



**UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DO TOCANTINS/CAMETÁ
FACULDADE DE SISTEMAS DE INFORMAÇÃO**

CAIO CORRÊA GAIA

**SERVIDOR NAS DOMÉSTICO: UMA SOLUÇÃO DE ARMAZENAMENTO E
BACKUP PARA USO PESSOAL**

**CAMETÁ
2026**



**UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DO TOCANTINS/CAMETÁ
FACULDADE DE SISTEMAS DE INFORMAÇÃO**

CAIO CORRÊA GAIA

**SERVIDOR NAS DOMÉSTICO: UMA SOLUÇÃO DE ARMAZENAMENTO E
BACKUP PARA USO PESSOAL**

Trabalho de Conclusão de Curso
apresentado para obtenção do grau de
Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Allan Barbosa Costa

CAMETÁ
2026

CAIO CORRÊA GAIA

**SERVIDOR NAS DOMÉSTICO: UMA SOLUÇÃO DE ARMAZENAMENTO E
BACKUP PARA USO PESSOAL**

Trabalho de Conclusão de Curso
apresentado para obtenção do grau de
Bacharel em Sistemas de Informação.

Banca Examinadora

Prof. Dr. Allan Barbosa Costa

Faculdade de Sistemas de Informação - UFPA Orientador

Prof. Dr. Carlos dos Santos Portela

Faculdade de Sistemas de Informação - UFPA

Prof. Dr. Ulisses Weyl da Cunha Costa

Faculdade de Sistemas de Informação - UFPA

CAMETÁ
2026

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

C824s Corrêa Gaia, CAIO.
 SERVIDOR NAS DOMÉSTICO: UMA SOLUÇÃO DE
 ARMAZENAMENTO E BACKUP PARA USO PESSOAL /
 CAIO Corrêa Gaia. — 2026.
 38 f. : il. color.

Orientador(a): Prof. Dr. Allan Barbosa Costa
Trabalho de Curso (Graduação) - Universidade Federal do Pará,
Campus Universitário de Cametá, Curso de Sistemas de
Informação, Cametá, 2026.

1. Armazenamento em rede. I. Título.

CDD 004

AGRADECIMENTOS

Primeiramente, agradeço a Deus, por me conceder saúde, sabedoria, força e perseverança para enfrentar cada desafio ao longo desta caminhada acadêmica. Sem Sua presença em minha vida, nada disso seria possível.

À minha mãe, Maria Isabel Furtado Corrêa, expresso minha mais profunda gratidão por todo o amor, dedicação, incentivo e apoio incondicional. Obrigado por acreditar em mim, pelos ensinamentos, pelos conselhos e por nunca medir esforços para que eu pudesse alcançar meus objetivos. Ao meu pai, Benedito de Souza Gaia, agradeço por todo o apoio, pelos valores que me transmitiu e por sempre me incentivar a seguir em frente, mesmo diante das dificuldades. Sua contribuição foi essencial para que eu chegasse até aqui. À meu irmão, Leonardo, e à Leudiane, agradeço pelo carinho, pela amizade, pela compreensão e por estarem presentes em tantos momentos importantes da minha vida. O apoio de vocês tornou essa jornada muito mais leve.

À minha namorada, Raynara, deixo um agradecimento especial por todo o amor, paciência, compreensão e incentivo durante este percurso. Obrigado por permanecer ao meu lado nos momentos de alegria e também nas fases mais desafiadoras, sempre acreditando no meu potencial e me motivando a nunca desistir. Ao meu grande amigo, Edinaldo, minha sincera gratidão pela amizade verdadeira, pelas palavras de incentivo, pelas conversas, pelo companheirismo e por todo o apoio oferecido durante essa caminhada. Sua presença fez toda a diferença em diversos momentos.

Agradeço também a todos os meus familiares, que de alguma forma contribuíram para minha formação, seja por meio de palavras de incentivo, apoio ou orações. Cada gesto de carinho e confiança foi importante para que eu pudesse seguir em frente.

Por fim, registro meu profundo agradecimento a todos os professores que fizeram parte da minha trajetória acadêmica. Cada um contribuiu significativamente para minha formação profissional e pessoal, compartilhando conhecimentos, experiências e valores que levarei por toda a vida. Em especial, agradeço pela dedicação, pela paciência e pelo compromisso com o ensino, fundamentais para a construção deste trabalho e para a conclusão desta importante etapa da minha vida. A todos que, direta ou indiretamente, contribuíram para a realização deste sonho, deixo meu mais sincero muito obrigado. Esta conquista não é apenas minha, mas de todos que caminharam ao meu lado e acreditaram que este momento seria possível.

RESUMO

O crescimento na produção de dados digitais pessoais contrasta com a crescente perda de soberania do usuário frente aos modelos monopolistas de nuvem pública e às limitações de infraestrutura das redes domésticas brasileiras, marcadas pelo mecanismo de CGNAT. Diante disso, este Trabalho de Conclusão de Curso apresenta o desenvolvimento e a homologação técnica de um servidor NAS (*Network Attached Storage*) residencial de baixo custo, estruturado a partir do reaproveitamento de hardware, a pesquisa caracteriza-se como um estudo aplicado e experimental, ancorado na implementação do sistema operacional TrueNAS Scale e do sistema de arquivos OpenZFS em arranjo de espelhamento (*mirroring*) para garantir a integridade contra a corrupção silenciosa de dados. Para o isolamento perimetral imposto pelas operadoras de internet, integrou-se uma camada de rede sobreposta via Tailscale, baseada no protocolo WireGuard, viabilizando a travessia de NAT (*NAT traversal*) de forma transparente e segura, sem custos adicionais com IPs públicos dedicados. A automação das rotinas de salvaguarda foi validada em segundo plano em dispositivos móveis através do aplicativo FolderSync, enquanto o acesso remoto dos arquivos foi operado via protocolo SMB pelo CX Explorador de Arquivos. Os resultados demonstraram a estabilidade em redes móveis (4G/5G), taxas de transferência condizentes com o link residencial e a total eliminação de processos manuais de backup. Conclui-se que a proposta se consolida como uma alternativa viável e de baixo custo para o uso pessoal.

Palavras-chave: Armazenamento em rede; Nuvem privada; TrueNAS Scale; Tailscale; CGNAT.

ABSTRACT

The growth in the production of personal digital data contrasts with the increasing loss of user sovereignty in the face of monopolistic public cloud models and the infrastructure limitations of Brazilian domestic networks, which are marked by the CGNAT mechanism. Therefore, this undergraduate thesis presents the development and technical validation of a low-cost residential NAS (Network Attached Storage) server, structured from repurposed hardware. The research is characterized as an applied and experimental study, anchored in the implementation of the TrueNAS Scale operating system and the OpenZFS file system in a mirroring array to ensure data integrity against silent corruption. To overcome the perimeter isolation imposed by internet service providers, an overlay network layer was integrated via Tailscale, based on the WireGuard protocol. This enabled transparent and secure NAT traversal without the additional costs of dedicated public IPs. The automation of backup routines was validated in the background on mobile devices using the FolderSync application, while remote file access was operated via the SMB protocol through CX File Explorer. The results demonstrated stability on mobile networks (4G/5G), transfer rates consistent with residential internet links, and the complete elimination of manual backup processes. It is concluded that the proposal is consolidated as a viable and low-cost alternative for personal use.

Keywords: Network attached storage; Private cloud; TrueNAS Scale; Tailscale; CGNAT.

LISTA DE ILUSTRAÇÕES

Figura 1 – Discos Rígidos (HDs)	25
Figura 2 – Memória RAM	26
Figura 3 – Placa de Vídeo	26
Figura 4 – Placa-Mãe	27
Figura 5 – Processador	28
Figura 6 – Fonte de Alimentação	28
Figura 7 – Gabinete	29
Figura 8 – Diagrama da Solução Proposta	30
Figura 9 – Tela da interface inicial do servidor	32
Figura 10 – Dashboard do TrueNAS	32
Figura 11 – Interface do TrueNAS em dispositivo móvel	32
Figura 12 – Acesso ao servidor pelo navegador Brave	32
Figura 13 – Estrutura física do servidor NAS	33
Figura 14 – Sistema de armazenamento em espelhamento (Mirror)	33
Figura 15 – Setup completo do ambiente NAS	33
Figura 16 - Interface inicial do aplicativo Cx Explorador de Arquivos ...	34
Figura 17 – Tela de acesso ao Nas	34
Figura 18 – Usuario Configurado	34
Figura 19 – Pastas do Usuario no NAS	34
Figura 20 – Interface da sincronização automática	35

LISTA DE ABREVIATURAS E SIGLAS

BIOS	Basic Input/Output System
CGNAT	Carrier Grade Network Address Translation
CID	Confidencialidade, Integridade e Disponibilidade
CPU	Central Processing Unit
DDR	Double Data Rate
DNS	Domain Name System
GPU	Graphics Processing Unit
HD	Hard Disk Drive
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
OpenZFS	Open Zettabyte File System
RAID	Redundant Array of Independent Disks
RAID-Z	Redundant Array of Independent Disks – ZFS
RAM	Random Access Memory
SAN	Storage Area Network
SMB	Server Message Block
TCP/IP	Transmission Control Protocol / Internet Protocol
TI	Tecnologia da Informação
USB	Universal Serial Bus
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
ZFS	Zettabyte File System

Sumário

1	INTRODUÇÃO	11
1.1	CONTEXTO	12
1.2	JUSTIFICATIVA.....	12
1.3	OBJETIVOS	15
2	REFERENCIAIS TEÓRICOS	16
2.1	ARMAZENAMENTO DE DADOS EM REDE	16
2.2	SERVIDORES NAS (NETWORK ATTACHED STORAGE).....	16
2.3	BACKUP E SEGURANÇA DA INFORMAÇÃO.....	17
2.4	ACESSO REMOTO E REDES VPN.....	17
2.5	COMPARAÇÃO ENTRE SERVIÇOS COMERCIAIS DE ARMAZENAMENTO EM NUVEM.....	18
3	TRABALHOS RELACIONADOS	18
4	METODOLOGIA.....	20
4.1	SOFTWARES UTILIZADOS	24
4.2	FERRAMENTAS DE HARDWARE	25
4.3	DIAGRAMA DA SOLUÇÃO UTILIZADA.....	30
5	RESULTADOS.....	30
6	CONCLUSÃO.....	35
	REFERÊNCIA	38

1 INTRODUÇÃO

A nossa relação com a tecnologia mudou drasticamente nos últimos anos. Vivemos uma fase em que a produção de dados se tornou uma ação quase involuntária no nosso dia a dia. Toda vez que tiramos uma foto em alta resolução, gravamos um vídeo ou salvamos uma nova versão de um documento de trabalho, estamos alimentando um volume de informações digitais que não para de crescer, impulsionado pelo avanço da internet e dos dispositivos móveis (Tanenbaum; Bos, 2023). Essa facilidade de gerar conteúdo esconde um problema silencioso com o qual todo mundo acaba esbarrando uma hora ou outra: onde e como vamos guardar tudo isso com segurança a longo prazo?

Historicamente, a saída mais comum para usuários domésticos sempre foi recorrer a pendrives e discos rígidos externos. No entanto, o desgaste físico cobra seu preço. É exatamente por conta dessa fragilidade que os serviços de armazenamento em nuvem, como o Google Drive, Google Fotos e TeraBox, ganharam tanto espaço de forma tão rápida, tornando-se a solução padrão de mercado. A grande questão é que a nuvem não é isenta de falhas ou limitações. Embora entregue muita praticidade na palma da mão, ela cria uma dependência financeira contínua devido aos custos recorrentes, exigência de internet constante e levanta questionamentos cada vez mais sérios sobre a privacidade e a verdadeira propriedade dos nossos dados (Buyya, 2021).

É justamente nesse contexto de dependência que a ideia de ter um servidor NAS (Network Attached Storage) dentro de casa deixa de ser um equipamento exclusivo de empresas de TI e passa a ser uma alternativa real, acessível e extremamente eficiente para o usuário comum (NEGUS, 2021). Um servidor NAS nada mais é do que um dispositivo conectado diretamente na rede local da residência, permitindo o armazenamento, o compartilhamento e a automação de backups de forma totalmente centralizada. Com as configurações adequadas e o uso integrado de redes virtuais (VPNs), o usuário consegue acessar seus arquivos remotamente com enorme controle e disponibilidade (Stallings, 2022).

Diante disso, este trabalho tem como proposta central apresentar o servidor NAS doméstico como uma solução viável para organizar da melhor forma nossos dados. A ideia é mostrar de forma prática os conceitos básicos, o funcionamento do sistema e analisar sua aplicação em um ambiente residencial, provando que é possível proteger nosso patrimônio de dados de forma autônoma e segura.

1.1 CONTEXTO

Para entender o verdadeiro impacto e a utilidade de um projeto como este, basta observar a rotina frustrante da grande maioria das pessoas que possuem um smartphone hoje. Receber aquele temido aviso de "armazenamento cheio" no meio de uma viagem ou durante um evento importante virou uma dor de cabeça constante. A partir do momento em que a memória física do celular ou do notebook lota, o caminho mais rápido imposto pela indústria de tecnologia é o aluguel de espaço digital nas plataformas de nuvem amplamente conhecidas (Tanenbaum; Bos, 2023).

Acabamos normalizando a ideia de assinar pacotes mensais para não perder nossos trabalhos acadêmicos e documentos pessoais que possuem imenso valor sentimental e funcional. No entanto, ao aceitarmos o que o mercado impõe, entregamos nossa privacidade para serviços terceirizados, ficando completamente sujeitos a vazamentos e interrupções de serviço (Buyya, 2021). Apesar da vontade de construir uma nuvem particular ser algo que atrai muita gente, sempre existiu um obstáculo técnico muito frustrante pelo caminho o CGNAT. Para mitigar o esgotamento de endereços na internet, as operadoras passaram a utilizar em massa uma tecnologia chamada CGNAT (Carrier Grade Network Address Translation), que dificulta imensamente as conexões externas diretas em redes domésticas (Kurose; Ross, 2021). Isso simplesmente mudou a internet como ela foi planejada originalmente. Se você tentasse abrir uma porta no seu roteador para acessar o seu próprio servidor de fora de casa, a conexão batia na barreira da operadora e se perdia.

Felizmente, as ferramentas de software evoluíram rápido o suficiente para contornar isso. O amadurecimento de sistemas de armazenamento em rede e inovações incríveis em túneis de VPN viraram esse jogo completamente, permitindo maior controle e segurança das informações (Stallings, 2022). Hoje, o cenário tecnológico finalmente alinhrou as peças que faltavam para democratizar as nuvens privadas em nossas casas.

1.2 JUSTIFICATIVA

Para compreender a real necessidade e a urgência de um projeto como este, precisamos primeiro olhar para a forma como a nossa relação com as memórias e com o trabalho se transformou. Se pararmos para pensar, grande parte da nossa vida hoje existe de forma intangível. Nossos álbuns de família não estão mais revelados em gavetas, nossos documentos de identidade são digitais, e nossos trabalhos acadêmicos e profissionais são sequências de bits. A quantidade de dados digitais produzidos

diariamente por um único indivíduo hoje supera, de longe, o que uma família inteira produzia há dez anos (Tanenbaum; Bos, 2023). O smartphone deixou de ser apenas um meio de comunicação para se tornar o principal repositório da história de vida das pessoas. No entanto, essa facilidade imensa de registrar tudo em vídeos e fotos de alta resolução trouxe uma consequência pesada: a exaustão rápida e constante do espaço de armazenamento físico dos nossos aparelhos. É neste exato ponto que o usuário comum se vê encurralado, e é aqui que a relevância deste trabalho começa a se desenhar.

A saída imediata oferecida pela indústria de tecnologia para esse problema de espaço foi a nuvem pública. No início, ela foi vendida como uma solução quase mágica e gratuita. Contudo, a grande verdade é que o armazenamento em nuvem se transformou em um dos modelos de negócio mais lucrativos e implacáveis da atualidade. Quando o limite gratuito de uma conta do Google ou da Apple se esgota, o usuário é praticamente forçado a assinar um plano mensal para não perder a capacidade de receber e-mails ou fazer o backup de suas fotos.

O que muita gente não percebe é que essa assinatura cria um ciclo de dependência financeira vitalício. Pagar trinta ou cinquenta reais por mês pode parecer inofensivo a curto prazo, mas, se colocarmos na ponta do lápis, estamos falando de milhares de reais ao longo dos anos. É um modelo de "aluguel digital" onde você nunca é dono do espaço (Buyya, 2021). A implementação de um servidor NAS (Network Attached Storage) dentro do ambiente doméstico justifica-se, antes de tudo, como uma decisão de inteligência econômica. Com um investimento inicial único em discos rígidos, o usuário se liberta completamente das mensalidades, transformando um gasto passivo e infinito em um ativo tecnológico próprio. Mas a justificativa para fugir das nuvens comerciais vai muito além do aspecto financeiro; ela esbarra em um pilar fundamental da nossa sociedade moderna: a privacidade.

Estamos atravessando a era da mineração de dados e do treinamento de Inteligências Artificiais. Quando subimos nossas fotos, contratos, projetos e planilhas financeiras para os servidores de grandes corporações, nós aceitamos Termos de Serviço que mudam unilateralmente e que, muitas vezes, dão a essas empresas o direito de escanear, catalogar e utilizar nosso conteúdo para treinar seus algoritmos (Stallings, 2022). A sensação de propriedade sobre o próprio arquivo se perde na nuvem. Montar um servidor NAS devolve ao usuário o que chamamos de "soberania digital". Ter o HD rodando fisicamente dentro da sua própria casa, conectado à tomada da sua sala, traz uma garantia inegociável de que ninguém, absolutamente ninguém, além de você mesmo ou

de quem você autorizar, terá acesso ao que está armazenado ali. É uma retomada de controle que se faz cada vez mais necessária em tempos de hipervigilância.

Se ter um NAS em casa é tão vantajoso economicamente e tão seguro do ponto de vista da privacidade, surge uma pergunta natural: por que isso já não é o padrão na casa de todas as pessoas? A resposta para isso justifica o núcleo técnico deste Trabalho de Conclusão de Curso, historicamente, montar um servidor em casa esbarrava em uma barreira de infraestrutura de rede extremamente frustrante. Para que você conseguisse acessar o seu servidor doméstico estando na rua, pelo 4G, seu roteador precisava de um endereço IP público válido. O problema é que esses endereços (no padrão IPv4) se esgotaram mundialmente. Para resolver isso, os provedores de internet brasileiros passaram a colocar bairros inteiros atrás de uma tecnologia chamada CGNAT (Carrier Grade Network Address Translation) (Kurose; Ross, 2021).

De forma simples, o CGNAT funciona como a portaria de um prédio gigantesco: a internet sabe como chegar até a portaria do seu provedor, mas não consegue entregar o pacote diretamente no roteador do seu "apartamento" porque o seu endereço não é único. Isso inviabilizava a abertura de portas. Projetos de servidores caseiros acabavam abandonados porque o usuário só conseguia acessar seus arquivos se estivesse conectado no Wi-Fi de casa, o que matava o propósito da mobilidade.

Este trabalho se justifica e ganha um peso enorme justamente por provar que esse obstáculo técnico foi superado. Ao invés de aceitarmos essa limitação do CGNAT ou pagarmos taxas abusivas para os provedores nos fornecerem um IP fixo, este projeto demonstra a eficácia de utilizar tecnologias modernas de rede virtual privada (VPN), especificamente o Tailscale (Tailscale, 2025; Silva, 2021). Ao integrar túneis criptografados baseados no protocolo WireGuard, conseguimos literalmente perfurar o bloqueio das operadoras. A pesquisa não fica apenas na teoria; ela documenta e valida um roteiro prático para que qualquer leigo consiga conectar seu celular de forma direta e segura ao seu servidor, de qualquer lugar do mundo, provando que o acesso remoto fluido finalmente foi democratizado (Sampaio, 2022). Além das justificativas econômicas, de privacidade e da superação das barreiras de rede, é impossível não destacar o forte apelo sustentável e de consciência ecológica desta pesquisa.

Vivemos uma crise global de descarte de lixo eletrônico (e-waste). Computadores que ficam "lentos" para rodar jogos ou sistemas operacionais pesados modernos são sumariamente descartados no lixo ou esquecidos em armários, mesmo com processadores

e placas mãe perfeitamente funcionais. Este trabalho mostra que o TrueNAS Scale, um sistema operacional focado exclusivamente em gerenciamento de armazenamento, consegue extrair um desempenho absurdo de hardwares antigos ou reaproveitados (Ixsystems, 2024). Dar uma sobrevida a esses equipamentos, transformando o que seria sucata em um servidor de arquivos de altíssima confiabilidade e redundância, é uma atitude responsável e ecologicamente inteligente (Sousa; Neves, 2025). O projeto prova que você não precisa comprar o servidor mais caro da loja de informática para proteger seus dados.

Por fim, a justificativa deste TCC se consolida no seu valor educacional e prático. Enquanto muitos trabalhos acadêmicos orbitam o campo das ideias abstratas, este estudo entrega uma solução arquitetada para resolver um problema real, diário e estressante. Configurar uma rotina onde um smartphone sincroniza suas fotos automaticamente (usando ferramentas como o FolderSync), sem depender de cliques manuais, e saber que esses arquivos estão sendo enviados diretamente para um sistema robusto que previne falhas físicas (graças ao sistema de arquivos ZFS). Portanto, este trabalho não é apenas um manual de configuração de software; ele é a prova técnica de que o cidadão comum tem, hoje, todas as ferramentas necessárias para construir e gerir sua própria infraestrutura de dados com segurança, independência e excelência.

1.3 OBJETIVOS

Objetivo Geral

Desenvolver e implementar um servidor NAS (Network Attached Storage) em ambiente doméstico, com a finalidade de oferecer uma solução eficiente para o armazenamento centralizado e a realização de backups automatizados de dados pessoais, visando garantir maior segurança, controle, disponibilidade das informações e viabilizar o acesso remoto, mesmo diante de limitações de infraestrutura de rede.

Objetivos Específicos

Entender como funciona o armazenamento em rede;

Montar um servidor NAS em casa;

Configurar o envio automático de arquivos;

Criar uma ponte segura para acessar os dados remotamente, driblando as limitações de rede como o CGNAT;

Verificar se o sistema funciona de forma estável e confiável.

2 REFERENCIAIS TEÓRICOS

2.1 ARMAZENAMENTO DE DADOS EM REDE

Olhando para trás, os métodos antigos de guardar coisas em HDs separados geravam muita confusão e dados duplicados (Kurose; Ross, 2021). Com o surgimento de tecnologias voltadas para rede, passamos a separar o mundo do armazenamento em duas grandes áreas: as redes SAN (Storage Area Network) e os famosos NAS (Network Attached Storage).

As redes SAN focam em transferências em altíssima velocidade no nível de blocos (usando Fibre Channel) e são feitas para o universo corporativo pesado (Lacerda; Soares; Lenz, 2022). Já o NAS é incrivelmente mais amigável, trabalhando na camada de arquivos e utilizando a boa e velha infraestrutura TCP/IP que já temos na nossa rede local (LAN) (Negus, 2021). O NAS age como um diplomata na rede: ele usa protocolos como o SMB/CIFS e o NFS para exibir uma pasta centralizada para todo mundo, de forma que o Windows, o celular e a TV enxerguem os arquivos como se estivessem dentro deles mesmos (Comer, 2021). Essa facilidade de comunicação universal transforma a forma como consumimos nossos próprios dados em casa (Forouzan, 2022).

2.2 SERVIDORES NAS (NETWORK ATTACHED STORAGE)

Um servidor NAS não é um computador comum; é uma máquina desenhada sob medida para compartilhar e preservar arquivos (Negus, 2021). A inteligência de um NAS moderno se apoia fortemente na união entre o hardware e o sistema de arquivos. Quando sistemas maravilhosos como o ZFS (Zettabyte File System) entraram em cena, o cenário mudou. O ZFS, utilizado no TrueNAS, não só guarda o arquivo, como verifica a integridade dele o tempo todo (usando checksums), protegendo nossas fotos daquela corrupção invisível e silenciosa dos discos mais antigos (Ixsystems, 2024; Patterson; Hennessy, 2021).

Outro recurso brutalmente essencial abordado nesse tipo de servidor é a redundância RAID (Redundant Array of Independent Disks) (STALLINGS, 2022). No universo do ZFS, usamos as lógicas de espelhamento ou RAID-Z, que garantem que, se um disco morrer fisicamente de uma hora para outra, o sistema continua rodando sem perder um byte sequer. Você troca o disco quebrado e o servidor se reconstrói sozinho.

2.3 BACKUP E SEGURANÇA DA INFORMAÇÃO

Qualquer conversa sobre dados precisa passar pela Tríade CID: Confidencialidade, Integridade e Disponibilidade (Stallings, 2022). Em um ambiente doméstico, perder um HD é quase uma tragédia anunciada se não houver preparo. A regra de ouro da indústria, defendida pelas cartilhas de segurança, é a estratégia 3-2-1: ter três cópias da sua informação, em duas mídias diferentes, sendo uma delas em um lugar físico diferente (Cert.br, 2024).

Ter um NAS em casa ajuda imensamente nessa automação, pois ele elimina aquele velho costume de "deixar para fazer backup amanhã" (Preston, 2022). A automação cuida do toda burocracia de ter que enviar manualmente, mas isso não exclui a necessidade de manter senhas fortes, segmentar quem acessa o quê e proteger os dados contra invasores externos (Sampaio, 2022).

2.4 ACESSO REMOTO E REDES VPN

O diferencial de qualquer nuvem privada é a capacidade de acessá-la do conforto de sua casa ou de um saguão de aeroporto. Anos atrás, a gente resolvia isso mexendo nas configurações de DNS dinâmico e portas do roteador, uma prática que deixava o servidor perigosamente exposto aos perigos da internet aberta (Kurose; Ross, 2021). Com a massificação do CGNAT pelas provedoras (que dividem o mesmo IP público para dezenas de casas), esse método manual simplesmente parou de funcionar na maioria das residências (Silva, 2021).

A mágica para resolver isso foi adotar túneis criptografados de VPN, especialmente as soluções modernas como o Tailscale (Tailscale, 2025). O Tailscale é especialista em criar uma ponte invisível e super protegida entre o seu celular e o seu servidor, furando os bloqueios de firewall e CGNAT das operadoras de forma espetacular. Sob a ótica de sistemas distribuídos, é como se os seus dispositivos espalhados pelo mundo sentassem magicamente na mesa da sua sala de estar para trocar arquivos com segurança (Tanenbaum; Van Steen, 2023).

2.5 COMPARAÇÃO ENTRE SERVIÇOS COMERCIAIS DE ARMAZENAMENTO EM NUVEM

Critério	Google Drive	OneDrive	Dropbox	TeraBox	NAS (TrueNAS SCALE)
Espaço gratuito	15 GB	5 GB	2 GB	1 TB	Conforme os discos
Expansão de armazenamento	Plano pago	Plano pago	Plano pago	Plano pago	Adição de discos
Sincronização automática	✓	✓	✓	✓	✓
Compartilhamento de arquivos	✓	✓	✓	✓	✓
Acesso remoto	✓	✓	✓	✓	✓
Controle de versões	✓	✓	✓	Limitado	✓ (Snapshots ZFS)
Controle físico dos dados	✗	✗	✗	✗	✓
Dependência do provedor	Alta	Alta	Alta	Alta	Baixa
Custo recorrente	Sim	Sim	Sim	Sim	Não
Privacidade dos dados	Média	Média	Média	Média	Alta

3 TRABALHOS RELACIONADOS

A literatura e a comunidade técnica vêm acompanhando o aumento gigantesco no volume de dados com muita curiosidade sobre o impacto disso no ambiente doméstico. O grande farol que iluminou muitas das escolhas feitas aqui foi o trabalho de Sousa e Neves (2025), chamado "Servidor NAS Residencial: Projeto, Implementação e

Benefícios Econômicos". Eles desenharam um servidor do zero usando hardwares convencionais e colocaram sob os holofotes a plataforma TrueNAS. Esse trabalho deixou muito claro que ter uma nuvem em casa não precisa custar uma fortuna e é um caminho inteligente para quem quer fugir das assinaturas caras de nuvem pública, especialmente reutilizando peças velhas de computador.

Ampliando a discussão sobre a proteção de arquivos no ambiente caseiro, a obra de Preston (2022), intitulada *Proteção Moderna de Dados*, serviu como um pilar fundamental para o nosso projeto. O autor realiza um estudo profundo sobre a importância de assegurar a capacidade de recuperação contra falhas sistêmicas e o esquecimento humano. O trabalho dele atesta que sistemas automatizados de cópia de segurança aumentam drasticamente as chances de recuperação em caso de falhas físicas dos aparelhos. Foi justamente baseando-nos nos cenários práticos apontados por Preston (2022) que justificamos a necessidade de implementar a rotina autônoma de sincronização com o aplicativo FolderSync neste TCC, tirando definitivamente a responsabilidade manual das costas do usuário.

Outro referencial recente que fundamenta fortemente essa visão de autonomia tecnológica é o estudo de Barbosa (2026). Embora o autor aborde o problema em uma escala governamental de interoperabilidade, sua pesquisa estabelece uma premissa que se aplica diretamente ao cenário desta monografia: a adoção de softwares de código aberto (*open-source*) e instâncias de nuvem privada é essencial para eliminar a dependência de infraestruturas compartilhadas de terceiros, que se tornam gargalos e pontos de vulnerabilidade na gestão da informação. O grande mérito da obra de Barbosa é sustentar, academicamente, que a soberania de dados jamais pode depender de um fornecedor proprietário. Esse embasamento valida o núcleo central deste TCC: ao construir o próprio servidor de arquivos, o usuário não está apenas economizando recursos de assinatura, mas retomando o controle jurisdicional, a privacidade e a verdadeira posse de seu patrimônio digital.

Já no campo da infraestrutura de rede, que é onde a maioria dos projetos de servidores residenciais esbarra e morre, o trabalho de Sampaio (2022) sobre a tecnologia VPN foi uma leitura obrigatória. Um dos maiores fantasmas de quem tenta montar um servidor em casa é o medo de abrir configurações no roteador e acabar sofrendo ataques virtuais, ou ser sumariamente barrado pelos bloqueios do provedor de internet. Sampaio detalha a criptografia de túneis de rede e aborda diretamente o uso de redes virtuais privadas

(VPNs) como a ferramenta mais segura e moderna para contornar esses bloqueios sem expor o hardware à internet pública.

A leitura dessa pesquisa foi o que nos deu o embasamento e a segurança técnica para fechar as portas de rede e apostar totalmente nos túneis criptografados do Tailscale para o nosso acesso remoto. Além dos estudos focados puramente em usuários residenciais, até mesmo as gigantes da tecnologia validam esse movimento do mercado. A própria IBM (2026) ressalta em seus relatórios técnicos que o conceito de NAS, antes algo que existia apenas dentro de datacenters fechados, se tornou uma ferramenta flexível que invadiu o ambiente corporativo e residencial de forma muito natural, impulsionada pela altíssima demanda por mídias digitais e pela facilidade de gerenciamento moderno.

Apesar de todas essas referências incríveis entregarem muita base teórica sobre como armazenar dados na rede local, a maioria delas acaba focando em pedaços isolados do problema: ou falam só do armazenamento em si, ou focam apenas no compartilhamento de arquivos localmente. Quase nenhuma delas mergulha fundo no problema prático do usuário comum, que é sincronizar automaticamente os arquivos do celular ao mesmo tempo em que precisa driblar os temidos roteadores bloqueados por CGNAT das operadoras de internet.

É exatamente aqui que este trabalho se desgarra e traz inovação: nós amarramos o poder bruto de armazenamento do TrueNAS Scale com a fluidez dos aplicativos móveis e fechamos a conta usando os túneis do Tailscale (via sub-rota) para quebrar as amarras do acesso remoto seguro. O grande diferencial e a contribuição direta desta pesquisa foi justamente costurar soluções de diferentes áreas para entregar um ecossistema blindado e 100% pronto para a vida real.

4 METODOLOGIA

A estrutura metodológica deste trabalho foi desenhada não apenas para validar conceitos teóricos extraídos de manuais clássicos de redes, mas para resolver um problema cotidiano na vida digital moderna. Por essa razão, a pesquisa caracteriza-se, em sua essência, como uma pesquisa aplicada e de forte caráter experimental, ancorada também em uma abordagem qualitativa na hora de avaliar os resultados finais, a escolha por uma pesquisa aplicada é amplamente justificada pela própria natureza do problema: a necessidade de desenvolver uma solução de engenharia de software e hardware que

fosse imediatamente útil, funcional e capaz de atender às demandas reais de armazenamento de uma residência (Negus, 2021).

Neste trabalho optou-se por utilizar simulações não virtuais, para assim construir de forma física/real um servidor NAS (Network Attached Storage) que fosse capaz de organizar o caos dos arquivos pessoais e, acima de tudo, libertar o usuário da dependência exclusiva e onerosa dos serviços de nuvem de terceiros (Buyya, 2021). O ponto de partida do projeto ocorreu por meio de uma rigorosa pesquisa bibliográfica intensiva e exploratória, antes de plugar o primeiro cabo de rede ou formatar o primeiro disco rígido, era fundamental compreender o "estado da arte" do armazenamento em rede e das arquiteturas de sistemas distribuídos (Tanenbaum; Van Steen, 2023).

Mergulhamos em documentações técnicas contemporâneas, manuais de sistemas operacionais e literatura acadêmica atualizada que debatiam as melhores práticas de backup, segurança da informação e, crucialmente, os desafios modernos de roteamento e redes privadas virtuais (Kurose; Ross, 2021; Stallings, 2022). Esse embasamento teórico foi o que nos permitiu desenhar uma arquitetura lógica que fizesse sentido para o orçamento de um usuário comum, mas que herdasse a robustez exigida por ambientes corporativos fechados, com a base teórica consolidada, o trabalho avançou para a fase de planejamento da infraestrutura e seleção do hardware.

O grande diferencial metodológico desta etapa foi a decisão consciente de não utilizar servidores de alto custo (arquitetura *enterprise*), mas sim adotar equipamentos de baixo custo e componentes de computadores reaproveitados (Sousa; Neves, 2025). Essa escolha não foi apenas uma restrição orçamentária, mas uma premissa sustentável do projeto: queria provar de forma incontestável que é possível alcançar um nível altíssimo de confiabilidade e desempenho dando uma sobrevida a hardwares que, de outra forma, seriam sumariamente descartados como lixo eletrônico. O ambiente físico de experimentação foi montado em uma rede local residencial padrão, conectada a um roteador fornecido pela operadora de internet, contando com smartphones e notebooks atuando como os "clientes" que consumiriam os dados do servidor (Tanenbaum; BOS, 2023).

A etapa seguinte consistiu na seleção e implantação do cérebro lógico do nosso servidor NAS. Após analisarmos várias distribuições, optamos pelo TrueNAS Scale, uma plataforma de código aberto baseada em Linux, reconhecida globalmente por sua estabilidade incomparável e foco absoluto em gestão de armazenamento em rede

(Ixsystems, 2024). A instalação do TrueNAS Scale justificou-se pela sua integração nativa com o sistema de arquivos ZFS (Zettabyte File System).

Conforme apontam os referenciais técnicos modernos, o ZFS muda as regras do jogo no ambiente doméstico porque ele une o gerenciamento de partições e o controle de integridade de dados na mesma camada, impedindo que arquivos se corrompam silenciosamente ao longo dos anos (Patterson; Hennessy, 2021). Durante essa fase experimental, os discos rígidos foram formatados, os conjuntos de armazenamento (pools) foram criados e os diretórios foram cuidadosamente compartilhados na rede local usando o protocolo SMB. Também foi aplicado, na prática, os princípios da Tríade CID (Confidencialidade, Integridade e Disponibilidade), configurando regras estritas de permissão para garantir que apenas usuários autenticados pudessem ler ou alterar os documentos críticos (Stallings, 2022).

No entanto, o projeto encontrou seu maior desafio metodológico e experimental na fase de configuração do acesso remoto. Conforme já havíamos mapeado na fase de revisão de literatura, o provedor de internet da residência onde os testes estavam sendo realizados utilizava o CGNAT (Carrier Grade Network Address Translation). O CGNAT atua como um verdadeiro bloqueio arquitetônico nas redes atuais, mascarando o IP público da residência e impossibilitando o redirecionamento tradicional de portas (Silva, 2021). Se essa barreira não fosse transposta, o servidor seria inútil fora de casa.

Foi aqui que a metodologia exigiu a implementação de uma solução moderna de rede virtual privada (VPN). Para furar o bloqueio do provedor com elegância e segurança, instalamos o software Tailscale. O Tailscale é uma ferramenta avançada baseada no protocolo de código aberto WireGuard (Tailscale, 2025). Ele foi acoplado diretamente ao servidor através do sistema de contêineres virtuais oferecido nativamente pelo TrueNAS Scale. A configuração fundamental aqui foi ativar a função de "subnet router" (sub-rotas). Em termos práticos, isso significa que nós criamos um túnel criptografado direto e impenetrável entre o celular do usuário na rua e o servidor na residência, resolvendo de imediato o problema de roteamento (Sampaio, 2022).

A grande vitória experimental desta fase foi comprovar que conseguimos acesso total aos arquivos estando a quilômetros de distância, via 4G, sem a necessidade de solicitar ou pagar por um IP fixo à operadora e sem expor nosso equipamento aos ataques comuns da internet aberta.

Superado o gargalo da rede, o passo seguinte foi automatizar a rotina de proteção de dados, removendo ao máximo o fator de "esquecimento" humano, uma das maiores causas de perda de dados pessoais (Preston, 2022). Para que o NAS cumprisse seu papel de guardião autônomo, configuramos o aplicativo FolderSync no smartphone Android do usuário principal. Neste ponto da metodologia, é fundamental destacar que todo o envio de dados foi orquestrado utilizando ativamente o protocolo SMB. A escolha do SMB como protocolo padrão de transferência não foi acidental; optamos por ele devido à sua altíssima compatibilidade com o sistema Android e sua estabilidade comprovada para o tráfego de grandes volumes de dados na rede.

O experimento consistiu em programar rotinas silenciosas de sincronização diretamente para os endereços de rede mapeados. Toda vez que uma nova foto era tirada ou um documento importante salvo, o FolderSync detectava a mudança e, em segundo plano, utilizava as credenciais SMB para despachar o arquivo com segurança para as pastas protegidas do servidor NAS. Essa configuração materializou o conceito de backup automatizado no nosso cenário doméstico, conversando na mesma "língua" nativa do servidor. Simultaneamente, adotamos o aplicativo CX Explorador de Arquivos como nossa principal janela de gerenciamento visual no ambiente móvel. Em vez de acessar o servidor por linhas de comando complexas e inviáveis para um usuário comum, o CX Explorador nos permitiu mapear os discos do NAS diretamente na tela do celular. Através dessa interface, conduzimos testes diretos de usabilidade, avaliando a capacidade de mover arquivos pesados de vídeo, organizar diretórios e excluir documentos desnecessários remotamente.

Por fim, a fase de fechamento metodológico baseou-se na execução de uma rigorosa bateria de testes de funcionamento, qualidade e estresse do sistema. Não bastava atestar que a tecnologia ligava; era crucial validar a sua resiliência (Forouzan, 2022). Conduzimos transferências de lotes volumosos de arquivos para medir a velocidade da rede local e o comportamento da memória do servidor. Simulamos o comportamento da VPN trocando repetidamente entre redes de Wi-Fi públicas e redes celulares móveis 4G e 5G, verificando a estabilidade e a continuidade da conexão remota, a análise e interpretação dos resultados de todos esses ensaios foram documentadas com foco estrito na estabilidade, segurança e viabilidade do NAS como a solução definitiva para o usuário doméstico.

Cada gargalo encontrado e cada processo validado contribuiu para provar, de forma empírica, que a adoção de uma infraestrutura de armazenamento caseira e independente é não só tecnicamente possível, mas altamente recomendada para a soberania digital (Sousa; Neves, 2025).

4.1 SOFTWARES UTILIZADOS

A consolidação da arquitetura do servidor exigiu a adoção de uma suíte de softwares capaz de integrar, com segurança e eficiência, o hardware físico às interfaces de acesso remoto do usuário. O núcleo lógico do projeto foi estruturado sobre o TrueNAS Scale, um sistema operacional de código aberto baseado em Linux, projetado especificamente para gerenciar ambientes de armazenamento em rede (NAS).

A escolha por esta plataforma justificou-se pela oferta de uma interface de controle unificada e, fundamentalmente, pelo suporte nativo ao OpenZFS, um sistema de arquivos avançado que entrega alta resiliência e proteção contínua contra a corrupção silenciosa de dados. Para o provisionamento do sistema operacional na máquina física, optou-se por um método de instalação *bare-metal* utilizando o Ventoy.

Trata-se de um utilitário de código aberto que otimiza a criação de unidades USB inicializáveis (*bootáveis*). Com o Ventoy, a imagem ISO do TrueNAS Scale foi alocada diretamente no pendrive, possibilitando o *boot* pela BIOS do equipamento reaproveitado. Esse procedimento viabilizou uma instalação limpa e isolada no disco rígido principal do servidor, estabelecendo o alicerce do sistema de forma prática e segura.

Com a infraestrutura de base plenamente operacional e conectada à rede local (LAN), a etapa seguinte consistiu na integração da camada de aplicações. O objetivo foi estabelecer uma comunicação segura e autônoma entre o servidor residencial e os dispositivos móveis. Para orquestrar essa topologia, as seguintes ferramentas foram implementadas:

Tailscale: Atuando como o pilar de conectividade do projeto, o Tailscale foi implementado para construir uma Rede Privada Virtual (VPN) descentralizada, alicerçada no moderno protocolo de criptografia WireGuard. No ecossistema deste trabalho, ele foi configurado sob a função de *subnet router* (roteador de sub-rede). Essa manobra arquitetônica foi crucial para transpor as severas restrições de roteamento impostas pelo CGNAT das operadoras de internet, garantindo ao usuário um acesso externo transparente aos dados sem a necessidade de expor ou abrir portas vulneráveis no roteador doméstico.

FolderSync: Adotado como o agente de automação no dispositivo cliente (smartphone Android). O aplicativo atua de forma ininterrupta em segundo plano, sendo o responsável por mapear os diretórios locais do aparelho e orquestrar as rotinas assíncronas de backup. Ao utilizar o protocolo de rede SMB, ele despacha cópias de fotografias e documentos diretamente para os discos do servidor de maneira totalmente autônoma, eliminando o risco de perda de dados atrelado ao esquecimento humano.

CX Explorador de Arquivos: Integrado como a principal interface gráfica para o consumo e gerenciamento dos dados no ambiente móvel. Graças à sua compatibilidade nativa com o protocolo SMB, este utilitário viabilizou o mapeamento dos volumes de rede do NAS diretamente na interface do smartphone. Com isso, o usuário adquire a capacidade de navegar pelos diretórios, ajustar permissões e manipular arquivos volumosos remotamente com a mesma fluidez e responsividade de um armazenamento interno, materializando, na prática, a experiência de uma nuvem privada.

4.2 FERRAMENTAS DE HARDWARE

Disco Rígido

Figura 1 – Discos Rígidos HDs



Fonte: Elaborado pelo autor

O HD (Hard Disk Drive), também chamado de disco rígido, é o componente encarregado de guardar o sistema operacional, além de armazenar todos os dados utilizados pelo servidor, como programas, documentos e demais arquivos necessários para o funcionamento do sistema. Dois desses Hds da imagem estão funcionando como contêiner, e o terceiro armazena o sistema.

Memória RAM

Figura 2 – Memória RAM

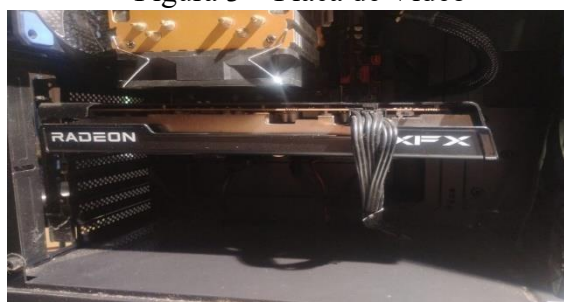


Fonte: Elaborado pelo autor

A memória RAM (*Random Access Memory* – Memória de Acesso Aleatório) é a memória principal do computador, responsável por armazenar temporariamente os dados e instruções utilizados pela CPU durante a execução do sistema operacional e das aplicações. Trata-se de uma memória volátil, ou seja, seu conteúdo é perdido quando o equipamento é desligado ou ocorre interrupção no fornecimento de energia. Por apresentar alta velocidade de acesso, a memória RAM reduz o tempo de resposta do sistema e influencia diretamente o desempenho do computador ou servidor. Atualmente, as tecnologias mais utilizadas pertencem à família DDR (Double Data Rate), como DDR3, DDR4 e DDR5, que se diferenciam pela taxa de transferência, frequência de operação e eficiência energética. No contexto deste trabalho, a memória RAM é um componente essencial para o funcionamento do servidor NAS, contribuindo para o gerenciamento do sistema de arquivos ZFS, execução dos serviços do TrueNAS SCALE e melhoria do desempenho nas operações de armazenamento e compartilhamento de dados.

Placa de Vídeo

Figura 3 – Placa de Vídeo



Fonte: Elaborado pelo autor

A GPU, conhecida como Unidade de Processamento Gráfico, é um componente eletrônico desenvolvido para executar operações matemáticas complexas com grande rapidez. Sua principal função é auxiliar no processamento de imagens e vídeos, permitindo a geração do sinal gráfico exibido no monitor. Além disso, esse componente também é amplamente utilizado em atividades que exigem alto desempenho computacional, como inteligência artificial, aprendizado de máquina, modelagem 3D e edição de vídeos.

Placa Mãe

Figura 4 – Placa Mãe



Fonte: Elaborado pelo autor

A placa mãe é o principal componente responsável pela integração de todas as partes de um servidor ou computador. Trata-se de uma placa eletrônica composta por circuitos impressos que permitem a comunicação entre os diversos hardwares do sistema, utilizando conectores, slots e interfaces específicas para cada componente.

Processador

Figura 5 – Processador



Fonte: Shopee (2026)

Disponível em: [CPU Intel XEON E5-2670 V3 LGA 2011-3 2.3Ghz - 3.1Ghz 12 Core 24 Thread ส่งฟรี 1 ปี ออก vat](#)

[|Shopee Thailand](#)

A CPU é um circuito eletrônico fundamental para o funcionamento do servidor, pois realiza a execução de comandos e o tratamento das informações recebidas pelo sistema. Esse componente trabalha processando dados digitais representados em linguagem binária, além de controlar e coordenar as operações necessárias para o desempenho das aplicações e serviços executados no equipamento.

Fonte de Alimentação

Figura 6 – Fonte de Alimentação



Fonte: Elaborado pelo autor

A fonte de alimentação é o componente responsável por distribuir energia elétrica para todas as partes do servidor, garantindo o funcionamento adequado dos dispositivos internos. Sua capacidade é medida em Watts, indicando a quantidade de energia que pode fornecer ao sistema. Além disso, muitas fontes contam com certificações 80 Plus, que avaliam o nível de eficiência energética do equipamento.

Gabinete

Figura 7 – Gabinete

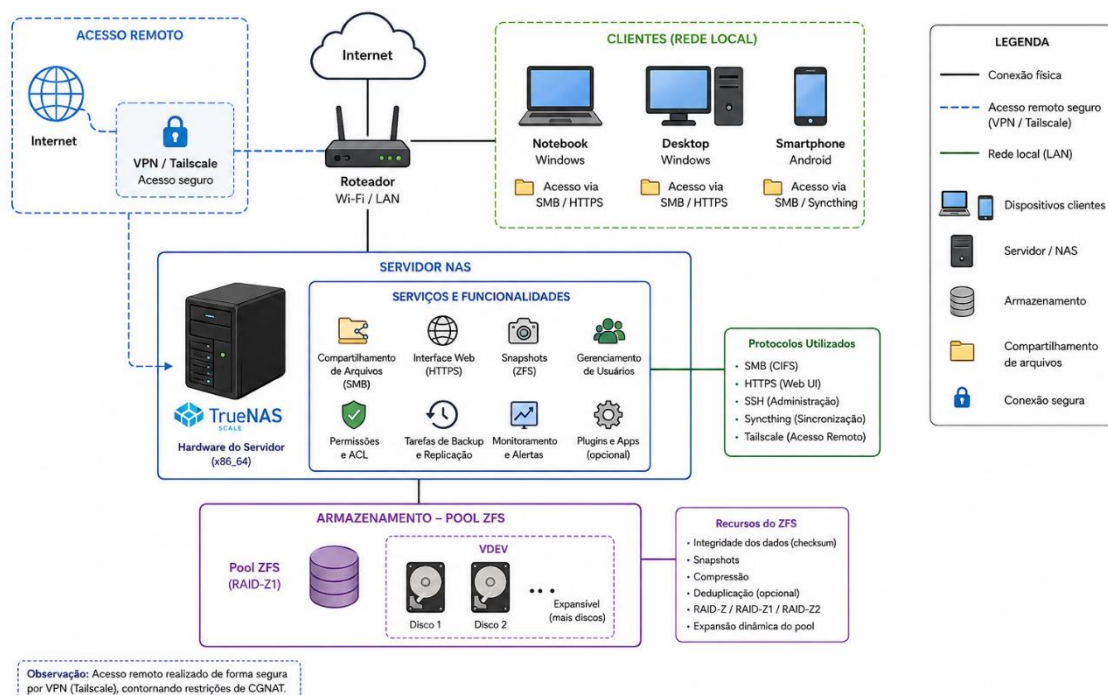


Fonte: Elaborado pelo autor

O gabinete é a estrutura física destinada a acomodar e proteger os componentes internos do computador ou servidor, como placa mãe, unidades de armazenamento e memórias. Além da organização dos equipamentos, a escolha de um gabinete adequado influencia diretamente na ventilação e no controle térmico do sistema. Uma boa refrigeração é essencial para manter o desempenho dos componentes, evitar superaquecimento e aumentar a durabilidade do hardware.

4.3 DIAGRAMA DA SOLUÇÃO UTILIZADA

Figura 8 – Diagrama da Solução Proposta



Fonte: Elaborada pelo autor

5 RESULTADOS

Após a implementação do servidor NAS doméstico, foram realizados testes práticos com o objetivo de avaliar o funcionamento, estabilidade, acessibilidade e eficiência do sistema desenvolvido. Os resultados obtidos demonstraram que a solução implementada apresentou desempenho satisfatório para utilização em ambiente residencial, atendendo aos objetivos propostos no trabalho. Inicialmente, verificou-se o funcionamento do armazenamento centralizado de arquivos na rede local.

O sistema operacional TrueNAS Scale apresentou estabilidade durante o gerenciamento do armazenamento, permitindo configuração adequada dos discos, criação de diretórios compartilhados e gerenciamento dos serviços utilizados no servidor. Além disso, os mecanismos de controle de acesso configurados no sistema possibilitaram maior organização e segurança dos arquivos armazenados. Os testes relacionados ao envio automático de arquivos também apresentaram resultados satisfatórios.

O aplicativo FolderSync foi configurado para sincronizar automaticamente arquivos do dispositivo móvel com diretórios específicos do servidor NAS. Durante os testes realizados, fotografias, vídeos e documentos foram enviados automaticamente ao servidor sem necessidade de intervenção manual do usuário, demonstrando eficiência no processo de backup automatizado. Em relação ao acesso remoto, o software Tailscale

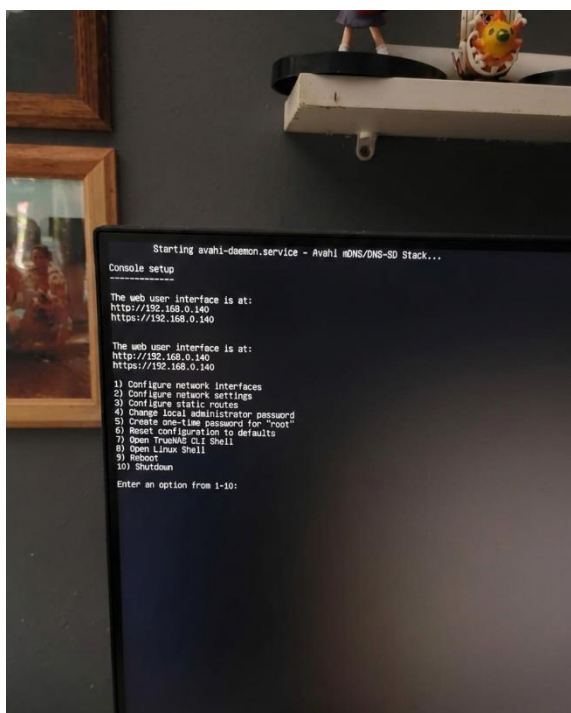
apresentou funcionamento estável durante os testes realizados. A configuração da VPN permitiu acesso seguro ao servidor NAS mesmo fora da rede local, possibilitando conexão remota aos arquivos armazenados.

A utilização do recurso de subnet router possibilitou acesso aos dispositivos presentes na rede doméstica, contornando as limitações causadas pelo uso de CGNAT na conexão residencial. Os testes de acesso remoto foram realizados utilizando diferentes redes de internet e dispositivos móveis, demonstrando estabilidade na comunicação e disponibilidade dos arquivos armazenados no servidor. Além disso, verificou-se que a utilização da VPN contribuiu significativamente para a segurança da conexão remota, o aplicativo CX Explorador de Arquivos também apresentou bom desempenho durante os testes realizados. Por meio dele, foi possível acessar os diretórios compartilhados do NAS copiar arquivos, mover documentos, excluir conteúdo e gerenciar os dados armazenados diretamente pelo smartphone.

Durante a utilização do sistema, observou-se melhora significativa na organização dos arquivos pessoais, centralização dos dados e facilidade de acesso aos conteúdos armazenados. O servidor NAS também contribuiu para reduzir a dependência exclusiva de serviços de armazenamento em nuvem, oferecendo maior controle sobre os dados pessoais, mas, algumas limitações também foram identificadas durante o desenvolvimento do projeto, a velocidade de transferência dos arquivos mostrou-se dependente da qualidade da rede local e da conexão com a internet utilizada no acesso remoto, e a utilização de hardware de baixo custo pode limitar o desempenho do sistema em cenários com grande volume de acessos simultâneos.

Porém, mesmo diante dessas limitações, os resultados demonstraram que a implementação de um servidor NAS doméstico utilizando ferramentas gratuitas e hardware acessível é viável para usuários residenciais, oferecendo uma solução eficiente para armazenamento, backup automatizado e acesso remoto seguro aos dados pessoais.

Figura 9



Fonte: Elaborado pelo autor

Tela da interface do servidor após ligado, contendo as informações necessárias para que possa ser feita a configuração pelo navegador.

Figura 10

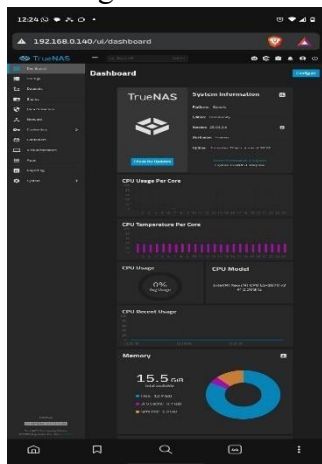


Figura 11

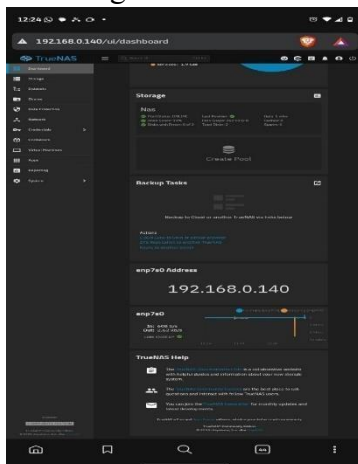
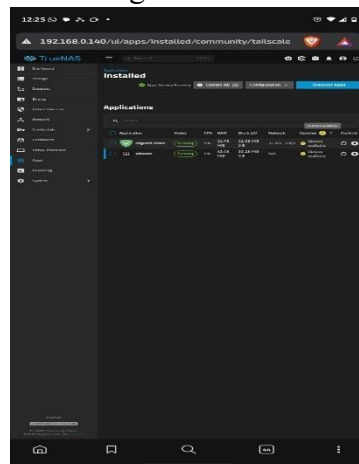


Figura 12



Fonte: Elaborada pelo autor

Dashboard/Interface do TrueNAS, acesso sendo feito por um dispositivo móvel via IP no navegador Brave.

Figura 13



Figura 14



Fonte: Elaborado pelo autor

Imagem do Servidor montado, os dois Hds em cima da caixa, um deles está executando o sistema o outro está funcionando como contêiner principal e o outro Hd que está na case em cima do gabinete, este está servindo como espelho (MIRROR).

Figura 15



Fonte: Elaborado pelo autor

Imagem do Setup inteiro montado

Figura 16

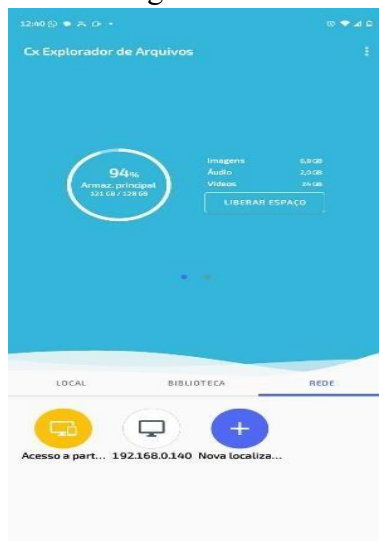
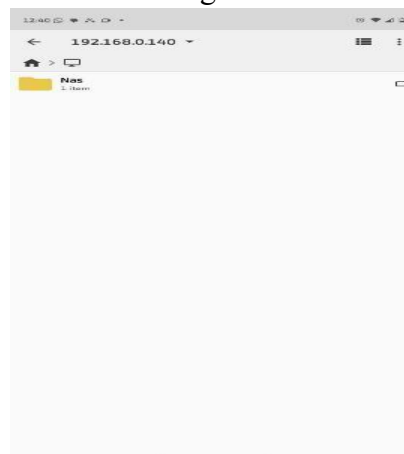


Figura17



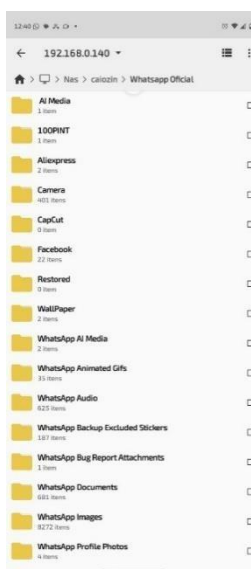
Fonte: Elaborado pelo autor

Imagem da interface do aplicativo Cx Explorador de Arquivos, na Figura, consta a tela inicial do aplicativo, na tela consta três abas, Local, Biblioteca e Rede, em (Local) é o armazenamento local do dispositivo móvel (celular), em (Biblioteca) fica o filtro de arquivos do dispositivo móvel, (Imagens, Áudio, Vídeos e Documentos), e em (Rede) é onde o NAS pode ser acessado. Na Figura, é o acesso ao Nas, dentro da pasta Nas, está o usuário e suas respectivas pastas sincronizadas que serão mostradas nas figuras a seguir.

Figura 18



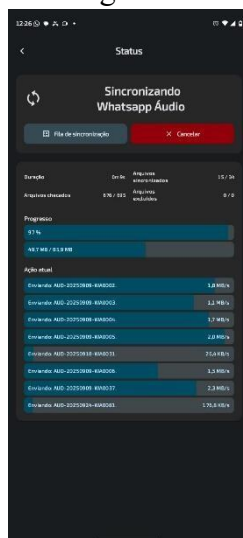
Figura 19



Fonte: Elaborado pelo autor

Na Figura, consta o usuário que foi configurado, e na figura, consta as pastas dos arquivos do dispositivo móvel que foram sincronizados.

Figura 20



Fonte: Elaborado pelo autor

Na Figura, consta a interface da sincronização de arquivos feita pelo aplicativo FolderSync.

6 CONCLUSÃO

O desenvolvimento deste trabalho permitiu construir um servidor NAS doméstico funcional, provando que a centralização e a proteção de dados pessoais podem ser alcançadas de forma autônoma e eficiente em ambientes residenciais. Ao longo do trabalho, ficou claro que é muito bom possuir um sistema de armazenamento próprio ao invés de ficar dependendo do modelo de dependência das nuvens comerciais, as quais, frequentemente, impõem políticas restritivas de governança e custos de assinatura muitas vezes caros (Veras, 2021).

O sistema implementado superou as expectativas de estabilidade. O uso do TrueNAS Scale provou ser a escolha acertada, oferecendo não apenas uma interface intuitiva, mas um gerenciamento de recursos sob o sistema de arquivos OpenZFS que, como discutido por Sousa e Neves (2025), é hoje a barreira mais eficaz contra a corrupção silenciosa de dados em servidores de baixo custo. A integração com o Tailscale foi o ponto de virada para a acessibilidade: ao contornar o CGNAT por meio de uma malha *WireGuard*, eliminamos a necessidade de exposição perimetral do roteador, um risco de segurança que a literatura recente classifica como crítico para servidores domésticos (Stallings, 2022).

A automação da camada de transferência, estruturada via protocolo SMB e gerenciada pelo FolderSync, validou que a segurança não precisa sacrificar a conveniência. A capacidade de realizar backups assíncronos e remotos aproxima o servidor caseiro da experiência de uso das plataformas *cloud* corporativas, porém com a vantagem da privacidade total sobre o *dataset* do usuário. Os testes de estresse confirmaram que, embora o desempenho esteja atrelado à infraestrutura de rede local (especificamente à taxa de *upload* da banda larga contratada), a arquitetura é robusta o suficiente para demandas de uso pessoal.

Como pontuado por ISOC Brasil (2024), a soberania digital na era do *Big Data* não é mais um luxo, mas uma necessidade técnica. O servidor NAS doméstico, portanto, deixa de ser um projeto de simples para se tornar uma solução de infraestrutura essencial na mitigação de riscos de perda de dados e na proteção contra a mercantilização da privacidade (Sousa; Neves, 2025).

Conclui-se que a implementação de um servidor NAS doméstico é como uma solução viável e eficiente para o armazenamento centralizado e a realização de backups de dados pessoais. Ao longo deste trabalho, foi possível demonstrar que a utilização de ferramentas como o TrueNAS Scale, associada a mecanismos de sincronização automática e acesso remoto seguro, permite ao usuário maior controle sobre suas informações, reduzindo a dependência de serviços de armazenamento em nuvem e minimizando os riscos relacionados à perda de dados.

Os resultados obtidos durante os testes evidenciaram que o sistema implementado apresentou desempenho satisfatório nas atividades de armazenamento, compartilhamento e sincronização de arquivos, além de possibilitar o acesso remoto seguro por meio de VPN, mesmo em ambientes com limitações de infraestrutura de rede, como a utilização de CGNAT. Dessa forma, verificou-se que a solução proposta atende adequadamente às necessidades de usuários domésticos que buscam maior segurança, disponibilidade e organização de seus dados digitais, além dos benefícios técnicos observados, foi possível ver que a adoção de um servidor NAS doméstico pode representar uma alternativa economicamente vantajosa a longo prazo, uma vez que reduz custos recorrentes com serviços de armazenamento em nuvem e proporciona maior autonomia na gestão das informações pessoais.

Como trabalhos futuros, sugere-se a ampliação da infraestrutura de armazenamento por meio da implementação de arranjos RAID mais robustos, visando

aumentar a redundância e a tolerância a falhas. Recomenda-se também a adoção de sistemas avançados de monitoramento do servidor, integração com plataformas de streaming e gerenciamento de mídia, utilização de snapshots automatizados, replicação de dados para ambientes externos e o fortalecimento das políticas de segurança, incluindo criptografia avançada, autenticação multifator e mecanismos adicionais de proteção contra ameaças cibernéticas. Essas melhorias poderão contribuir para elevar ainda mais a confiabilidade, disponibilidade e segurança da solução proposta.

REFERÊNCIA

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 14724:2023:** Informação e documentação — trabalhos acadêmicos — apresentação. Rio de Janeiro: ABNT, 2023.
- BARBOSA, Wellington. **Estudo de Caso do Sistema X-Road da Estônia:** Lições para a Interoperabilidade no Brasil. Dissertação (Mestrado em Avaliação de Políticas Públicas) – Escola Nacional de Administração Pública (ENAP), Brasília, 2026. Disponível em: <https://repositorio.enap.gov.br/>.
- BUYYA, Rajkumar et al. **Cloud Computing:** princípios, arquitetura e aplicações. 2. ed. São Paulo: Editora Atlas, 2021.
- CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet.** São Paulo: NIC.br, 2024.
- COMER, Douglas E. **Interconexão de Redes com TCP/IP:** Princípios, protocolos e arquiteturas. 7. ed. Rio de Janeiro: Elsevier, 2021.
- FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores.** 6. ed. Porto Alegre: AMGH, 2022.
- IBM. **What is Network Attached Storage (NAS)?** IBM Technology, 2026.
- ISOC BRASIL. **Soberania digital:** para quê e para quem? Análise conceitual e política do conceito a partir do contexto brasileiro. São Paulo: Internet Society Brasil, 2024. Disponível em: <https://isoc.org.br/>.
- IXSYSTEMS. **TrueNAS SCALE Documentation Hub.** San Jose: iXsystems, 2024.
- KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet.** 8. ed. São Paulo: Pearson, 2021.
- LACERDA, Paulo S. P. de; SOARES, Juliane A.; LENZ, Maikon L. **Projeto de redes de computadores.** Porto Alegre: SAGAH, 2022.
- NEGUS, Christopher. **Linux Bible.** 10. ed. Indianapolis: Wiley, 2021.
- PATTERSON, David A.; HENNESSY, John L. **Organização e Projeto de Computadores.** 6. ed. Rio de Janeiro: Elsevier, 2021.
- PRESTON, W. Curtis. **Proteção Moderna de Dados:** Assegurando a capacidade de recuperação de todos os workloads modernos. São Paulo: Novatec, 2022.
- SAMPAIO, Anderson. **Tecnologia VPN e um estudo de caso.** 2. ed. Joinville: Clube de Autores, 2022.

SILVA, Antonio Eduardo Marques da. **Redes de computadores: teoria e prática**. São Paulo: Senac São Paulo, 2021.

SOUSA, Ítalo Freire de; NEVES, Rafael Henrique dos Santos. Servidor NAS residencial: projeto, implementação e benefícios econômicos. **Revista FT**, v. 29, ed. 142, jan. 2025.

STALLINGS, William. **Segurança de computadores: princípios e práticas**. 8. ed. São Paulo: Pearson, 2022.

TAILSCALE. **Tailscale Concepts and Subnet Routing Documentation**. Toronto: Tailscale Inc., 2025.

TANENBAUM, Andrew S.; BOS, Herbert. **Sistemas operacionais modernos**. 5. ed. São Paulo: Pearson, 2023.

TANENBAUM, Andrew S.; VAN STEEN, Maarten. **Sistemas Distribuídos: princípios e paradigmas**. 4. ed. São Paulo: Pearson, 2023.

VERAS, Manoel. **Computação em Nuvem: Nova Arquitetura da TI**. Rio de Janeiro: Brasport, 2021.