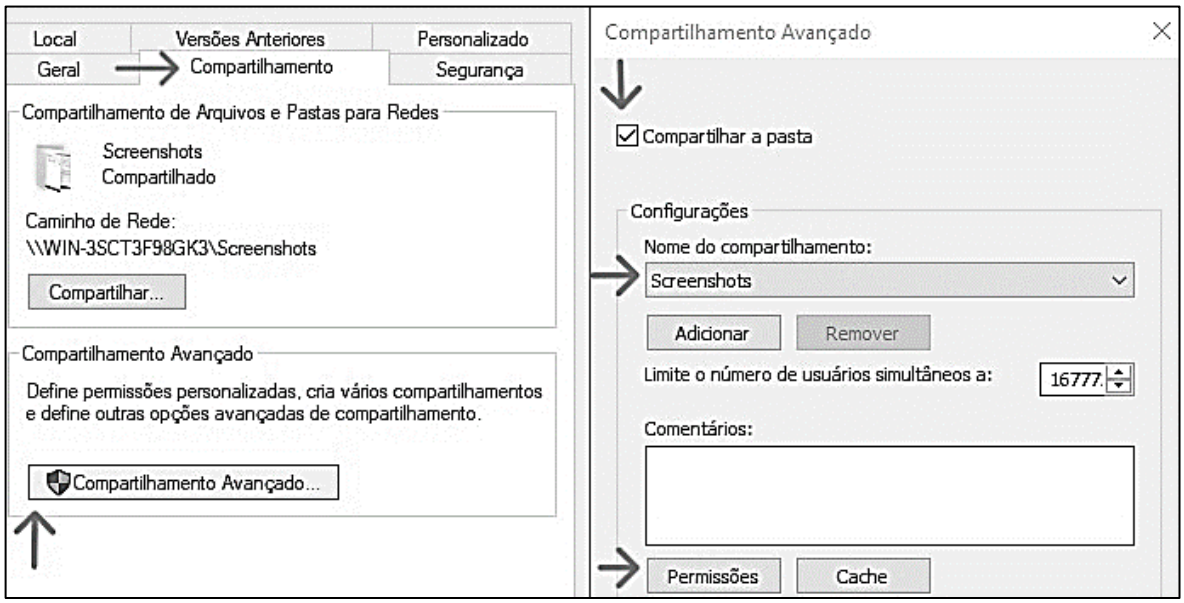
O mesmo procedimento foi replicado nas regras de saída, a fim de assegurar a consistência na configuração. Dessa forma a conexão VPN foi estabelecida.

5.2 Acesso ao diretório compartilhado

No servidor, ao escolher a pasta a ser compartilhada com os usuários, é necessário realizar uma sequência de ações para habilitar o compartilhamento. Inicialmente, é necessário clicar com o botão direito sobre a pasta escolhida, abrir as suas propriedades e acessar a aba denominada "Compartilhamento". Posteriormente, selecionar a opção de "Compartilhamento Avançado", selecionar a opção "Compartilhar Pasta" e atribuir um nome específico. Logo após definir as permissões

destinadas ao usuário que tem-se acesso à pasta. Esse passo a passo é mostrado na Figura 23.

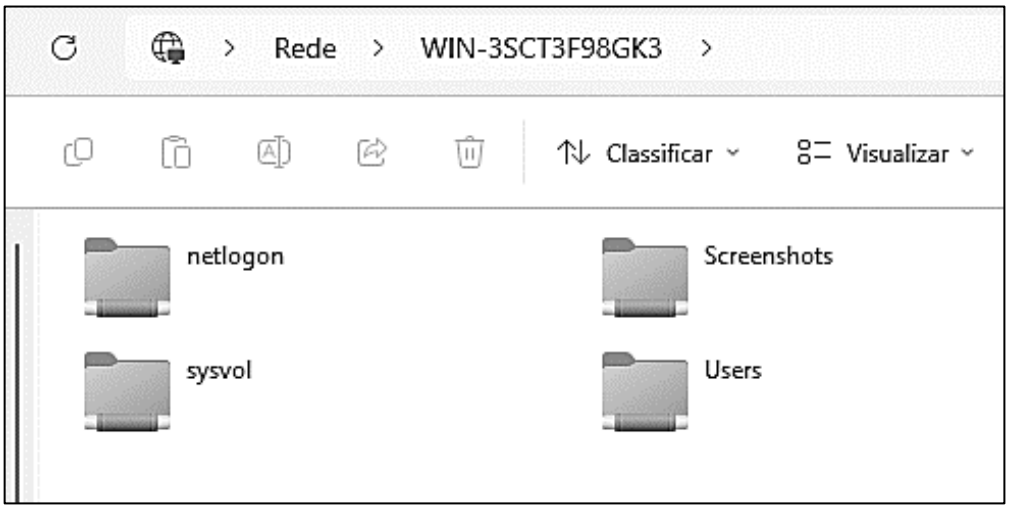
Figura 23: Compartilhando diretório com o cliente VPN



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

Na máquina do usuário, o acesso à pasta compartilhada é realizado mediante o estabelecimento da conexão VPN com o servidor. Acessar a pasta requer a digitação de "\\NomeDoServidor" no menu iniciar. Ao realizar essa ação, as pastas disponíveis para o usuário tornam-se visíveis. Neste trabalho, a pasta compartilhada, mostrada na Figura 24, foi acessada mediante ao comando "\WIN-3SCT3F98GK3".

Figura 24: Cliente VPN acessando as pastas compartilhadas do servidor



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

5.3 Resultados obtidos

Esse estudo mostra a configuração detalhada do ambiente de testes que permitiu a criação de uma infraestrutura funcional de teletrabalho, simulando um cenário realista.

A autenticação bem-sucedida do cliente VPN, após a correção das configurações de portas ICMPv4, reforça a importância da verificação minuciosa de parâmetros de segurança. O acesso ao diretório compartilhado, uma vez estabelecida a conexão VPN, demonstra a eficácia da configuração do servidor VPN e das permissões de compartilhamento de arquivos. A configuração e ativação do protocolo IPsec mostra os métodos de segurança utilizados para manter uma comunicação segura.

6 CONSIDERAÇÕES FINAIS

Com o aumento significativo do teletrabalho, os profissionais têm desempenhado suas atividades trabalhistas não apenas em domicílios, mas também em espaços públicos como ruas, *shopping centers*, e até mesmo durante suas viagens. Nesse cenário é necessário garantir que tais indivíduos possuam acesso seguro aos dados corporativos.

A VPN viabiliza que o usuário exerça seu trabalho a partir de qualquer localidade global, estabelecendo uma conexão segura com a infraestrutura corporativa e facilitando a troca de dados de maneira segura, evitando assim a ameaça de comprometimento e roubo de informações sensíveis. Desta maneira, a VPN proporciona um ambiente propício para a circulação segura de dados relevantes e privativos pela rede da *Internet*.

Este estudo apresentou detalhadamente o funcionamento da VPN, discorrendo sobre sua capacidade de manter uma comunicação segura, abordando as formas usadas para assegurar a integridade dos dados transmitidos através do uso de chaves e criptografia. Adicionalmente, foram abordados os requisitos fundamentais para a implementação de uma VPN, bem como os motivos para sua utilização. Além disso, foi mostrado o crescimento do teletrabalho em escala global, contextualizando-o dentro da temática abordada neste trabalho.

De acordo com a metodologia proposta nesse trabalho, foram realizadas pesquisas com o objetivo de abordar as características fundamentais das VPNs. Foram descritas as principais propriedades dessa tecnologia, além de apresentar uma orientação prática sobre sua implementação, evidenciando um cenário simulado de teletrabalho.

A VPN não se restringe à sua aplicação isolada, são necessários a integração de serviços de rede complementares, o DNS e o Active Directory. No contexto deste trabalho, o protocolo de segurança selecionado para a implementação da VPN foi o IPsec. Embora existam outros protocolos, essa escolha fundamentou-se em sua capacidade superior de proporcionar maiores medidas de segurança.

No ambiente de simulação, foi empregado um *switch* para estabelecer a conexão entre o usuário e o servidor. No entanto, em cenários reais, a comunicação entre o usuário e o servidor é comumente intermediada por um roteador.

Na configuração do ambiente de testes, a intenção inicial era utilizar a plataforma Azure para criar a máquina virtual e o servidor. Entretanto, devido às limitações da máquina utilizada, foi necessário efetuar uma transição para o recurso do Windows, o Hyper-V. Ressalta-se, contudo, que, a configuração da VPN é a mesma, independentemente do *software* de virtualização escolhido.

Este trabalho mostra que a VPN é uma solução de baixo custo para as empresas, por utilizar a infraestrutura da *Internet*, ao mesmo tempo em que oferece segurança na transmissão de dados, mediante a implementação de autenticação de usuários e criptografia.

Observa-se um crescimento global do trabalho remoto, no entanto, há também, aumento significativo de agentes maliciosos conectados à *Internet*, que buscam capturar informações privadas de corporações e clientes. Diante desse cenário, a aquisição de uma conexão segura torna-se uma necessidade, permitindo aos usuários a confiança necessária para a troca de informações pessoais com empresas do mundo todo.

A utilização de VPNs oferece uma solução eficiente e acessível para assegurar a integridade e confidencialidade das comunicações empresariais em um ambiente digital cada vez mais suscetível a ameaças, sendo essa uma importante contribuição desse trabalho, já que o trabalho remoto se expande cada vez mais.

6.1 Sugestões de trabalhos futuros

Como sugestão de trabalhos futuros, propõe-se:

- Realização da instalação do cliente e do servidor em um novo ambiente de virtualização;
- Realizar a instalação do cliente e servidor, considerando o roteador como meio de comunicação;
- Realizar a instalação da VPN com o propósito de compartilhar o uso de aplicativos de trabalho, como sistemas empresariais, instalados no servidor;
- Realizar a instalação do cliente e servidor para realizar o acesso através de um endereço IP fixo;
- Realizar testes de infiltração, utilizando o *pen test,* na VPN para identificar possíveis vulnerabilidades e reforçar a segurança;

- Utilizar o Wireshark para capturar e analisar o tráfego na VPN observando evidências da criptografia;
- Realizar testes de desempenho comparativos entre o OpenVPN e a solução nativa de VPN do Windows Server.

REFERÊNCIAS

BATTISTI, Júlio **DOMINE o Windows Server 2019 e o Active Directory.** Direção:. [*S. l.*]: Júlio Battisti - Livros e Cursos Ltda, 2022. Disponível em: https://membros.certificacoes.com.br/meus-cursos.html. Acesso em: 1 ago. 2023.

FEILNER, Markus. **OpenVPN**: Building and Integrating Virtual Private Networks. [*S. l.*: *s. n.*], Abril 2006. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=hKXEz92wtlMC&oi=fnd&pg=PA1&dq=open+vpn+linux&ots=ayTbXzuH7y&sig=YlcqelR-3GPfPZ343qUSHS8G5Pc#v=onepage&q=open%20vpn%20linux&f=false>. Acesso em: 12 dez. 2023.

FILHO, Fernando de Holanda Barbosa *et*. *al*. Revista brasileira de economia. **Trabalho remoto no Brasil**, [*s.l.*], v. 76, n. 3, p. 349-378, jul/set 2022. Disponível em: <https://bibliotecadigital.fgv.br/ojs/index.php/rbe/article/view/85168/83517>. Acesso em: 25 maio 2023.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores.** 4. ed. Porto Alegre: AMGH, 2010.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6. ed. São Paulo: Atlas, 2017.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet.** 6. ed. São Paulo: Pearson Education do Brasil, 2013.

MCDONALD, Grant; PAPADOPOULOS, Pavlos; PITROPAKIS, Nikolaos; AHMAD, Jawad; BUCHANAN, William J. Ransomware: Analysing the Impact on Windows Active Directory Domain Services. **Cyber Situational Awareness in Computer Networks**, Edimburgo - Reino Unido, v. 22, n. 3, p. 3, 26 jan. 2022. Disponível em: <https://www.mdpi.com/1424-8220/22/3/953>. Acesso em: 20 out. 2023.

MICROSOFT. **Requisitos de Sistema do Hyper-V do Windows 10**: Verificar a Compatibilidade de Hardware. [*S. l.*], 13 jul. 2023a. Disponível em: <https://learn.microsoft.com/pt-br/virtualization/hyper-v-on-windows/reference/hyper-v-requirements>. Acesso em: 20 out. 2023.

MICROSOFT. **Selecione seu download do Windows Server 2019**. [*S. l.*], 2023b. Disponível em: <https://www.microsoft.com/pt-br/evalcenter/download-windows-server-2019>. Acesso em: 1 nov. 2023.

MICROSOFT. **Windows Server 2019**. [*S. l.*], 2019. Máquina Virtual.

MICROSOFT. **Windows 11 Pro**. 22H2. [*S. l.*], 24 fev. 2023c. Notebook.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores**: princípios e práticas. 2. ed. Rio de Janeiro: Elsevier, 2014.

TANENBAUM, Andrew S. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TRIBUNAL SUPERIOR DO TRABALHO. Secretaria de Comunicação Social do TST. **Teletrabalho**: O trabalho de onde você estiver. 1. ed. [*S. l.*: *s. n.*], 2020. Disponível em: <https://www.tst.jus.br/documents/10157/2374827/Manual+Teletrabalho.pdf/e5486dfc-d39e-a7ea-5995-213e79e15947?t=1608041183815>. Acesso em: 25 maio 2023.

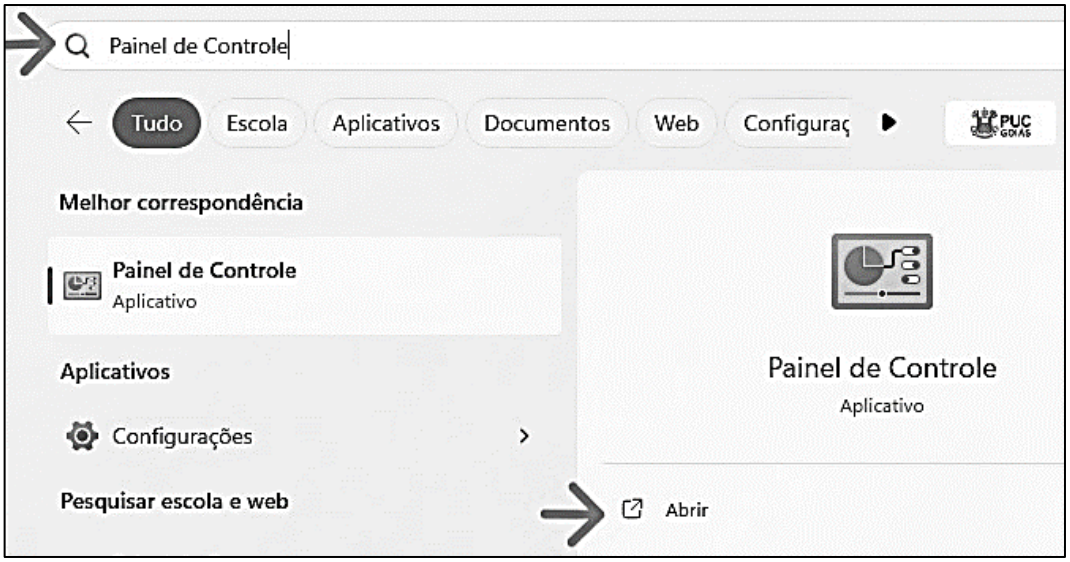
VIRALIZE MIDIA (MA). **Manutenção em Redes de Computadores**: Implantação e Configuração de Redes. Travessa Zuleide Bogéa, 157 - Alemanha, 2023. Disponível em: <http://www.viralizemidia.com.br/manutencao-em-redes-de-computadores/>. Acesso em: 27 maio 2023.

WAZLAWICK, R. S. **Metodologia da Pesquisa para Ciência da Computação.** 2ª. ed. [S.l.]: Campus, 2014.

APÊNDICE I – CRIANDO A MÁQUINA VIRTUAL

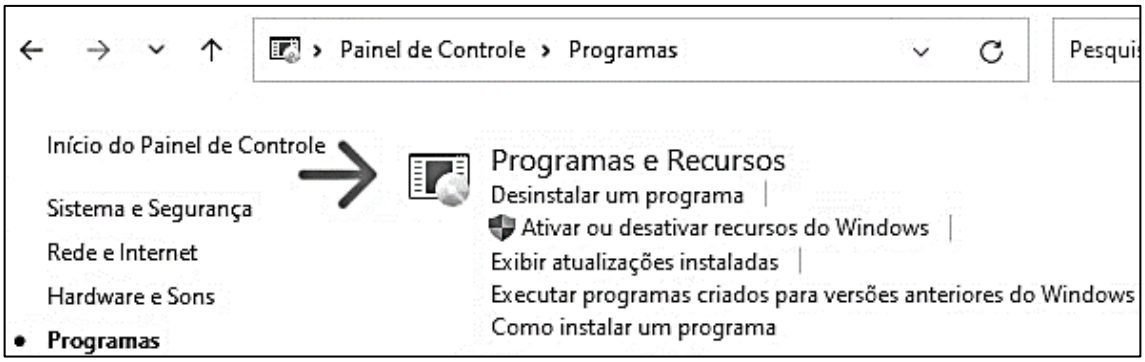
1 - No menu inicial do Windows 11 Pro, pesquisar por “painel de controle” e abrir. Clicar em “programas” e em seguida “programas e recursos”, conforme a Figura 25 e a Figura 26 mostram.

Figura 25: Abrindo o Painel de Controle



Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023a.

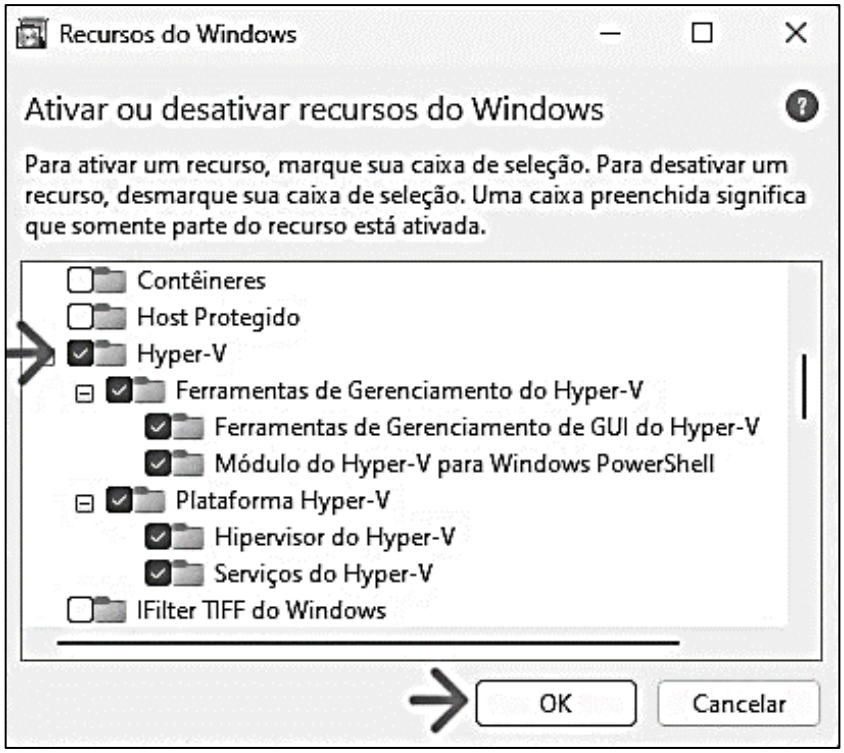
Figura 26: Abrindo Programa e Recursos no *Windows*



Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023a.

2 - Acessar na lateral esquerda da tela “ativar ou desativar recursos do Windows”. Procurar o recurso “Hyper-V” e selecioná-lo, mostrado na Figura 27. Clicar em “Ok” e, após os recursos serem instalados, é necessário a reinicialização do computador.

Figura 27: Ativando o Hyper-V



Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023a.

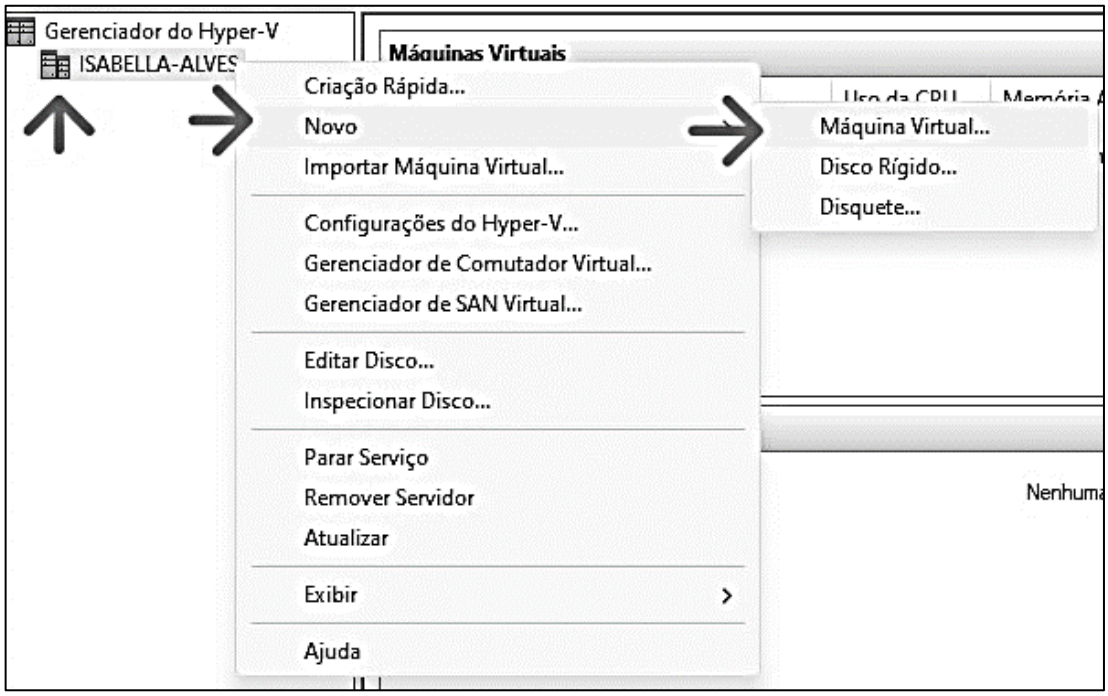
3 - No menu inicial, pesquisar por “Gerenciador do Hyper-V” e abrir. Na tela que abre é feita a criação da máquina virtual.

Figura 28: Abrindo o Gerenciador do Hyper-V

Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023a.

4 – Na tela do Gerenciador do Hyper-V, na lateral esquerda, clicar no nome do computador com o botão direito do *mouse*. Clicar em “novo” e em seguida na opção “máquina virtual”, mostrado na Figura 29.

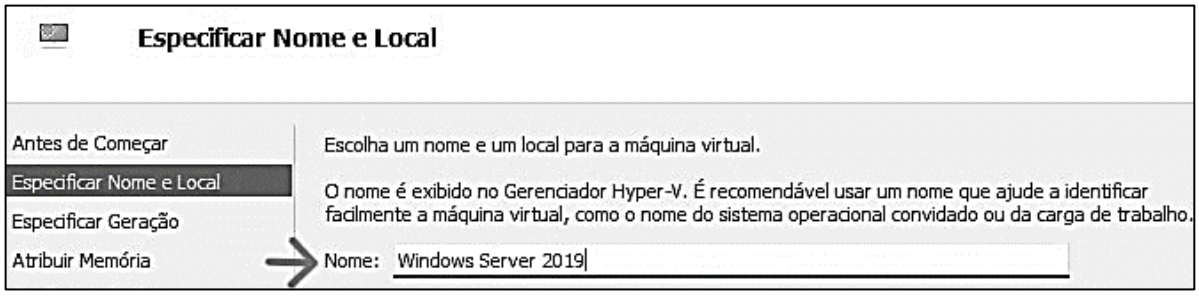
Figura 29: Criando a máquina virtual



Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023a.

5 – Abre-se uma nova janela. Para prosseguir com a criação da máquina virtual, clicar em avançar. Em seguida, colocar o nome da máquina virtual. Nesse trabalho, foi dado o nome “Windows Server 2019”, conforme mostrado na Figura 30. Clicar em avançar.

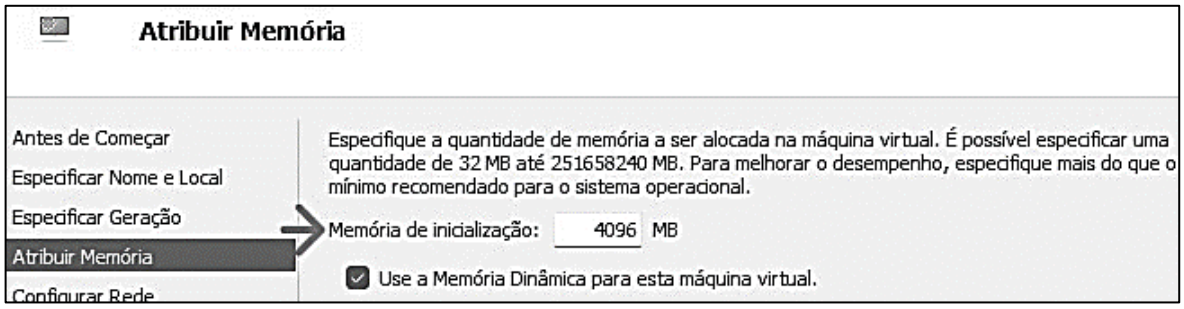
Figura 30: Dando nome a máquina virtual



Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

6 - Em “atribuir memória”, o requisito mínimo é de 512 MB, por padrão a máquina usada para este trabalho atribuiu 4096 MB de memória, foi deixado o valor padrão. Próximo passo, avançar.

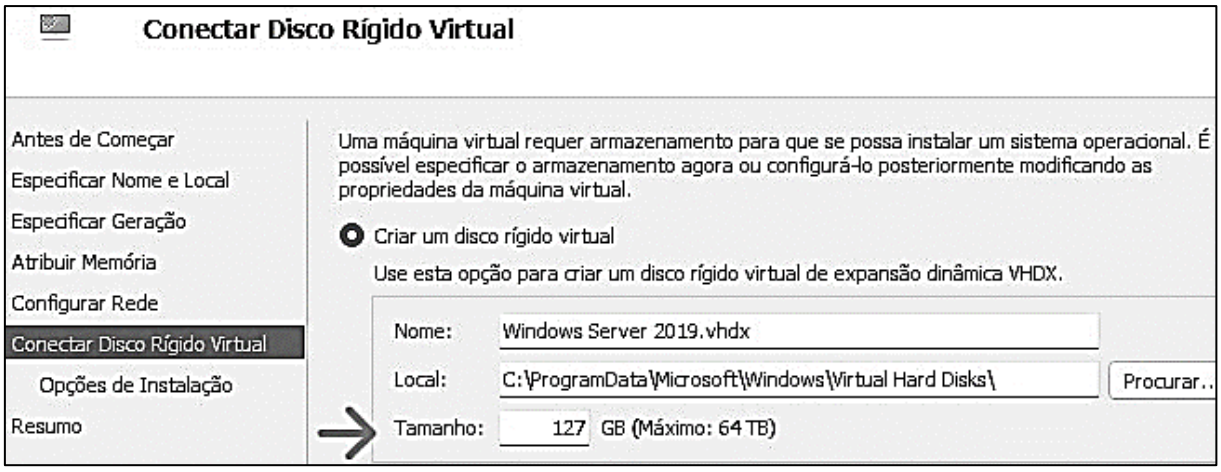
Figura 31: Atibuindo memória a máquina virtual



Fonte: Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

7 – Em “Configurar Rede”, escolher a rede de conexão padrão, “Default Switch”. Em seguida clicar em avançar. A próxima configuração é a aba “Conectar disco rígido virtual”. O requisito é que o disco rígido tenha no mínimo 32 GB para o funcionamento da máquina virtual. Por padrão, no computador utilizado para esse trabalho, atribuiu-se 127 GB. Também é mostrado o nome da máquina que foi definido no inicío da criação da máquina virtual e o local onde é armazenado no disco. Em seguida clicar em avançar.

Figura 32: Configurando o disco rígido



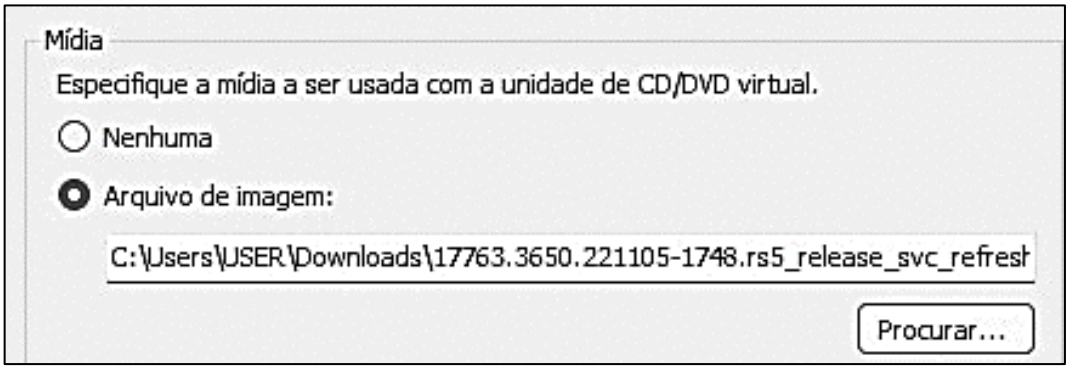
Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

8 – Em opções de instalação, escolher “Instalar um sistema operacional a partir de um CD/DVD-ROM inicializável”, marcando a opção “Arquivo de imagem”. Clicar

em procurar e adicionar o arquivo ISO que foi baixado na máquina física, assim como mostrado na Figura 33. Esse arquivo é disponibilizado pela Microsoft, e pode ser baixado em seu *site*.

Ao adicionar o arquivo, clicar em “Aplicar” e “Ok”. Na próxima aba aparece a descrição das configurações escolhidas para a máquina virtual, clicar em concluir e a máquina virtual é criada.

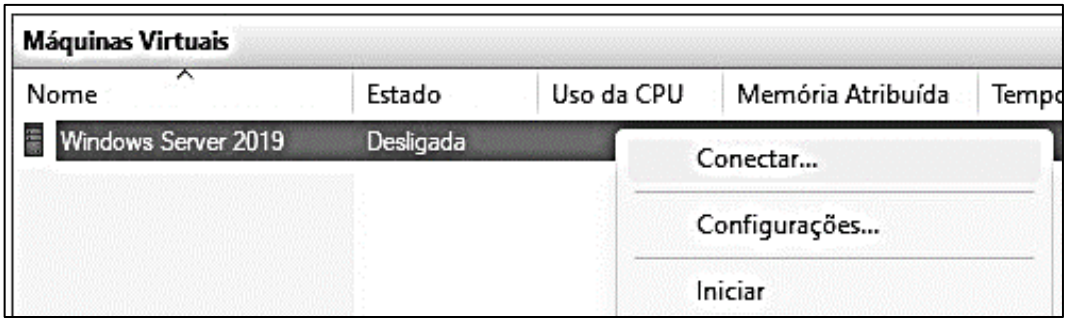
Figura 33: Adicionando o arquivo ISO para instalar o sistema operacional



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

9 – Para a instalação do sistema operacional Windows Server 2019, no Gerenciador do Hyper-V, clicar sobre o nome da máquina virtual com o botão direito do *mouse* e conectar, como mostrado na Figura 34.

Figura 34: Conectando a máquina virtual

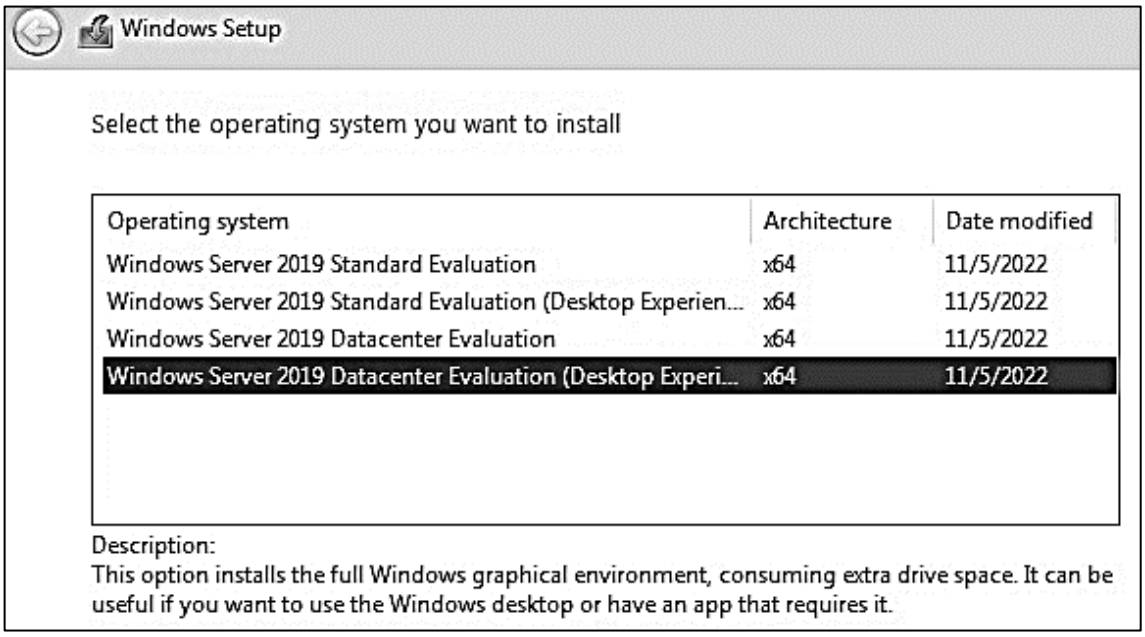


Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

10 – É aberta a máquina virtual, clicar em iniciar e inicia a instalação do sistema operacional. Durantes a instação o usuário pode escolher as configurações de sua preferência, como o idioma a ser instalado e o sistema opacional desejado. Nesse trabalho foi instalado o Windows Server 2019 Datacenter Evaluation, para realizar a

instalação do ambiente gráfico completo do Windows, como mostrado na Figura 35. Após a escolha do sistema operacional, avançar.

Figura 35: Instalação do sistema operacional



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

11 - É necessário criar uma senha para a conta de administrador, para acessar a máquina virtual, mostrado na Figura 36.

Após colocar a senha, a máquina está pronta uso. Ao abrir a máquina virtual, pode ser observado que já foi instalado um servidor, porém ainda deve ser configurado para se tornar um servidor VPN.

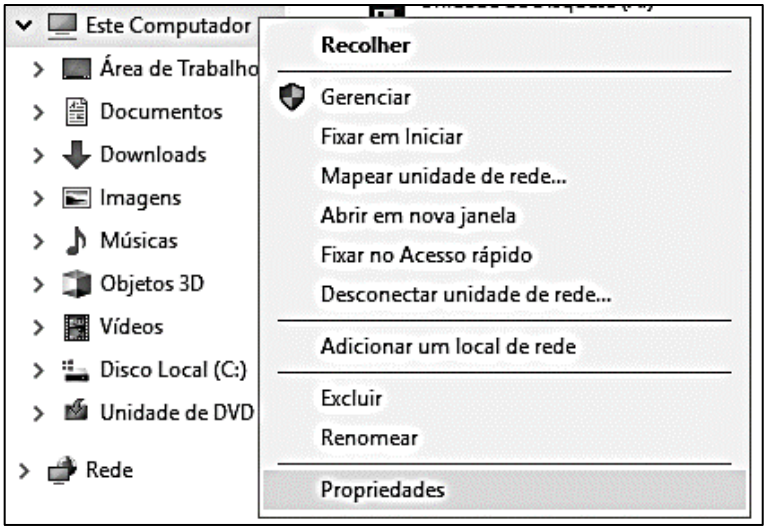
Figura 36: Configurando senha para acessar a máquina virtual.

Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

APÊNDICE II – CONFIGURAÇÃO DO ACTIVE DIRECTORY

1 – Para ativar o acesso remoto à máquina virtual, no explorador de arquivo da máquina virtual, clicar com o botão direito do *mouse* em “Este Computador” e ir em “Propriedades”, como mostrado na Figura 37.

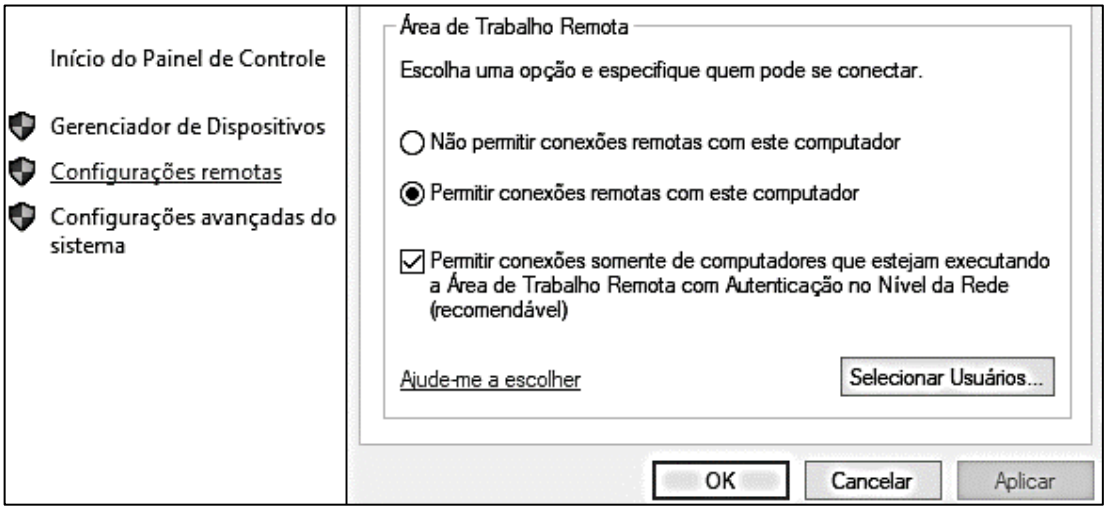
Figura 37: Ativando o Acesso Remoto na máquina virtual



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

2 – Em “Configurações remotas”, é aberta a aba “Propriedades do Sistema”. As opções de permissões em “Área de Trabalho Remota” devem ser selecionadas conforme mostrado na Figura 38, aplicar e clicar em “Ok” para habilitar as permissões.

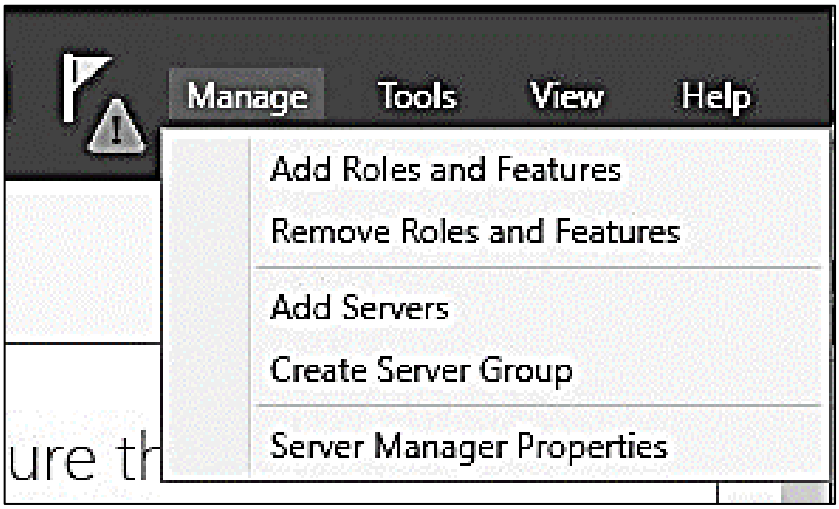
Figura 38: Ativando as permissões de acesso remoto na máquina virtual



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

3 – Para realizar a instação do Active Directory, abrir o “Gerenciador de Servidores” que pode ser encontrado no menu iniciar. “Adicionar funções e recursos” em “Gerenciar”, como mostrado na Figura 39.

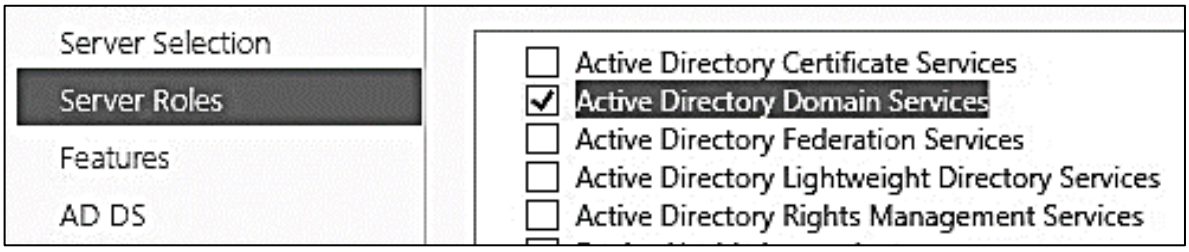
Figura 39: Adicionando novas funções e recursos ao servidor



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

4 – É aberto um assistente de instalação, avançar e selecionar o tipo de instalação baseada em funções ou recursos. Ao avançar, escolher como destino da instalação o servidor e prosseguir para escolher a função a ser instalada no servidor. Deve ser selecionado o Serviços de Domínio do Active Directory, conforme mostrado na Figura 40. Logo em seguida, avançar e instalar a função.

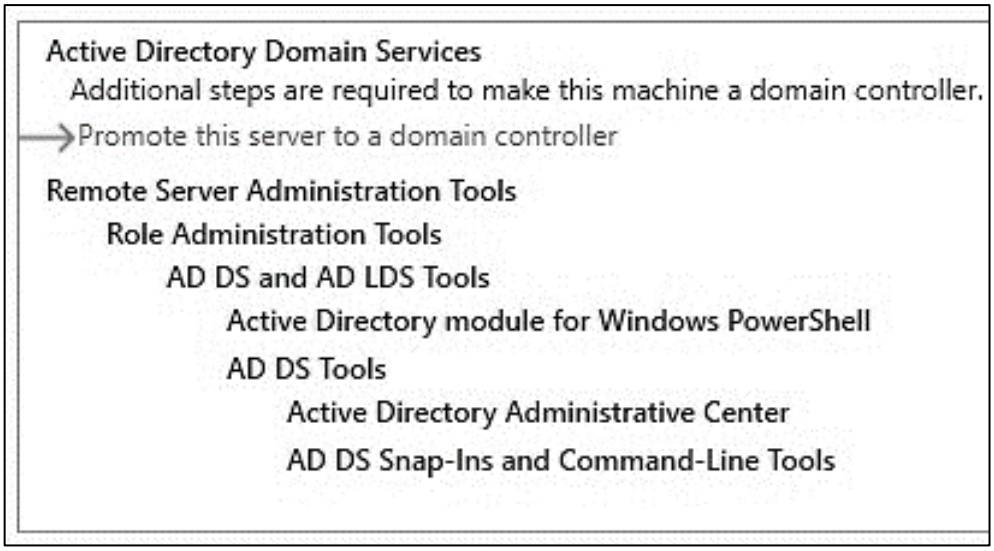
Figura 40: Instalando a função do Active Directory no servidor



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

5 - Ao finalizar a instalação, promover o servidor a um controlador de domínio, clicando na opção, mostrada na Figura 41.

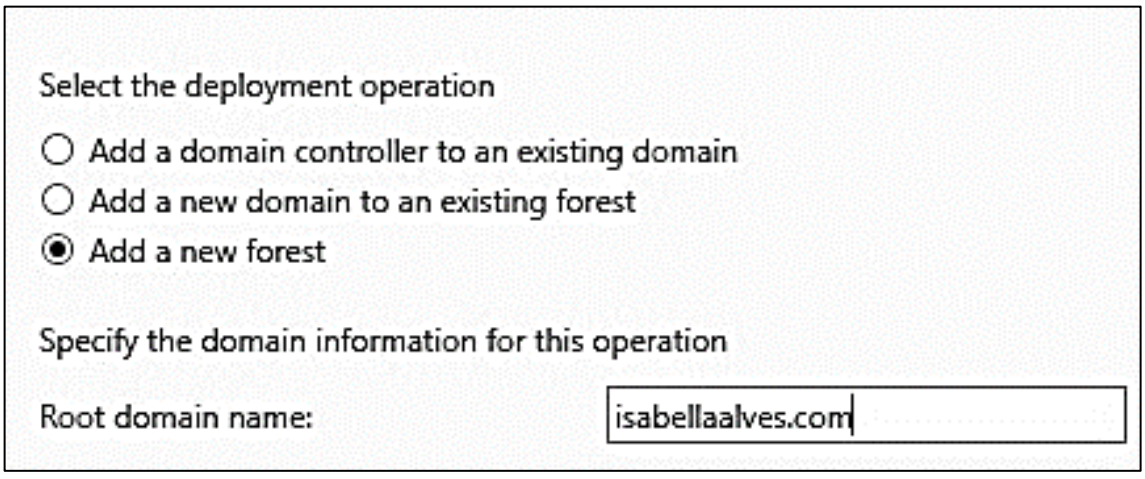
Figura 41: Promovendo o servidor a um controlador de domínio



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

6 – Selecionar “Adicionar uma nova floresta” e nomear a raiz de domínio, como mostrado na Figura 42. Logo em seguida avançar para as opções do controlador de domínio.

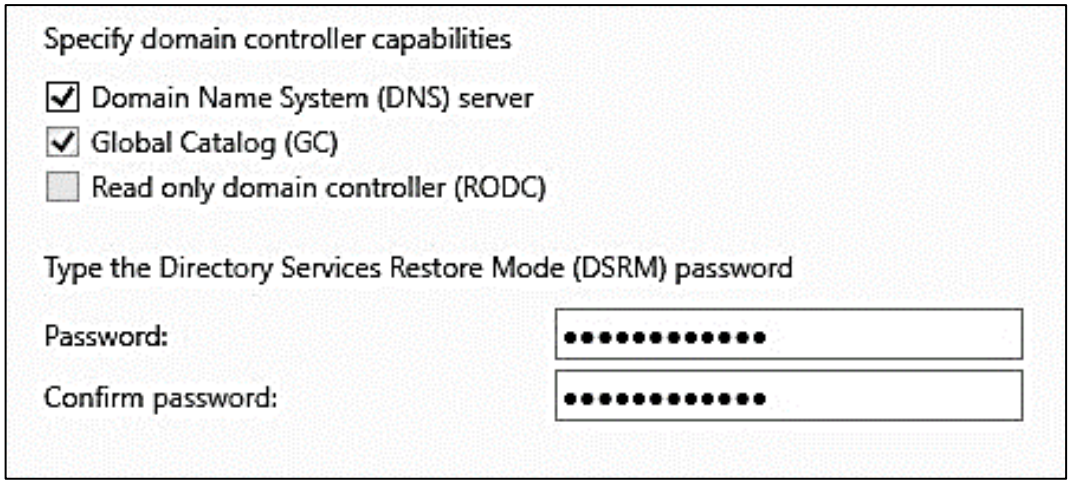
Figura 42: Adicionando uma nova floresta ao servidor



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

7 – Selecionar o recurso “Servidor do sistema de nomes de domínio”, adicionar uma senha e avançar, como mostrado na Figura 43. O nome da NetBIOS é colocado automaticamente, sendo o mesmo nome da raiz de domínio, antes do “.com”.

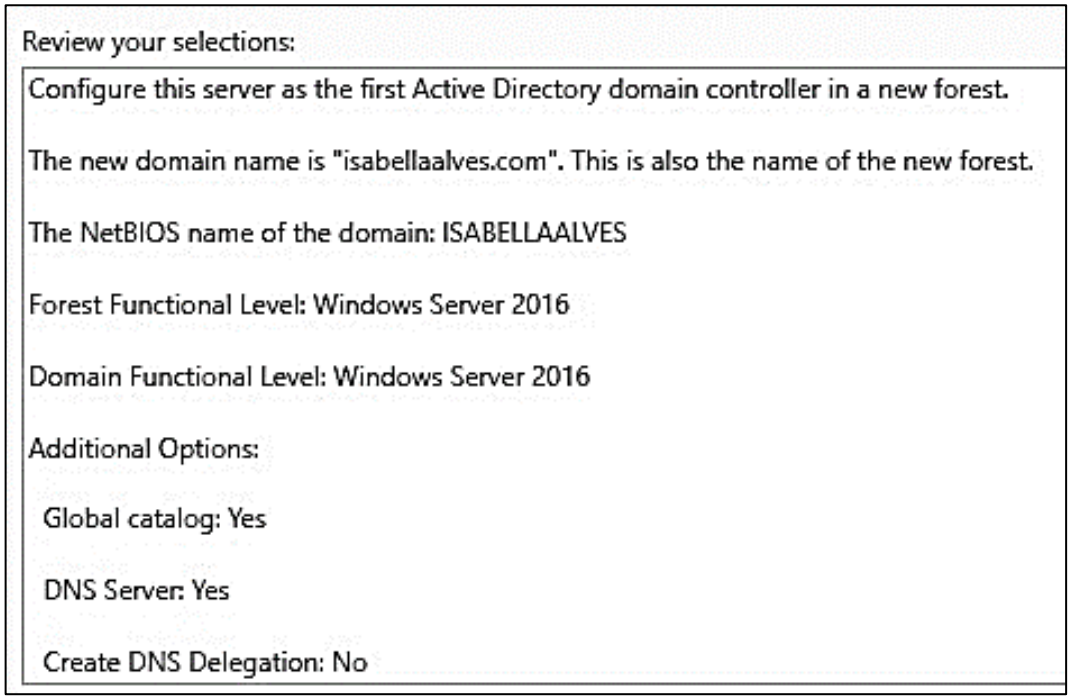
Figura 43: Especificando os recursos do controlador de domínio



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

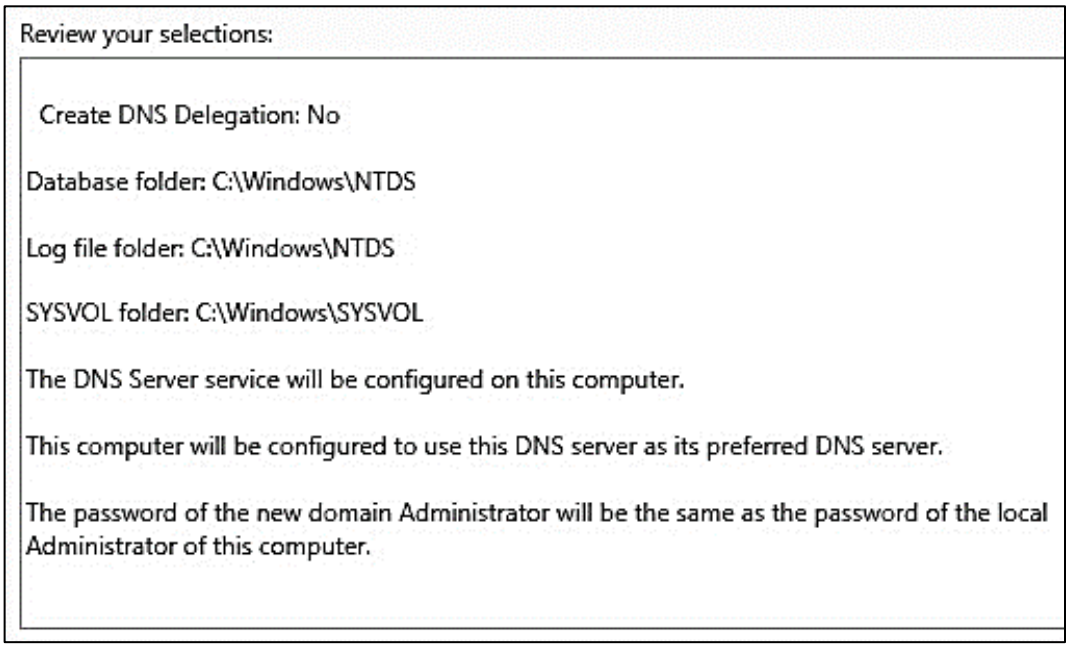
8 – Antes de instalar é mostrado uma tela com todas as configurações escolhidas, para o usuário poder verificar se está tudo correto e confirmar. As configurações colocadas nessa etapa do trabalho podem ser visualizadas nas Figuras 44 e 45. Após a instalação é necessário reiniciar o servidor para que as configurações sejam aplicadas.

Figura 44: Descrição das configurações selecionadas para a implementação do controlador de domínio



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

Figura 45: Descrição das configurações selecionadas para a implementação do controlador de domínio

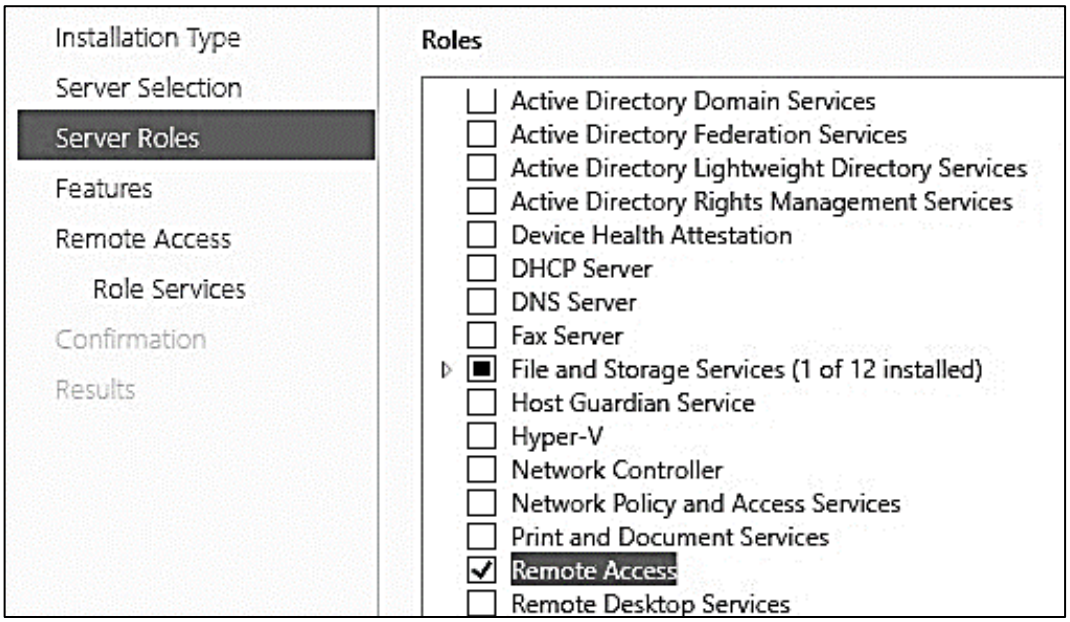


Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

APÊNDICE III – INSTALAÇÃO DA VPN

1 – Para instalar os recursos da VPN, no menu iniciar da máquina virtual, em gerenciar, dentro do gerenciador de servidores, clicar em “Adicionar funções e recursos”. Avançar até a tela de selecionar funções do servidor. Selecionar a função “Acesso Remoto”, mostrado na Figura 46.

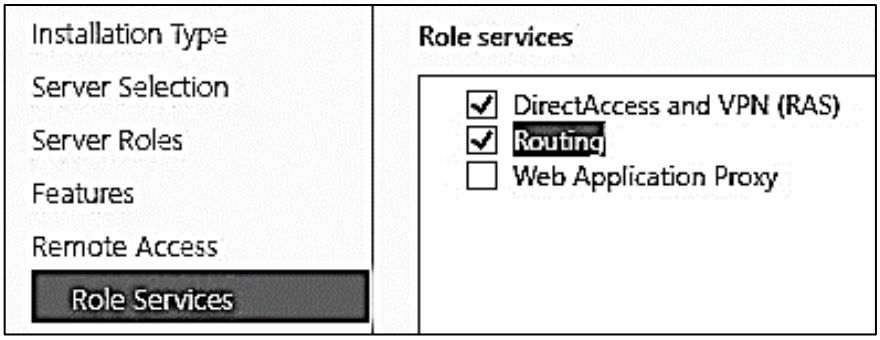
Figura 46: Instalando o Acesso Remoto



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

2 – Avançar até a tela de seleção de serviços de função, selecionar as funções de “DirectAccess e VPN” e a função de “Roteamento”, como mostrado na Figura 47. Após avançar, é mostrado uma tela com todas as configurações selecionadas, ao confirmar, instalar.

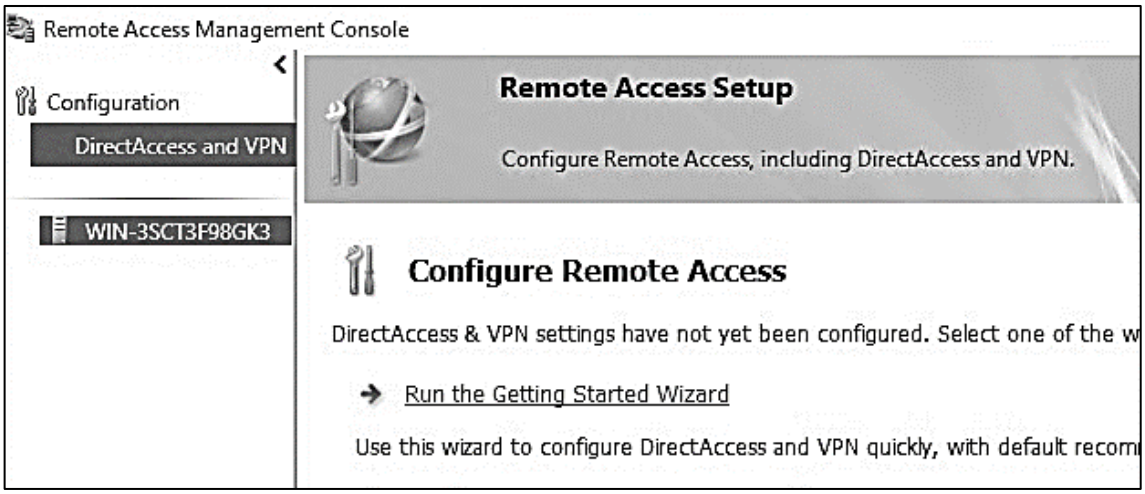
Figura 47: Instalando serviços de VPN e roteamento



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

3 – Em ferramentas, no gerenciador de servidores, pode ser encontrado o gerenciamento de acesso remoto. Ao abrir, clicar em DirectAccess e VPN. É mostrada a tela de configurações de acesso remoto, clicar em “Executar o assistente do guia de introdução”, mostrado na Figura 48.

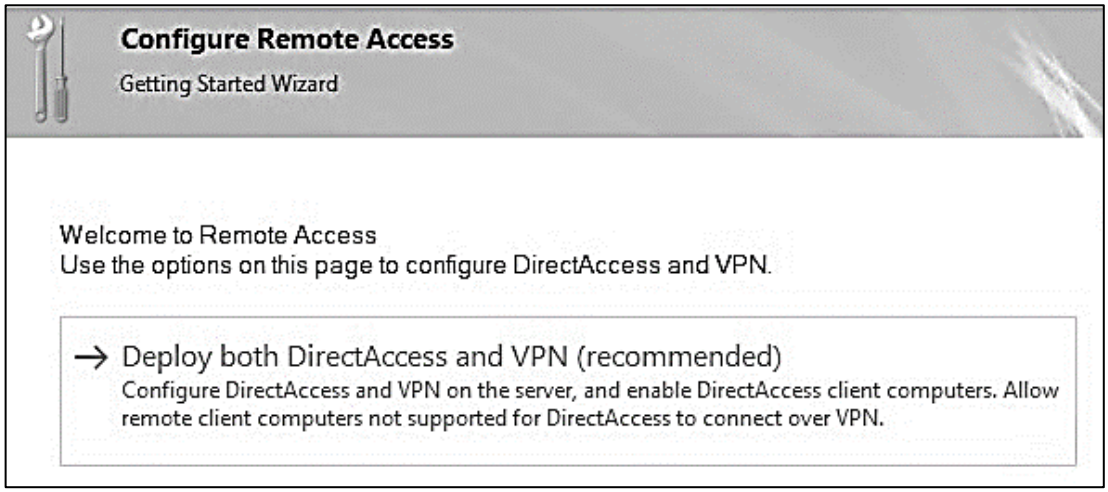
Figura 48: Configurando o Acesso Remoto



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

4 – É aberto o assistente, escolhe-se a opção de implantar DirectAccess e VPN (recomendado), conforme a Figura 49.

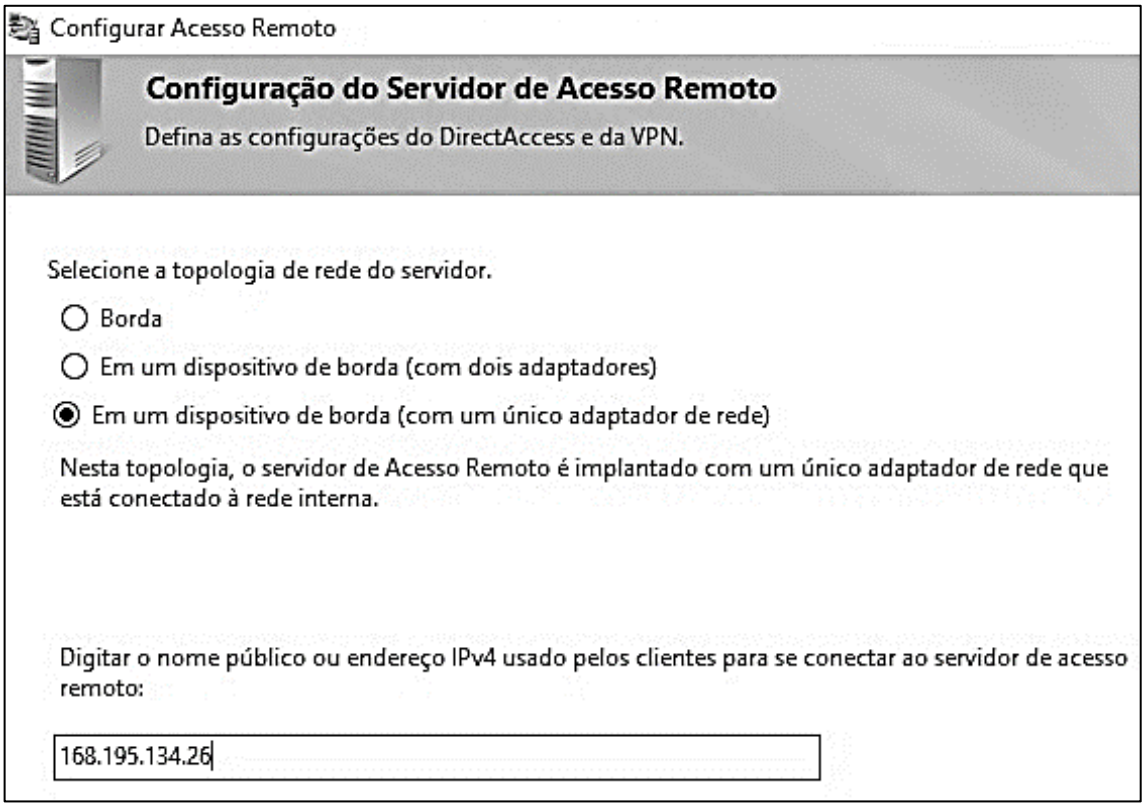
Figura 49: Implantando DirectAccess e VPN



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

5 – Inicialmente pode ser colocado um endereço de IP fixo para a VPN, como mostrado na Figura 50 e avançar. Este endereço pode ser consultado através do comando “ipconfig” no prompt de comando.

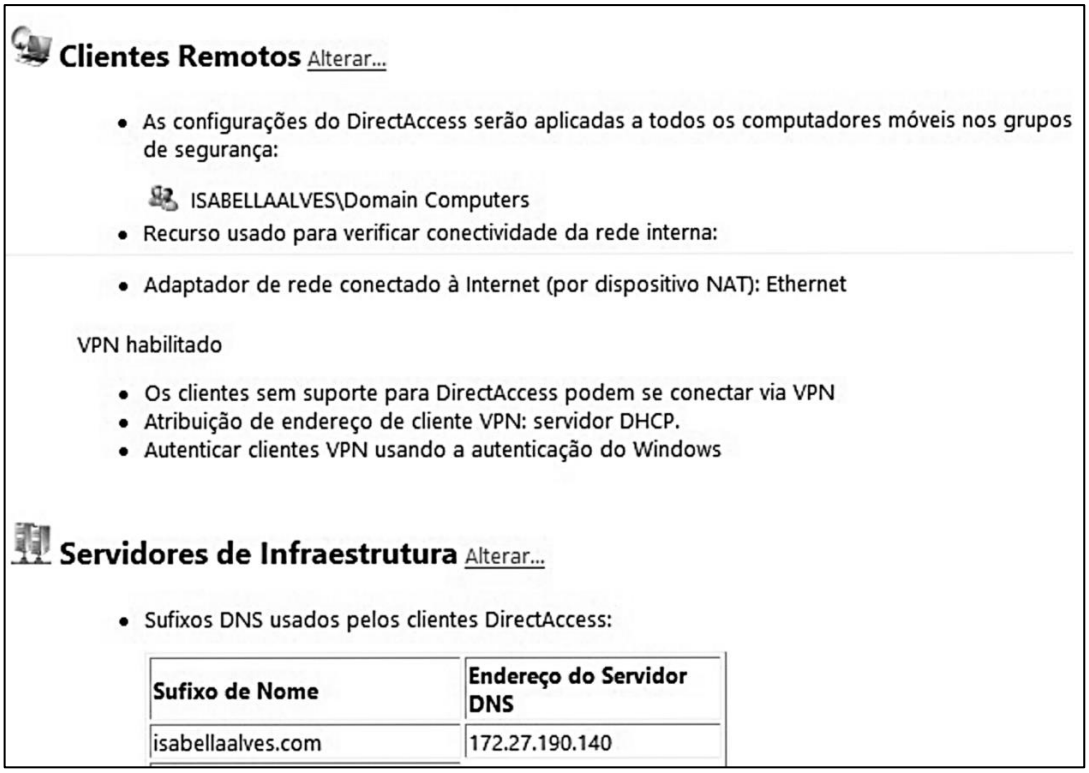
Figura 50: Definindo, inicialmente um IP fixo para a VPN



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

6 – As configurações que são aplicadas podem ser consultadas clicando em “aqui”. Na Figura 51 são mostradas todas as configurações definidas para a VPN. Clicar em “Ok” e “Concluir”.

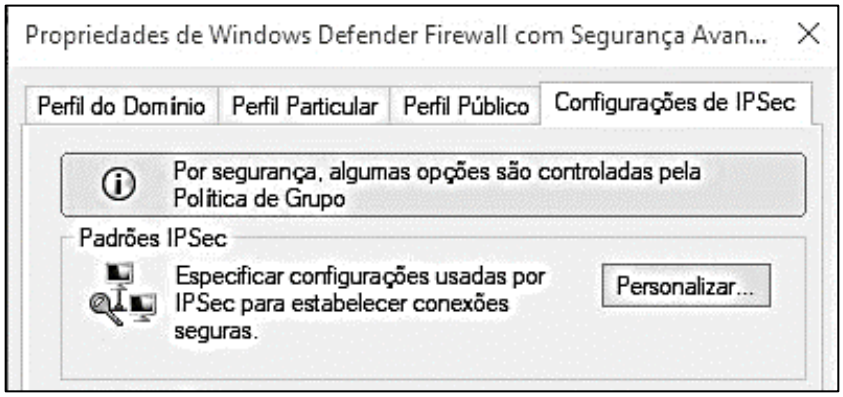
Figura 51: Verificando as configurações a serem aplicadas.



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

7 – Após a instalação, é necessário a criação de uma regra de segurança de conexão no *Firewall*, para o IPsec. Para verificar as configurações do IPsec, no menu iniciar digita-se “Windows Defender *Firewall* com Segurança Avançada”. Ao abrir, clicar com o botão direito do *mouse* em cima do nome “Windows Defender *Firewall* com Segurança Avançada” e abrir “Propriedades. Ao clicar na aba “Configurações de IPsec” É mostrada a tela da Figura 52. O próximo passo está em “Personalizar”, abre-se uma nova tela e clicar em “Personalizar” novamente.

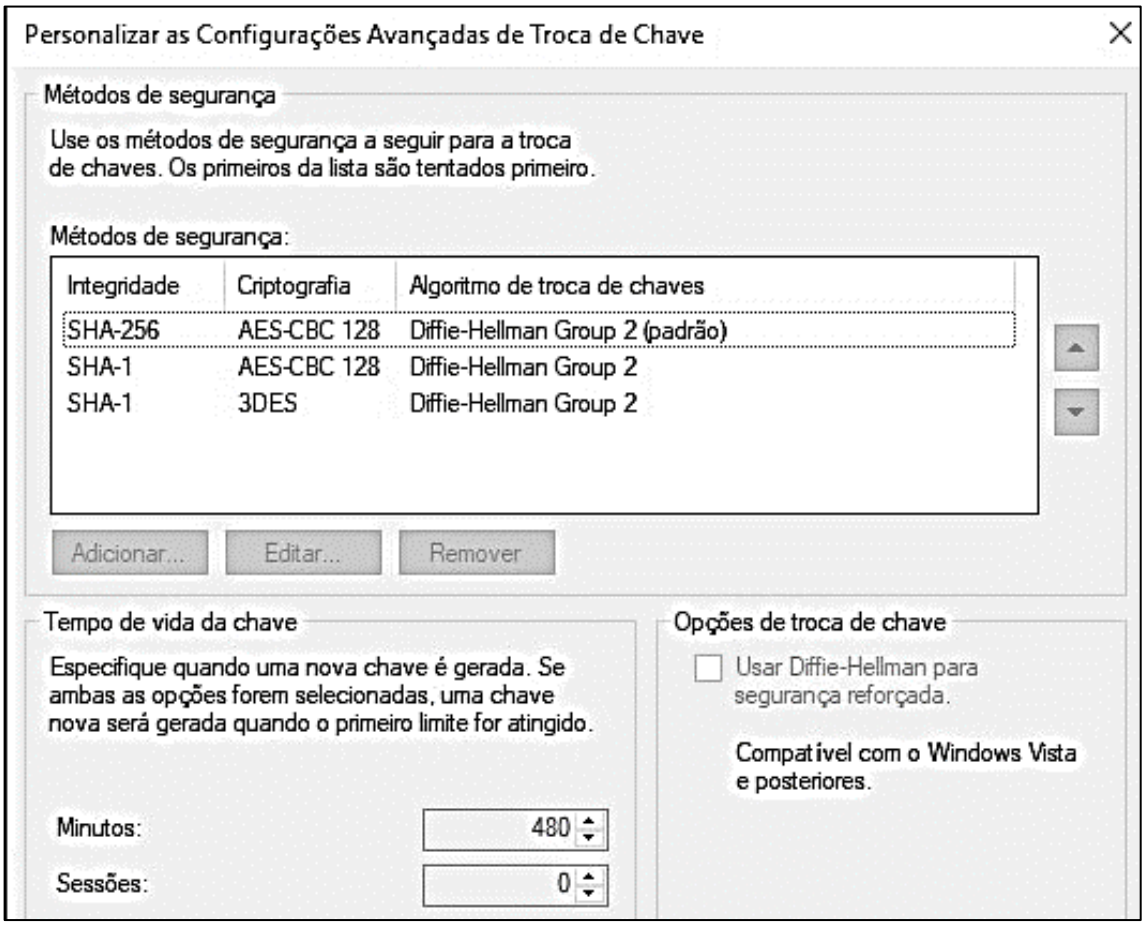
Figura 52: Propriedades do Windows Defender *Firewall* com Segurança Avançada.



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

8 – É aberta a tela da Figura 53, onde pode ser observado as configurações do algoritmo utilizado pelo IPsec para que haja segurança na troca de dados.

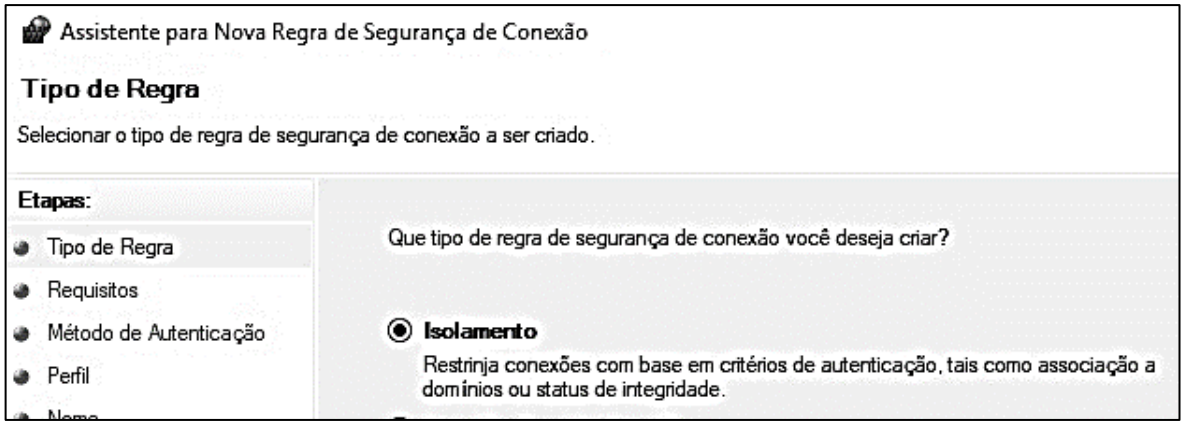
Figura 53: Configurações do IPSec



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

9 – Após ter verificado as configurações do IPsec, todas as janelas de propriedades podem ser fechadas. Ao lado esquerdo da tela do *Firewall*, clicar em “Regras de Segurança de Conexão”. Abre-se um assistente para criar uma regra, mostrada na Figura 54. Seleciona-se a opção “Isolamento” e clicar em “Avançar”.

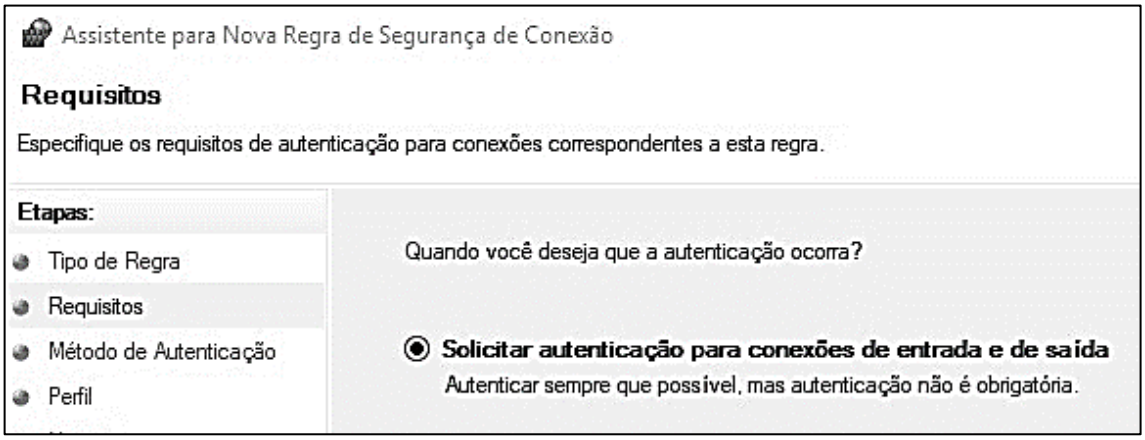
Figura 54: Criando Regra de Segurança de Conexão



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

10 – O próximo passo é definir o requisito para que ocorra a autenticação na conexão. Selecionar “Solicitar autenticação para conexões de entrada e de saída” como mostrado na Figura 55 e avançar.

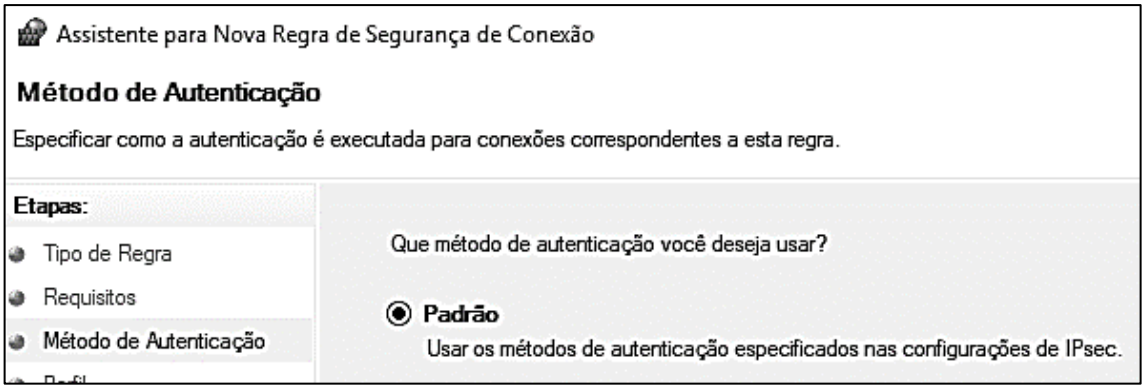
Figura 55: Definindo os requisitos da autenticação



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

11 – O próximo passo é definir o método de autenticação. Nesse trabalho foi escolhido o método padrão que estão especificados nas configurações do IPsec, como mostrado na Figura 56. Logo após avançar.

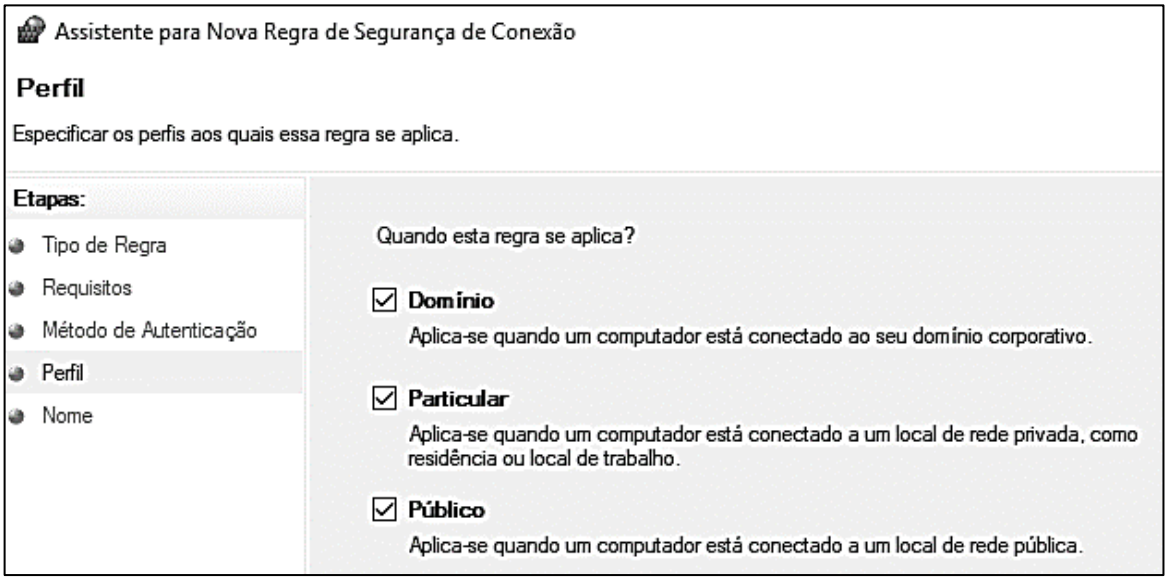
Figura 56: Definindo o método de autenticação



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

12 – O próximo passo é especificar quando a regra se aplica. Nesse caso, foi selecionado para ser aplicada em todos os perfis, conforme mostrado na Figura 57.

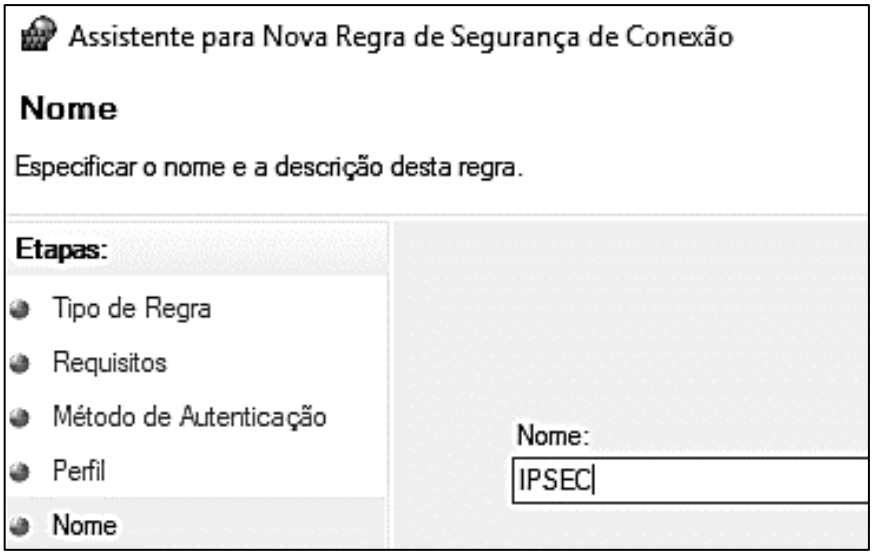
Figura 57: Selecionando os perfis de aplicação da Regra



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

13 – Ao avançar, é necessário atribuir um nome a regra. Nesse caso, atribuiu-se o nome IPSec, como mostrado na Figura 58. Após colocar o nome, clicar em “Concluir”, e a regra é criada.

Figura 58: Dando nome a Regra

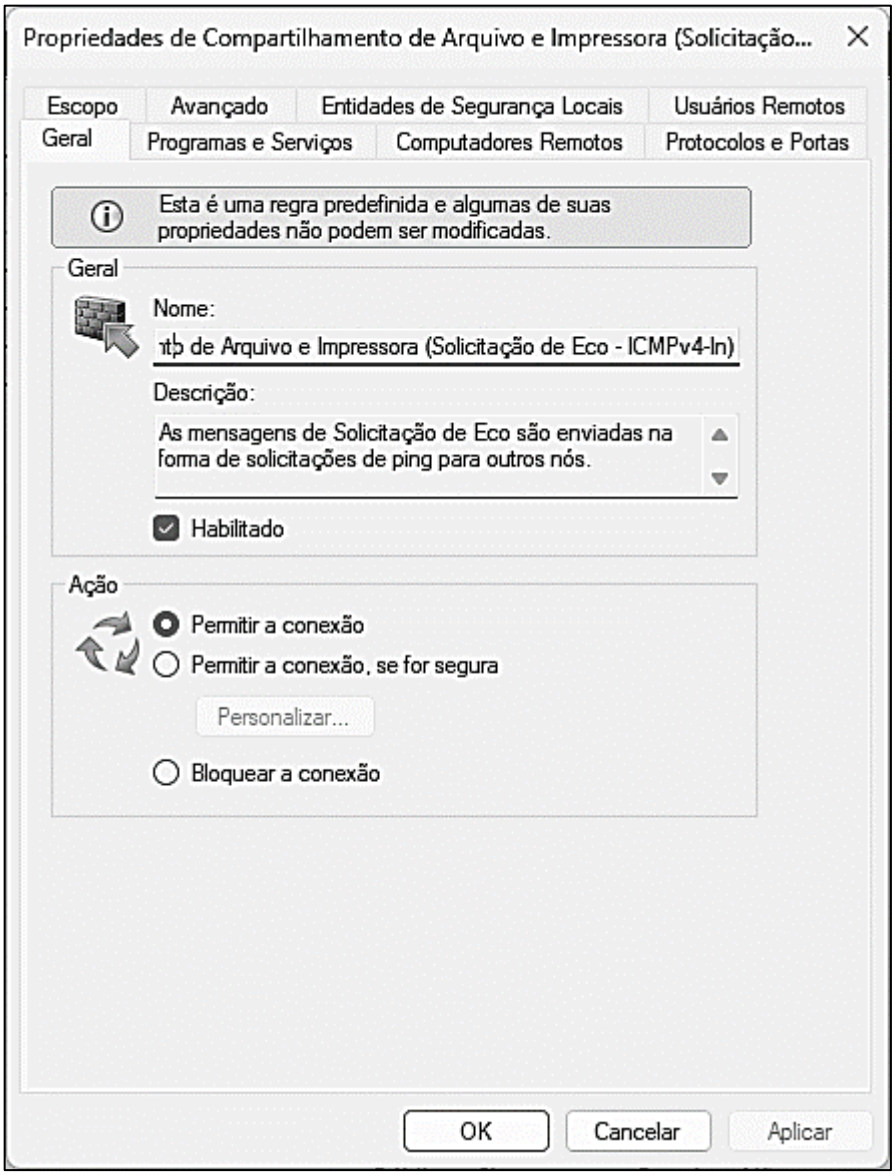


Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2019.

APÊNDICE IV – INSTALAÇÃO DO CLIENTE VPN

1 – Na máquina física do usuário, no menu iniciar digita-se “Windows Defender *Firewall* com Segurança Avançada”, na lateral esquerda clicar em “Regras de Entrada” e procurar por “Compartilhamento de Arquivo e Impressora (Solicitação de ECO – ICMPv4 -In). Ao clicar duas vezes, é aberta a tela de propriedades, como mostrado na Figura 59. Verificar se a opção “Habilitado” está marcada, caso não esteja, selecionar e aplicar.

Figura 59: Habilitando Solicitação de Eco ICMPv4

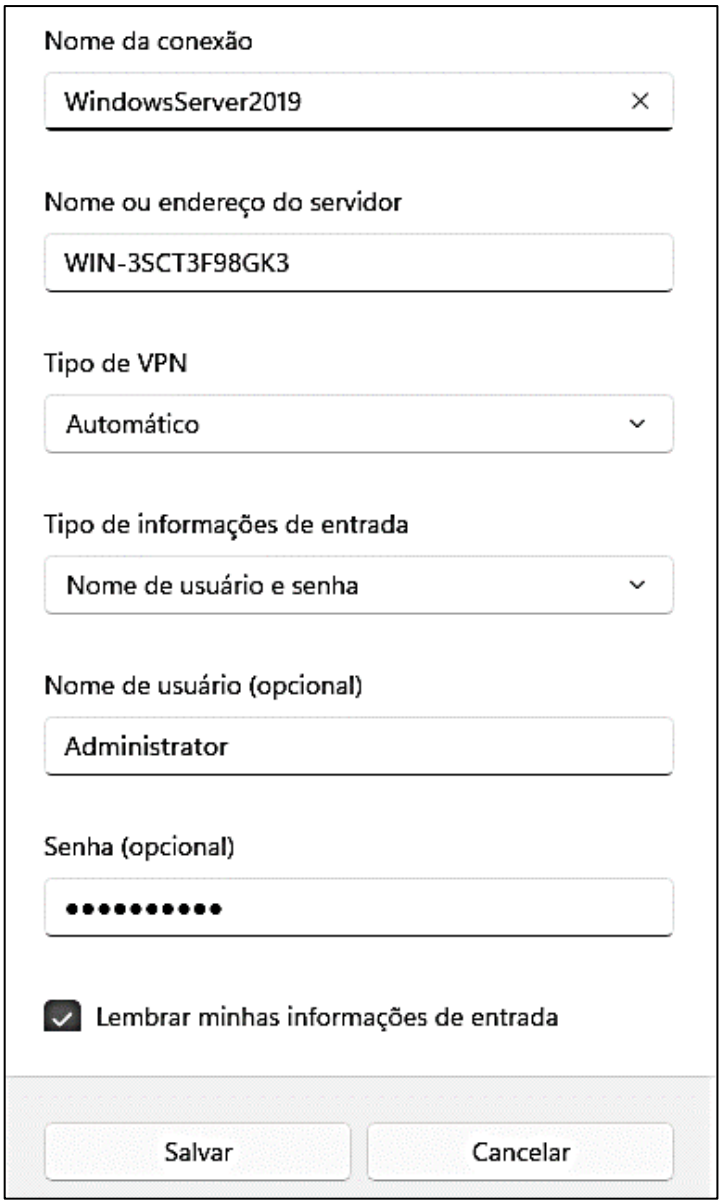


Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

2 – São encontradas duas regras de entrada com o mesmo nome, é desejável habilitar as duas. Nas Regras de Saída também é necessário procurar pelas mesmas regras e habilitá-las.

3 – Após as regras habilitadas, no menu iniciar procurar por “Configurações de VPN” e abrir. Aparece uma tela de conexões VPN, clicar em adicionar VPN. É aberta a tela mostrada na Figura 60, onde se deve colocar o nome da conexão que é a escolha do usuário, colocado o nome ou endereço do servidor, o nome de usuário e a senha de acesso. Nesse trabalho foram colocados o nome da conexão “WindowsServer2019” e o nome do servidor. Clicar em Salvar.

Figura 60: Conectando à VPN



Fonte: Imagem capturada pela autora do trabalho em MICROSOFT, 2023c.

4 – A conexão VPN é criada, clicar em conectar e tem-se acesso as pastas compartilhadas do servidor.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Isabella Alves Carvalho
do Curso de Engenharia de Computação, matrícula 2016.1.0033.0076-2,
telefone: (62) 99570-6773 e-mail isabellac98@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Utilização da VPN no cenário de teletrabalho, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 21 de setembro de 2023.

Assinatura do(s) autor(es): Isabella Alves Carvalho

Nome completo do autor: Isabella Alves Carvalho

Assinatura do professor-orientador:

Nome completo do professor-orientador: Angélica da Silva Nunes