



## PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

# Projeto de Infraestrutura de Rede: Cooperativa - Cred Vale Doce\*

Carlos Alberto Vieira de Souza<sup>1</sup>  
Laura de Freitas Mendes Losque<sup>2</sup>  
Luana Horta de Souza<sup>3</sup>  
Lucas Araújo Pacheco<sup>4</sup>  
Odair Cordeiro Marra<sup>5</sup>  
Victor Samuel Costa Pereira<sup>6</sup>  
Yan Oyama Moura<sup>7</sup>  
Fábio Leandro Rodrigues Cordeiro<sup>8</sup>

## Resumo

O presente trabalho propõe a elaboração e documentação de uma estrutura de rede para a Cred Vale Doce, cooperativa de crédito cuja matriz está localizada em Guanhães e que conta ainda com mais cinco filiais. O objetivo central do projeto é analisar o ambiente e apresentar soluções de rede que conciliem viabilidade técnica e econômica, atendendo às necessidades de integração, desempenho e suporte às atividades estratégicas, operacionais e administrativas da instituição. Considerando o cenário atual, em que a eficiência, a segurança e a escalabilidade das infraestruturas tecnológicas são essenciais para a continuidade e a competitividade das organizações, no qual o desenvolvimento de uma arquitetura de rede robusta e bem planejada torna-se imprescindível. O projeto contempla o planejamento

\*Artigo apresentado ao Instituto de Ciências Exatas e Informática da Pontifícia Universidade Católica de Minas Gerais, campus Contagem, como pré-requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

<sup>1</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [carlos.souza.984054@sga.pucminas.br](mailto:carlos.souza.984054@sga.pucminas.br).

<sup>2</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [laura.losque@sga.pucminas.br](mailto:laura.losque@sga.pucminas.br).

<sup>3</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [luana.horta@sga.pucminas.br](mailto:luana.horta@sga.pucminas.br).

<sup>4</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [luca.pacheco@sga.pucminas.br](mailto:luca.pacheco@sga.pucminas.br).

<sup>5</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [odair.marra@sga.pucminas.br](mailto:odair.marra@sga.pucminas.br).

<sup>6</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [victor.pereira.1416479@sga.pucminas.br](mailto:victor.pereira.1416479@sga.pucminas.br).

<sup>7</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [yan.moura@sga.pucminas.br](mailto:yan.moura@sga.pucminas.br).

<sup>8</sup>Professor(a) do Programa de Graduação em Sistemas de Informação – [fabio@pucminas.br](mailto:fabio@pucminas.br).

da infraestrutura de rede, o desenvolvimento do protótipo no Cisco Packet Tracer, a configuração dos serviços essenciais utilizando máquinas virtuais, além da implantação de um ambiente virtualizado na nuvem (AWS). Em seguida, realizam-se o monitoramento dos serviços por meio do Zabbix e, por fim, a elaboração da Política de Segurança da Informação da cooperativa, incluindo uma Cartilha de Segurança e o desenvolvimento do backend com a análise de vulnerabilidades.

**Palavras-chave:** **Cooperativa, Infraestrutura de Rede, Segurança da Informação, Monitoramento, Máquina virtual, Ambiente em nuvem, Ambiente local.**

## 1 ANÁLISE, PLANEJAMENTO E PROTOTIPAÇÃO DA SOLUÇÃO

O projeto de infraestrutura de redes da Cooperativa de Crédito Cred Vale Doce tem como foco a criação de um ambiente tecnológico integrado, seguro e escalável, capaz de sustentar as operações financeiras, administrativas e comunitárias da instituição. A proposta contempla o planejamento físico e lógico da rede, a definição de topologia WAN e LAN, a implantação de serviços corporativos (DNS, DHCP, Web, AD, FTP, NFS e DB) e a prototipação da solução no Cisco Packet Tracer, garantindo a viabilidade técnica e econômica do sistema.

O objetivo principal deste projeto é planejar e implementar uma infraestrutura de rede estruturada que proporcione conectividade eficiente e segura entre a matriz (localizada em Guanhães – MG) e as cinco filiais distribuídas em cidades estratégicas da região. O projeto visa oferecer alta disponibilidade de serviços, redução de custos operacionais e melhoria no atendimento aos cooperados, sustentando o crescimento tecnológico da cooperativa e sua expansão regional.

### 1.1 Análise da Solução

A Cred Vale Doce foi fundada em 2015, na cidade de Guanhães – MG, por produtores rurais e comerciantes locais que buscavam uma alternativa justa aos bancos tradicionais, com o propósito de incluir financeiramente os cooperados e fortalecer a economia regional. Com o passar dos anos, a cooperativa expandiu suas atividades para cidades vizinhas, mantendo como pilares a cooperação, a ética e a inovação tecnológica.

Atualmente, a Cred Vale Doce possui uma matriz e cinco filiais, totalizando cerca de 125 colaboradores e atendendo aproximadamente 59.000 clientes. A seguir, apresenta-se um resumo das unidades operacionais e características econômicas de cada cidade de atuação, conforme Tabela 1:

**Quadro 1 – Distribuição das Unidades da Cred Vale Doce**

Unidade	Localização	Atividade Econômica Predominante
Matriz	Guanhães	Produção de leite
Filial 1	Conceição do Mato Dentro	Mineração de ferro
Filial 2	Serro	Produção de queijo do Serro
Filial 3	Virginópolis	Produção de jabuticaba
Filial 4	Diamantina	Produção de vinhos
Filial 5	Governador Valadares	Produção de frutas, indústria e serviços

**Fonte: Elaborado pelos autores**

### **1.1.1 Missão, Visão e Valores**

A Cred Vale Doce tem como missão oferecer serviços financeiros acessíveis e transparentes, promovendo o desenvolvimento econômico e social das comunidades onde atua.

Possui como visão ser reconhecida como a principal cooperativa financeira do Vale do Rio Doce Mineiro até 2030, destacando-se pela inovação tecnológica e proximidade com os cooperados.

Os seus valores são: Transparência, ética, valorização da comunidade, inclusão financeira e inovação com responsabilidade.

### **1.1.2 Identidade Visual**

A identidade visual da cooperativa reflete confiança e crescimento. A logomarca, em azul e verde, simboliza segurança e prosperidade, enquanto a seta ascendente dentro de um círculo representa integração e evolução (Figura 1).

**Figura 1 – Logomarca da Cred Vale Doce**

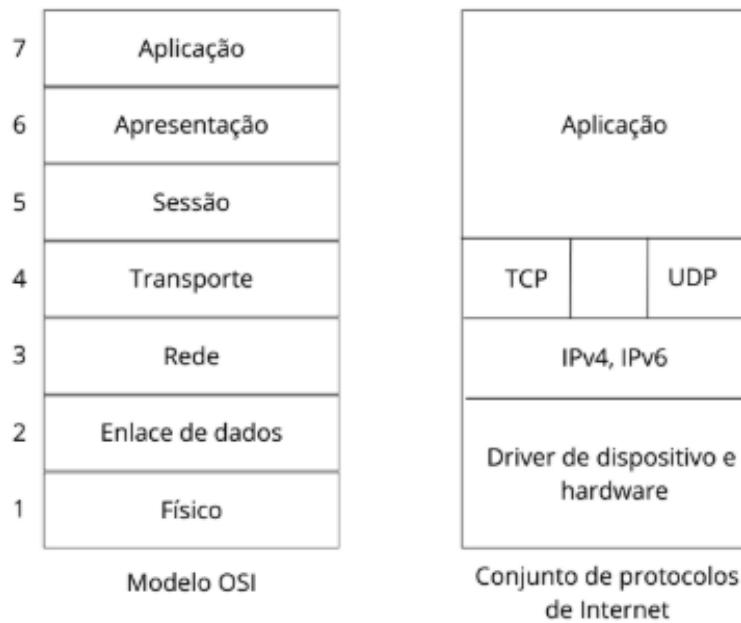


**Fonte:** Elaborada pelos autores

### **1.2 Planejamento da Solução**

O desenvolvimento do projeto de rede da Cred Vale Doce adotará a Metodologia Top-Down, que parte da análise das necessidades do cliente e avança para a definição dos equipamentos e tecnologias necessárias. Desta forma, o modelo lógico usado como referência nesse projeto será o TCP/IP, que é estruturado em quatro camadas principais: acesso à rede, internet, transporte e aplicação, o que assegura interoperabilidade e comunicação ponta a ponta entre matriz e filiais (Figura 2). O TCP/IP foi baseado no modelo OSI que, apesar de sua inegável importância histórica e didática, não é utilizado de forma direta no dia a dia, já que é visto como um guia conceitual para a compreensão do processo de comunicação (Oppenheimer, 1999).

**Figura 2 – Modelo OSI e Modelo TCP/IP**



**Fonte:** adaptada da aula do Professor Alexandre Teixeira

A aplicação desse modelo garante que a cooperativa disponha de comunicação confiável, escalável e segura, fundamentais para o funcionamento contínuo de sistemas corporativos como Internet Banking, ERPs e serviços internos.

### **1.2.1 Requisitos de Negócio**

Os principais objetivos estratégicos da Cred Vale Doce são:

- Aumentar a receita e o lucro da cooperativa;
- Expandir a presença regional;
- Melhorar a produtividade e o suporte técnico;
- Reduzir custos operacionais e riscos de segurança;
- Assegurar a continuidade dos serviços bancários;
- Tornar o Data Center mais eficiente.

### **1.2.2 Restrições do Projeto**

As principais restrições do projeto da Cred Vale Doce são:

- Orçamento disponível: R\$ 1.150.000,00;
- Prazo de execução: 4 meses.

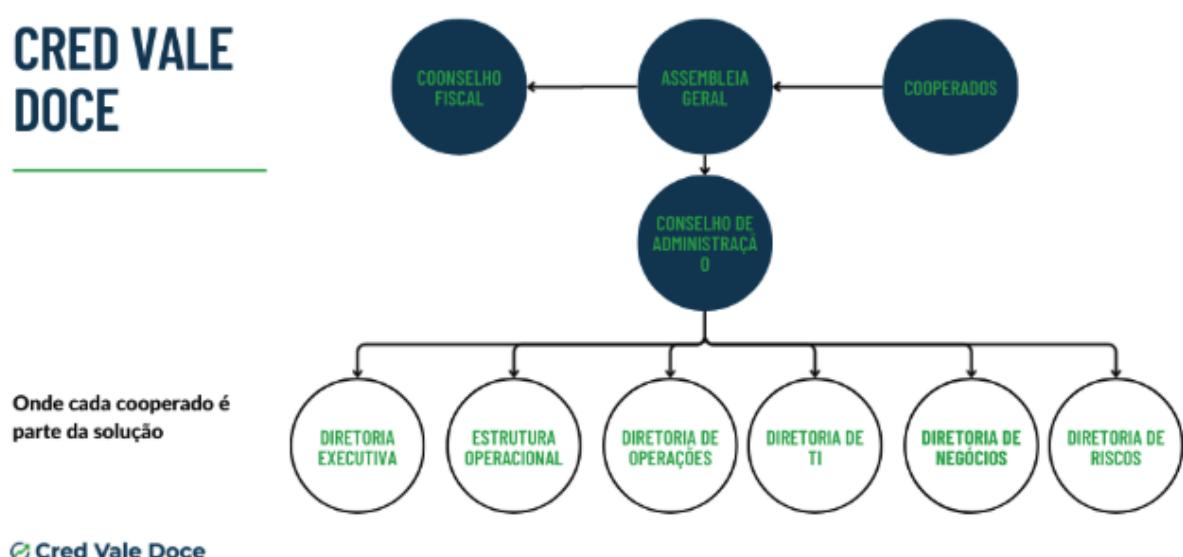
### 1.3 Análise Estrutural e Organizacional

A governança da Cred Vale Doce é composta por:

- Assembleia Geral (cooperados);
- Conselho de Administração (presidente, vice e conselheiros);
- Diretoria Executiva, composta por:
  - Diretor Geral (CEO)
  - Diretor Financeiro (CFO)
  - Diretor de Operações (COO)
  - Diretor de TI (CIO/CTO)
  - Diretor de Negócios e Relacionamento
  - Diretor de Riscos Compliance

Para uma melhor visualização, a Figura 3 apresenta o organograma da Cred Vale Doce:

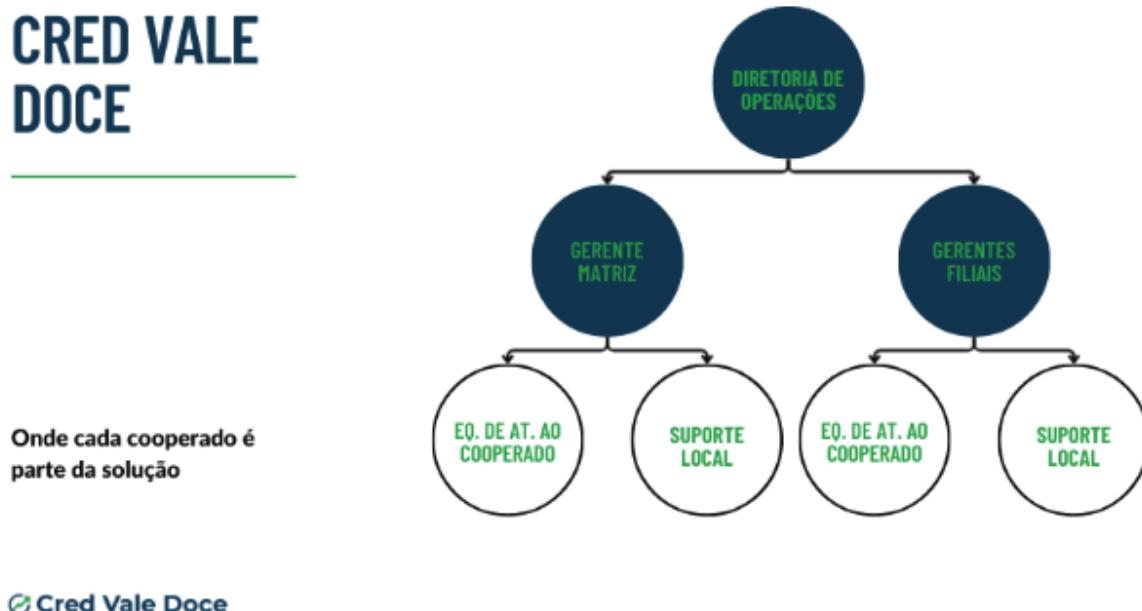
**Figura 3 – Organograma Matriz CRED VALE DOCE**



**Fonte: Elaborada pelos autores**

Cada filial é gerida por um gerente local, que responde à Diretoria de Operações. Todas as unidades seguem um padrão de estrutura organizacional e tecnológica definido pela sede. Nas filiais o organograma segue a estrutura disposta na Figura 4:

**Figura 4 – Organograma Filial CRED VALE DOCE**



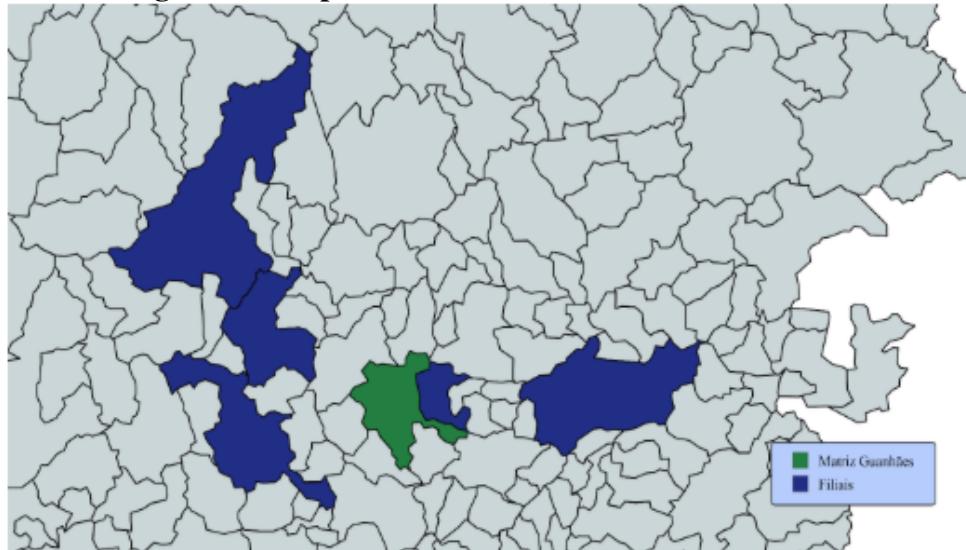
Cred Vale Doce

Fonte: Elaborada pelos autores

#### 1.4 Localização Geográfica

A localização geográfica das unidades podem ser visualizadas com maior clareza na Figura 5 e Figura 6:

**Figura 5 – Mapa Matriz e Filiais CRED VALE DOCE**



Fonte: Elaborada pelos autores

**Figura 6 – Distância entre a Matriz e as Filiais CRED VALE DOCE**



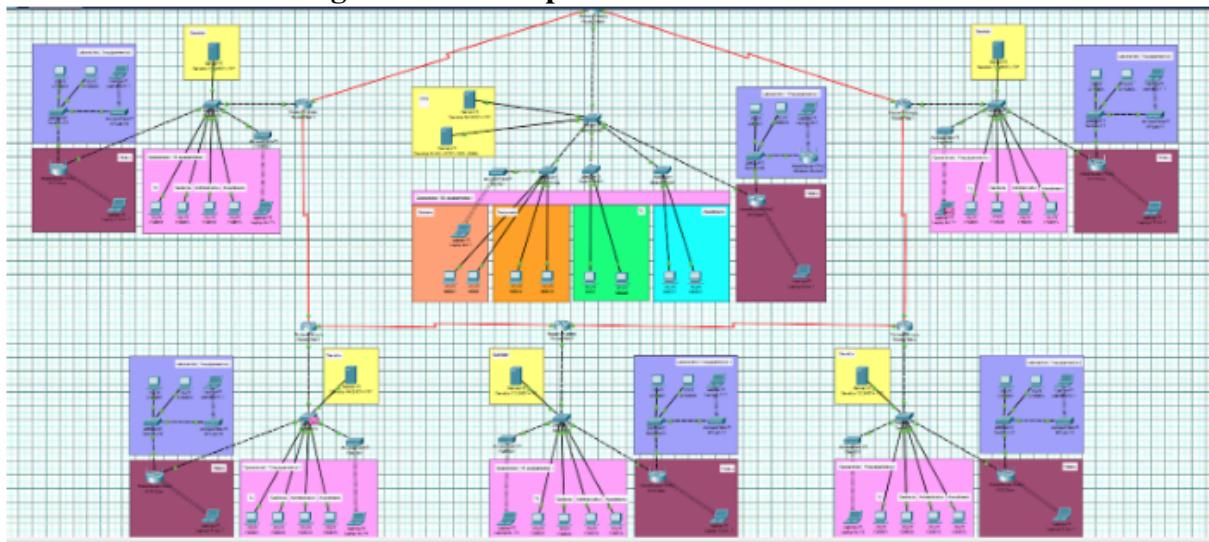
**Fonte:** Elaborada pelos autores

Embora a distância entre a matriz e as suas filiais seja considerável, isso não representa um problema para a conectividade e integração entre esses locais. Isso porque a comunicação e o tráfego de dados não dependem mais de conexões físicas manuais, mas sim de tecnologias modernas e automatizadas, que garantem uma ligação eficiente, independentemente da distância geográfica.

## **1.5 Prototipação da Solução**

### **1.5.1 Topologia e Arquitetura da Rede**

O protótipo foi desenvolvido no Cisco Packet Tracer, adotando uma topologia WAN em anel, a mais adequada às características do projeto (Figura 7).

**Figura 7 – Protótipo de Rede Cred Vale Doce**

**Fonte:** Elaborada pelos autores

Nele foi utilizado uma WAN em formato de anel que é o mais apropriado levando em consideração as características do projeto. A cooperativa com uma matriz e cinco filiais terá um maior equilíbrio entre o desempenho, o custo e confiabilidade se o projeto seguir essa topologia porque cada filial é interligada a próxima o que forma um circuito fechado, permitindo que os dados possam trafegar em ambas as direções, o que mantém a comunicação ativa mesmo que aconteça uma falha em um dos pontos porque existe um caminho alternativo, dando uma maior possibilidade de disponibilidade na rede. Além disso, o formato anel também facilita o gerenciamento do fluxo de informações entre a matriz e as filiais, o que reduz a possibilidade de congestionamento e otimiza a velocidade da transmissão.

Ao pensar em uma cooperativa de crédito, essa integração e o acesso contínuo aos sistemas são essenciais para o atendimento aos cooperados, a escolha da topologia em anel se mostra uma solução eficiente e segura e mantém os custos em infraestrutura mais acessíveis que outras mais complexas, como a malha completa. A malha completa seria uma solução inviável porque apesar de oferecer redundância, ela exige um custo de infraestrutura alto e uma complexidade desnecessária e aumentaria a possibilidade de erros, por causa da quantidade de rotas disponíveis, tornando o anel uma alternativa mais equilibrada e confiável. Outra possibilidade seria a em estrela, já que é uma rede relativamente pequena mas, por ser uma cooperativa é essencial evitar que ocorra uma falha crítica que possa derrubar toda a rede, porque a disponibilidade da rede é essencial para atender aos cooperados nas várias filiais.

A rede corporativa foi estruturada de forma a contemplar conectividade entre a Matriz e as cinco Filiais utilizando uma WAN, com enlaces redundantes e roteadores dedicados em cada unidade. Cada roteador da WAN conecta-se à sua respectiva LAN local, garantindo segmentação, desempenho e segurança. A Matriz é o ponto central de administração e gerenciamento dos serviços, conectando-se diretamente à todas as Filiais, fechando o circuito lógico. Cada filial possui roteadores configurados em faixas de endereçamento privadas distintas, conforme Tabela 1 dos IP'S definida no projeto, utilizando a Classe A - faixa (10.x.x.x), formando um

anel lógico que interliga todas as unidades.

### **1.5.2 Planilha de Endereçamento de IPs**

A planilha de Endereçamento de IPs apresenta a organização lógica da rede da Cooperativa de Crédito Cred Vale Doce, detalhando, para cada unidade (matriz e filiais), as informações referentes a nome do setor, endereço IP, máscara de sub-rede, gateway padrão e faixa de endereços disponíveis.

Essa estruturação é essencial para garantir uma administração de rede clara, segura e escalável, permitindo o controle eficiente dos dispositivos conectados, a facilidade de manutenção e a alocação organizada de novos equipamentos conforme o crescimento da cooperativa.

Logo abaixo, na Figura 8, são apresentados os endereços IPs referentes à matriz da Cred Vale Doce e à Filial 1 (Conceição do Mato Dentro). A planilha completa, contendo as informações de todas as seis unidades (matriz e cinco filiais).

**Figura 8 – Planilha de Endereçamento de IPs**

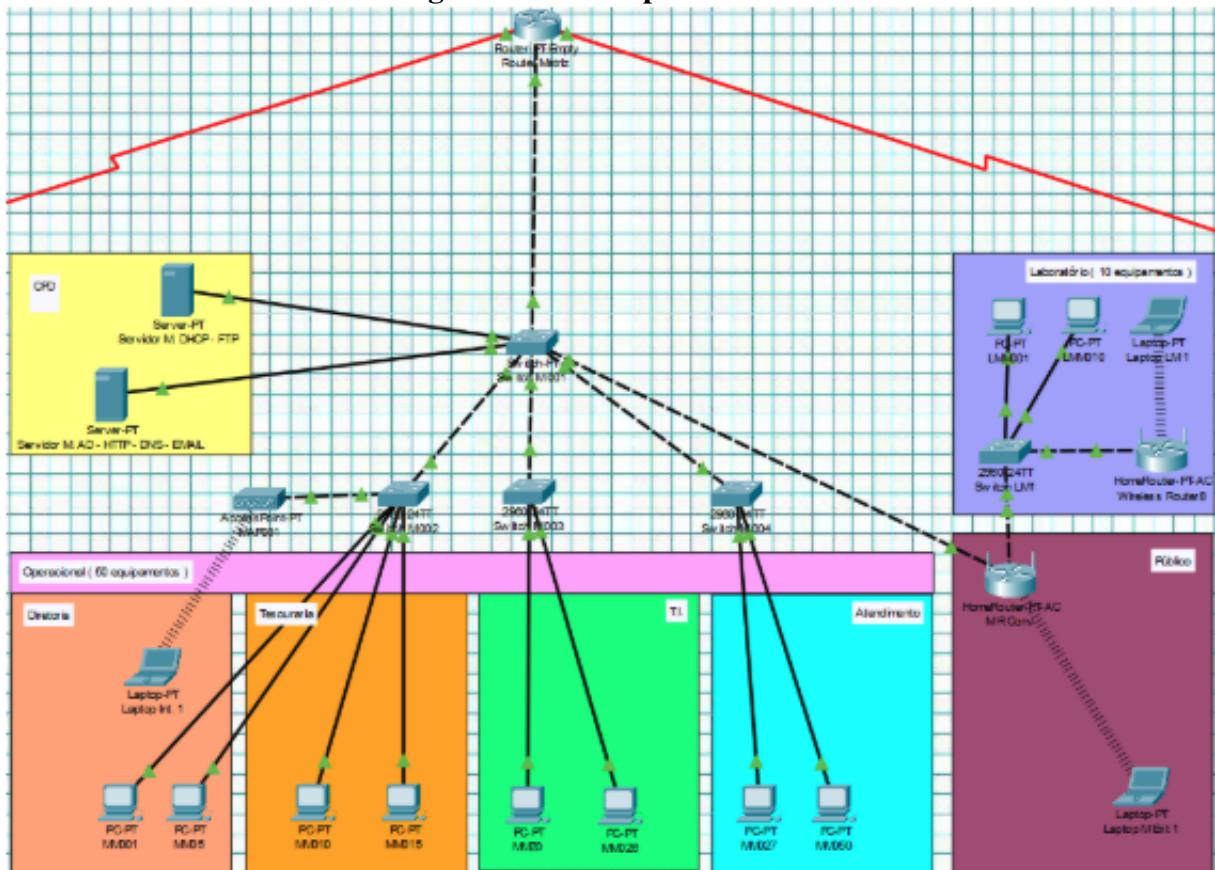
Planilha de IP's					
Nome	LAN				
	IP address	Subnet Mask	IP Gateway	IP Range	DHCP IP
Matriz	172.16.100.0	255.255.255.0	172.16.100.1	1 a 100	172.16.100.11 a 172.16.100.100
Filial 1	172.16.201.0	255.255.255.0	172.16.201.1	1 a 100	172.16.201.11 a 172.16.201.100
Filial 2	172.16.202.0	255.255.255.0	172.16.202.1	1 a 100	172.16.202.11 a 172.16.202.100
Filial 3	172.16.203.0	255.255.255.0	172.16.203.1	1 a 100	172.16.203.11 a 172.16.203.100
Filial 4	172.16.204.0	255.255.255.0	172.16.204.1	1 a 100	172.16.204.11 a 172.16.204.100
Filial 5	172.16.205.0	255.255.255.0	172.16.205.1	1 a 100	172.16.205.11 a 172.16.205.100
Nome	LAN - Pública				
	IP address	Subnet Mask	IP Gateway	IP Range	DHCP IP
Matriz	192.168.100.0	255.255.255.0	192.168.100.1	1 a 254	192.168.100.2 a 192.168.100.254
Filial 1	192.168.201.0	255.255.255.0	192.168.201.1	1 a 254	192.168.201.2 a 192.168.201.254
Filial 2	192.168.202.0	255.255.255.0	192.168.202.1	1 a 254	192.168.202.2 a 192.168.202.254
Filial 3	192.168.203.0	255.255.255.0	192.168.203.1	1 a 254	192.168.203.2 a 192.168.203.254
Filial 4	192.168.204.0	255.255.255.0	192.168.204.1	1 a 254	192.168.204.2 a 192.168.204.254
Filial 5	192.168.205.0	255.255.255.0	192.168.205.1	1 a 254	192.168.205.2 a 192.168.205.254
Nome	WAN				
	IP address	Subnet Mask			
Matriz	10.5.0.100 e 10.0.1.100	255.255.255.0			
Filial 1	10.0.1.201 e 10.1.2.201	255.255.255.0			
Filial 2	10.1.2.202 e 10.2.3.202	255.255.255.0			
Filial 3	10.2.3.203 e 10.3.4.203	255.255.255.0			
Filial 4	10.3.4.204 e 10.4.5.204	255.255.255.0			
Filial 5	10.4.5.205 e 10.5.0.205	255.255.255.0			

**Fonte:** Elaborada pelos autores

### **1.5.3 Protótipo Matriz**

A Figura 9 demonstra com mais detalhes o protótipo da matriz.

**Figura 9 – Protótipo da Matriz**



**Fonte: Elaborada pelos autores**

Na Matriz, o roteador da WAN conecta-se à infraestrutura LAN, que foi organizada para suportar os seguintes setores e serviços:

- Departamentos Operacionais: Diretoria, Tesouraria, T.I. e Atendimento, projetados para 50 equipamentos.
- Rede Pública Wi-Fi: disponível para visitantes e usuários externos.
- Laboratório de Informática: voltado à comunidade, com capacidade para 10 equipamentos.
- CPD, contemplando os seguintes serviços:
  - Servidor 1: Active Directory (AD), HTTP, DNS e E-mail (suportando Matriz e Filiais).
  - Servidor 2: DHCP e FTP (dedicado à Matriz).

A camada de rede foi planejada com 1 switch L3 na camada de Acesso e 3 switches de 24 portas na camada de Distribuição, permitindo expansão futura.

Quanto à Estrutura de Endereçamento IP, a rede LAN foi organizada em sub-redes distintas para garantir isolamento e controle de tráfego da rede:

LAN Operacional – Departamentos internos (Classe B)

- IP Address: 172.16.100.0
- Subnet Mask: 255.255.255.0 (/24)
- Gateway: 172.16.100.1
- Faixa de IPs: 172.16.100.1 – 172.16.100.100
- DHCP Pool: 172.16.100.11 – 172.16.100.100

LAN Pública / Laboratório (Classe C)

- IP Address: 192.168.100.0
- Subnet Mask: 255.255.255.0 (/24)
- Gateway: 192.168.100.1
- Faixa de IPs: 192.168.100.1 – 192.168.100.254
- DHCP Pool: 192.168.100.2 – 192.168.100.254

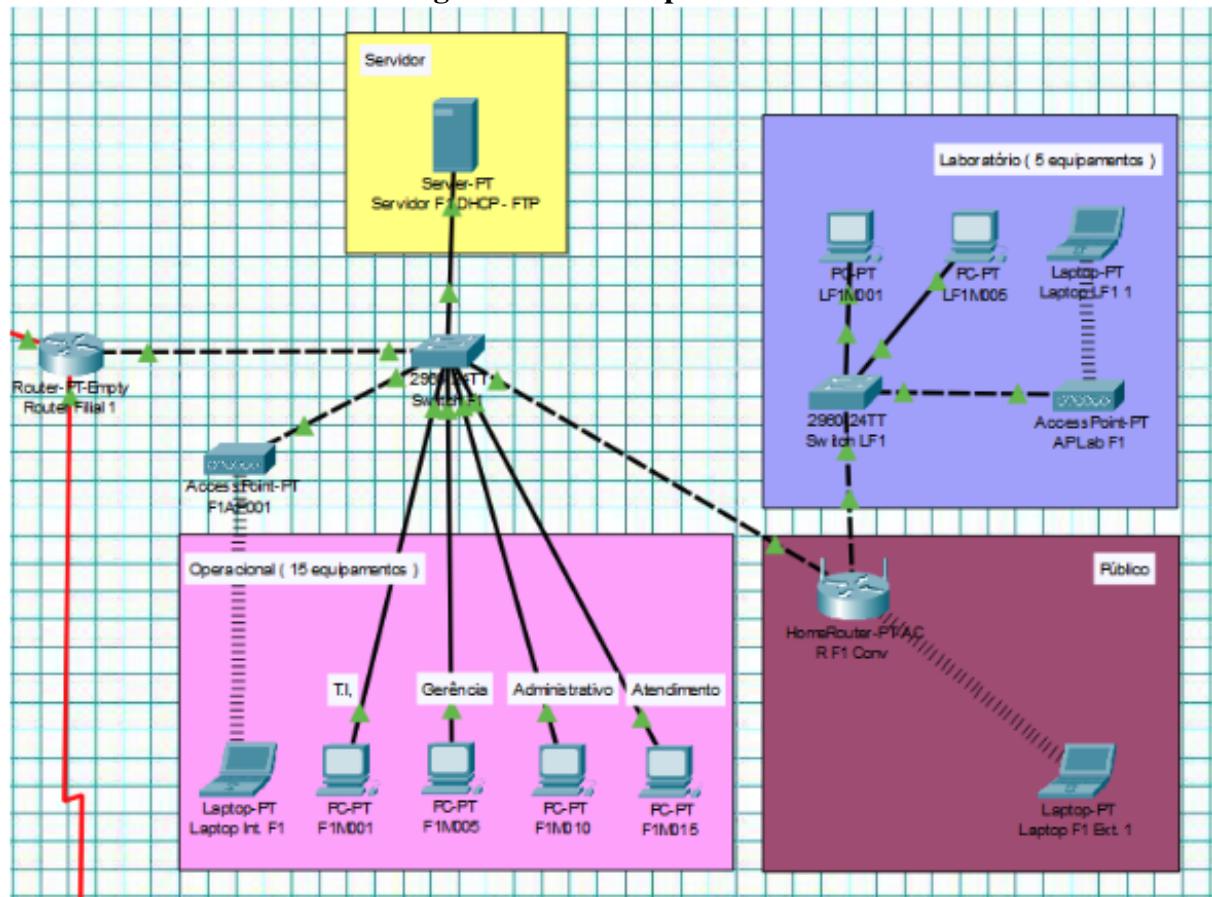
Adicionalmente, foram configuradas redes Wi-Fi independentes para os seguintes contextos:

- Operacional (uso interno e seguro).
- Público / Laboratório (uso externo e visitantes).

#### ***1.5.4 Protótipo Filial***

A Figura 10 demonstra com mais detalhes o protótipo da filial.

**Figura 10 – Protótipo da Filial**



**Fonte:** Elaborada pelos autores

Cada filial foi projetada com uma LAN estruturada, interligada ao respectivo roteador da WAN, garantindo independência lógica e conectividade com a Matriz e demais unidades. A configuração foi padronizada para todas as cinco filiais, assegurando uniformidade administrativa, facilidade de manutenção e expansão futura.

Estrutura da Rede LAN das Filiais, tem alocado:

- 15 equipamentos operacionais, distribuídos entre os departamentos de TI, Gerência, Administrativo e Atendimento.
- Laboratório de informática, com 5 equipamentos destinados à comunidade ou treinamentos internos.
- Rede Pública Wi-Fi, dedicada a visitantes e usuários externos.
- Pontos de Acesso Wi-Fi (APs) segmentados, sendo:
  - 1 AP para a rede Operacional (uso interno).
  - 1 AP para a rede Pública (uso de visitantes).
  - 1 AP para o Laboratório (uso comunitário).

- 1 Servidor dedicado, configurado para prover os serviços de DHCP e FTP em cada filial.
- 1 Switch de Distribuição, responsável pela conexão dos equipamentos locais e integração com o roteador WAN.

As redes foram segmentadas em sub-redes Operacionais e sub-rede Públicas e Laboratório, com escopos de DHCP próprios para cada filial, conforme detalhado na Tabela 1.

#### LAN Operacional – Filiais (Classe B)

- Filial 1: IP Address 172.16.201.0
- Filial 2: IP Address 172.16.202.0
- Filial 3: IP Address 172.16.203.0
- Filial 4: IP Address 172.16.204.0
- Filial 5: IP Address 172.16.205.0

#### LAN Pública / Laboratórios - Filiais (Classe C)

- Filial 1: IP Address 192.168.201.0
- Filial 2: IP Address 192.168.202.0
- Filial 3: IP Address 192.168.203.0
- Filial 4: IP Address 192.168.204.0
- Filial 5: IP Address 192.168.205.0

## 1.6 Planilha de equipamentos

A planilha de equipamentos tem um papel fundamental no desenvolvimento do projeto de rede estruturada da Cred Vale Doce. Ela proporciona uma visão clara das necessidades para a implementação do projeto conforme disposto nas Figuras 11 e 12:

**Figura 11 – Planilha de Inventário de Equipamentos - Matriz**

Planilha de Inventário de Equipamentos - Cooperativa/ Matriz						
Tipo Ativo	Modelo	Fabricante	Setor	Quantidade	Valor	Valor Total
Roteador Principal	C8200-1N-4T	Cisco	CPD / Infraestrutura	1	R\$ 15.000,00	R\$ 15.000,00
Switch de Distribuição	Catalyst C9200L-24T-4G	Cisco	CPD / Infraestrutura	1	R\$ 8.000,00	R\$ 8.000,00
Switch de Acesso	Catalyst WS-C2960S-24TS-L 24P Giga	Cisco	CPD / Infraestrutura	3	R\$ 1.450,00	R\$ 4.350,00
Access Point	Catalyst 9115AX C9115AXI-Z	Cisco	Todos	3	R\$ 3.600,00	R\$ 10.800,00
Servidor Central	PowerEdge R450	Dell	CPD / Infraestrutura	1	R\$ 18.000,00	R\$ 18.000,00
Computador	OptiPlex 7000	Dell	Operacional / Diretoria	15	R\$ 6.000,00	R\$ 90.000,00
Computador	OptiPlex 5000	Dell	Atendimento / Laboratório ( 10 )	40	R\$ 3.800,00	R\$ 152.000,00
Notebook	Latitude 5440	Dell	TI / Diretoria	5	R\$ 5.500,00	R\$ 27.500,00
Nobreak (Rack)	Nobreak Rack APC Smart-UPS RT 6Kva - SRT6KXL	APC		1	R\$ 19.000,00	R\$ 19.000,00
Rack 44U	Rack 44U Fechado	Lightera (Furukawa)		1	R\$ 2.700,00	R\$ 2.700,00
Patch Panel	Cat6A 24p	Lightera (Furukawa)		5	R\$ 994,00	R\$ 4.970,00
Guia de cabo	Guia de cabo horizontal fechado metálico	Lightera (Furukawa)		5	R\$ 150,00	R\$ 750,00
Patch Cord	Kit Cabo de rede 1m Cat6A - c/20und.	Lightera (Furukawa)		8	R\$ 217,60	R\$ 1.740,80
Cabo de Rede	Caixa de cabo de rede Cat6A - c/305m.	Lightera (Furukawa)		5	R\$ 971,85	R\$ 4.859,25
Conector	RJ45 Cat6A - c/25und.	Lightera (Furukawa)		6	R\$ 110,00	R\$ 660,00
Caixa de Conexão	Conector fêmea RJ45 Cat6A	Lightera (Furukawa)		75	R\$ 22,00	R\$ 1.650,00
Canaletas	2m.	Genérico		375	R\$ 47,40	R\$ 17.775,00
Storage/NAS (Backup e arquivos compartilhados)	ME5024	Dell		1	R\$ 60.293,00	R\$ 60.293,00

Fonte: Elaborada pelos autores

**Figura 12 – Planilha de Inventário de Equipamentos - Filiais**

Planilha de Inventário de Equipamentos - Cooperativa/ Filial 1						
Tipo Ativo	Modelo	Fabricante	Setor	Quantidade	Valor	Valor Total
Roteador de Borda	ISR 1111-8P	Cisco	Infraestrutura da Filial	1	R\$ 4.000,00	R\$ 4.000,00
Switch de Acesso	Catalyst WS-C2960S-24TS-L 24P Giga	Cisco	Infraestrutura da Filial	1	R\$ 1.450,00	R\$ 1.450,00
Access Point	Catalyst 9115AX C9115AXI-Z	Cisco	Todos	3	R\$ 3.600,00	R\$ 10.800,00
Servidor de Filial	PowerEdge T150	Dell	Infraestrutura da Filial	1	R\$ 7.000,00	R\$ 7.000,00
Computador	OptiPlex 5000	Dell	Atendimento / Laboratório ( 5 )	18	R\$ 3.800,00	R\$ 68.400,00
Notebook	Latitude 3440	Dell	TI / Gerência	2	R\$ 4.800,00	R\$ 9.600,00
Nobreak (Rack)	Nobreak Rack APC Smart-UPS RT 6Kva - SRT6KXL	APC		1	R\$ 19.000,00	R\$ 19.000,00
Rack 44U	Rack 44U Fechado	Lightera (Furukawa)		1	R\$ 2.700,00	R\$ 2.700,00
Patch Panel	Cat6A 24p	Lightera (Furukawa)		1	R\$ 994,00	R\$ 994,00
Guia de cabo	Guia de cabo horizontal fechado metálico	Lightera (Furukawa)		2	R\$ 150,00	R\$ 300,00
Patch Cord	Kit Cabo de rede 1m Cat6A - c/20und.	Lightera (Furukawa)		3	R\$ 217,60	R\$ 652,80
Cabo de Rede	Caixa de cabo de rede Cat6A - c/305m.	Lightera (Furukawa)		3	R\$ 971,85	R\$ 2.915,55
Conector	RJ45 Cat6A - c/25und.	Lightera (Furukawa)		3	R\$ 110,00	R\$ 330,00
Caixa de Conexão	Conector fêmea RJ45 Cat6A	Lightera (Furukawa)		25	R\$ 22,00	R\$ 550,00
Canaletas	2m.	Genérico		188	R\$ 47,40	R\$ 8.911,20

Fonte: Elaborada pelos autores

## 1.7 Cálculo de links de Dados e de Internet

A planilha Cálculo de Links de Dados e de Internet apresenta o dimensionamento da largura de banda necessária para atender às demandas de comunicação da Cooperativa de Crédito Cred Vale Doce, considerando a matriz, localizada em Guanhães – MG, e suas cinco filiais distribuídas nas cidades de Conceição do Mato Dentro, Serro, Virginópolis, Diamantina e Governador Valadares.

O dimensionamento leva em conta o tráfego gerado pelos principais serviços e aplicações corporativas utilizados pela cooperativa e essa análise fornece uma visão clara e detalhada da capacidade de tráfego necessária em cada unidade, sendo uma ferramenta essencial para o planejamento da rede, a contratação de links de dados adequados e a garantia de desempenho e conectividade estável entre matriz e filiais.

O resultado do cálculo e o dimensionamento proposto podem ser observados na Figura

13.

**Figura 13 – Planilha de Cálculo de Links de Dados e de Internet**

Cálculo de Links de dados e de Internet													
Necessidades Corporativas		Matriz = 50		Filial 1 = 15		Filial 2 = 15		Filial 3 = 15		Filial 4 = 15		Filial 5 = 15	
Aplicação	Requisitos (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)
Internet Banking	1200	35	42000	12	14400	12	14400	12	14400	12	14400	12	14400
Videoconferência	1800	16	28800	5	9000	5	9000	5	9000	5	9000	5	9000
Sistema Legado	200	50	10000	15	3000	15	3000	15	3000	15	3000	15	3000
Suporte Remoto	800	5	4000	2	1600	2	1600	2	1600	2	1600	2	1600
Web	1600	25	40000	8	12800	8	12800	8	12800	8	12800	8	12800
E-mail	400	25	10000	7	2800	7	2800	7	2800	7	2800	7	2800
	Total App	42800	Total App	13600	Total App	13600	Total App						
	Total Internet	92000	Total Internet	30000	Total Internet	30000	Total Internet						
	Link Internet	Link Matriz <-> Filial 1	68000	Filial 1 <-> Filial 2	54400	Filial 2 <-> Filial 3	40800	Filial 3 <-> Filial 4	40800	Filial 4 <-> Filial 5	54400	Filial 5 <-> Matriz	68000
Redutor capacid.	1	242000											

Fonte: Elaborada pelos autores

## 2 PREPARAÇÃO DO AMBIENTE EM NUVEM E VIRTUALIZAÇÃO LOCAL

A preparação do ambiente envolveu a criação de máquinas virtuais locais e instâncias em nuvem. Essa abordagem possibilitou o estudo prático de virtualização, redes e serviços em diferentes contextos de hospedagem.

### 2.1 Serviços em Máquinas Virtuais Locais pelo VirtualBox

No ambiente local, utilizou-se o VirtualBox para criar e configurar máquinas virtuais com diferentes sistemas operacionais.

#### 2.1.1 Serviço DHCP (Dynamic Host Configuration Protocol)

O Servidor DHCP (Dynamic Host Configuration Protocol) é um protocolo de rede utilizado para atribuir automaticamente endereços IP e outras configurações de rede, como máscara de sub-rede, gateway padrão e servidores DNS, aos dispositivos conectados.

No contexto da Cooperativa de Crédito, foi configurada uma arquitetura em que uma matriz atua como Servidor DHCP e as filiais operam como Cliente DHCP.

Com essa configuração ele simplifica a administração da rede, evitando a necessidade de configuração manual em cada máquina e garantindo que não haja conflitos de endereços IP entre os dispositivos.

#### 2.1.1.1 Topologia da Arquitetura

O ambiente foi configurado utilizando os sistemas operacionais Ubuntu Server 22.04 LTS e Windows Server 2025, como descrito na tabela 1, que forneceram a base necessária para

a instalação, execução e testes dos serviços implementados durante o projeto.

**Tabela 1 – Máquinas utilizadas para o DHCP**

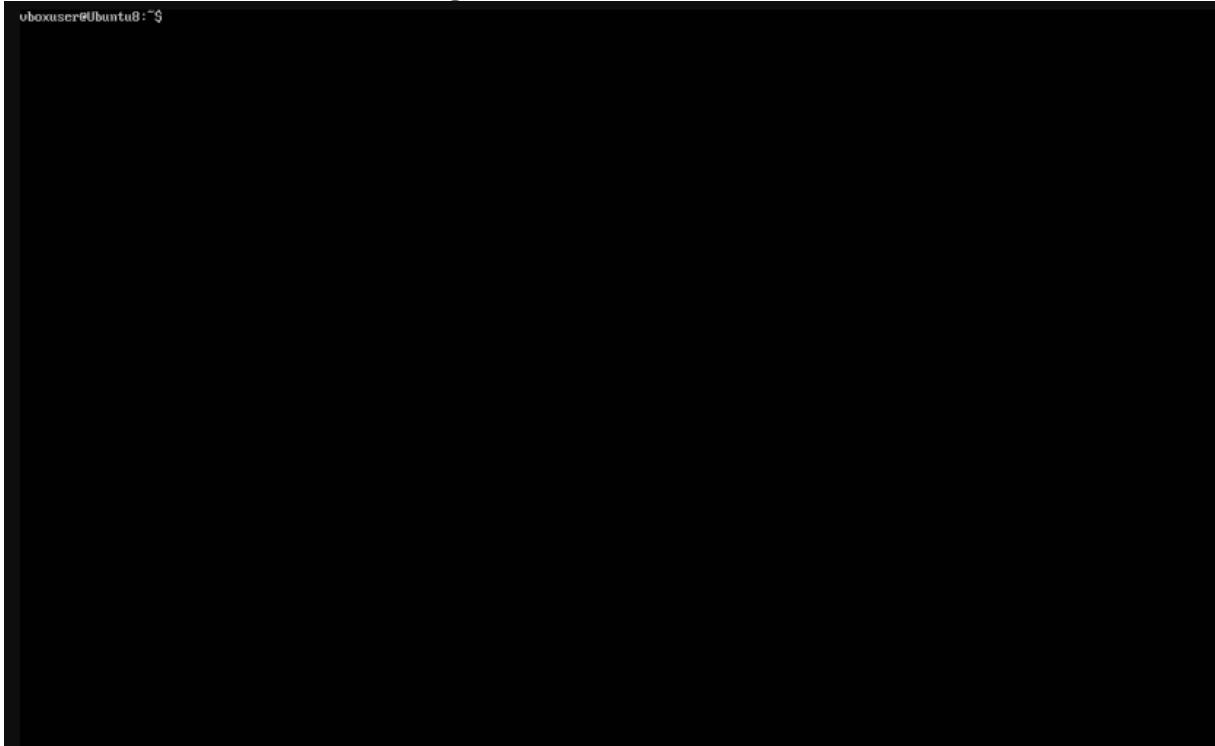
Função	Nome da Máquina	IPV4	Papel
Servidor	DHCP Server	192.168.1.1	Servidor de DHCP
Cliente	Cliente Windows	192.168.1.51	Máquina cliente

**Fonte:** Elaborada pelos autores.

### *2.1.1.2 Máquina Virtual*

Foi criada uma máquina virtual local no Virtual Box (Figura 14) para atuar como Servidor DHCP da Matriz da Cooperativa de Crédito. A instância foi feita utilizando o Ubuntu Server 22.04 LTS como sistema operacional e com Windows Server 2025 como cliente que irá se conectar a rede.

**Figura 14 – Servidor DHCP**



**Fonte:** Elaborada pelos autores.

Essa máquina representa o servidor DHCP da Cooperativa, responsável por disponibilizar informações de IP para os computadores que se conectam ao server.

A configuração foi realizada de forma que os arquivos estivessem na pasta /etc/netplan/00-installer-config.yaml, permitindo que o server tenha acesso as configurações estipuladas. Endereços de IP: 192.168.1.1/24, Gateway padrão: 10.0.2.15, DNS's padrão primário e secundários: 8.8.8.8, 1.1.1.1.

### 2.1.1.3 Configuração do Servidor DHCP

A visualização das Interfaces do Sistema é feita por meio do comando "ifconfig", o resultado pode ser visto na Figura 15.

**Figura 15 – Resultado do comando "ifconfig"**

```
vboxuser@Ubuntu8:~$ Ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:a00:27ff:fe55:b9cc  prefixlen 64  scopeid 0x0<global>
          inet6 fe80::a00:27ff:fe55:b9cc  prefixlen 64  scopeid 0x20<link>
            ether 08:00:27:55:b9:cc  txqueuelen 1000  (Ethernet)
              RX packets 13158  bytes 17723208 (17.7 MB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 1826  bytes 138639 (138.6 KB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe5b:744b  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:5b:74:4b  txqueuelen 1000  (Ethernet)
            RX packets 1876  bytes 139719 (139.7 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 208  bytes 16270 (16.2 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
            RX packets 396  bytes 39680 (39.6 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 396  bytes 39680 (39.6 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

vboxuser@Ubuntu8:~$ _
```

**Fonte:** Elaborada pelos autores.

A tela do comando ifconfig no Ubuntu, mostra informações detalhadas sobre todas as interfaces de rede do sistema, incluindo: Nome da Interface, Endereço IPv4, Máscara de sub-rede, Endereço IPv6, Endereço MAC, Status da Interface, Pacotes enviados e recebidos, e Informações de broadcast e multicast. Redes configuradas: enp0s3 - IP 10.0.2.15 enp0s8 - IP 192.168.1.1

A instalação do serviço foi realizada com o comando "sudo apt install isc-dhcp-server -y".

A configuração do arquivo na pasta netplan foi feita com o comando "sudo nano /etc/netplan/00-instaler-config.yaml", o conteúdo do arquivo é demostrado na Figura 16.

**Figura 16 – Arquivo de configuração do netplan**

```
GNU nano 7.2
/etc/netplan/00-installer-config.yaml
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      dhcp4: false
      addresses: [192.168.1.1/24]
      gateway4: 10.0.2.15
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
  version: 2
```

**Fonte:** Elaborada pelos autores.

Para garantir que o servidor mantenha IP fixo na sua interface, foi configurado o arquivo de rede /etc/netplan00-instaler-config.yaml. Na tela, vemos duas interfaces de rede configuradas.

A enp0s3 está com o DHCP ativado (dhcp4: true), ou seja, o endereço IP é obtido automaticamente do servidor DHCP. E a enp0s8 está com o DHCP desativado (dhcp4: false), então foi configurado manualmente com: Endereço IP fixo: 192.168.1.1/24 Gateway: 10.0.2.15 Servidores DNS: 8.8.8.8 e 1.1.1.1.

A configuração do serviço foi feita com "sudo nano /etc/dhcp/dhcpd.conf", como visto nas Figuras 17 e 18.

**Figura 17 – Arquivo de configuração do serviço 1**

```
GNU nano 7.2
# dhcpcd.conf
#
# Sample configuration file for ISC dhcpcd
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

#subnet 10.254.239.0 netmask 255.255.255.224 {
#    range 10.254.239.10 10.254.239.20;
#    option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#    range dynamic-bootp 10.254.239.40 10.254.239.60;
#    option broadcast-address 10.254.239.31;
#    option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#    range 10.5.5.26 10.5.5.30;
#    option domain-name-servers ns1.internal.example.org;
#    option domain-name "internal.example.org";
#    option subnet-mask 255.255.255.224;
#    option routers 10.5.5.1;
#    option broadcast-address 10.5.5.31;
#    default-lease-time 600;
#    max-lease-time 7200;
#}

# Hosts which require special configuration options can be listed in
# host statements. If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.

#host passacaglia {
#    hardware ethernet 0:0:c0:5d:bd:95;
#    filename "vmlinix.passacaglia";
#    server-name "toccata.example.com";
#}

# Fixed IP addresses can also be specified for hosts. These addresses
# should not also be listed as being available for dynamic assignment.
```

**Fonte: Elaborada pelos autores.**

**Figura 18 – Arquivo de configuração do serviço 2**

```
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.  Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
#host fantasia {
#    hardware ethernet 08:00:07:26:c0:a5;
#    fixed-address fantasia.example.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.  The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#    match if substring(option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#    subnet 10.17.224.0 netmask 255.255.255.0 {
#        option routers rtr-224.example.org;
#    }
#    subnet 10.0.29.0 netmask 255.255.255.0 {
#        option routers rtr-29.example.org;
#    }
#    pool {
#        allow members of "foo";
#        range 10.17.224.10 10.17.224.250;
#    }
#    pool {
#        deny members of "foo";
#        range 10.0.29.10 10.0.29.230;
#    }
#}
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.11 192.168.1.254;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8, 1.1.1.1;
    option domain-name "example.org";
}
```

**Fonte:** Elaborada pelos autores.

A tela mostra a configuração do serviço DHCP através do arquivo /etc/dhcp/dhcpd.conf, foi configurada a rede 192.168.1.0 com máscara 255.255.255.0, onde o range de IP's vai de 192.168.1.11 a 192.168.1.254, o gateway definido foi 192.168.1.1 e os servidores DNS's são 8.8.8.8, 1.1.1.1 e o domínio example.org.

A configuração da interface de rede foi feita com "sudo nano /etc/default/isc-dhcp-server", exposta na Figura 19.

**Figura 19 – Arquivo de configuração da interface de rede**

```
GNU nano 7.2
/etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)
# Path to dhcpcd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf
# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDv4_PID=/var/run/dhcpcd.pid
#DHCPDv6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#   Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#   Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s8"
INTERFACESv6=""
```

**Fonte:** Elaborada pelos autores.

Para definir qual interface de rede será responsável por distribuir o range de IP's configurado no servidor DHCP, é utilizado o comando sudo nano /etc/default/isc-dhcp-server para abrir o arquivo de configuração para informar a interface. Como eu só possuo a INTERFACEv4, eu coloco “enp0s8” para a interface que eu quero entregar esses IP's.

Por fim o serviço foi reiniciado com "sudo service isc-dhcp-server restart"

#### 2.1.1.4 Configuração do Cliente DHCP

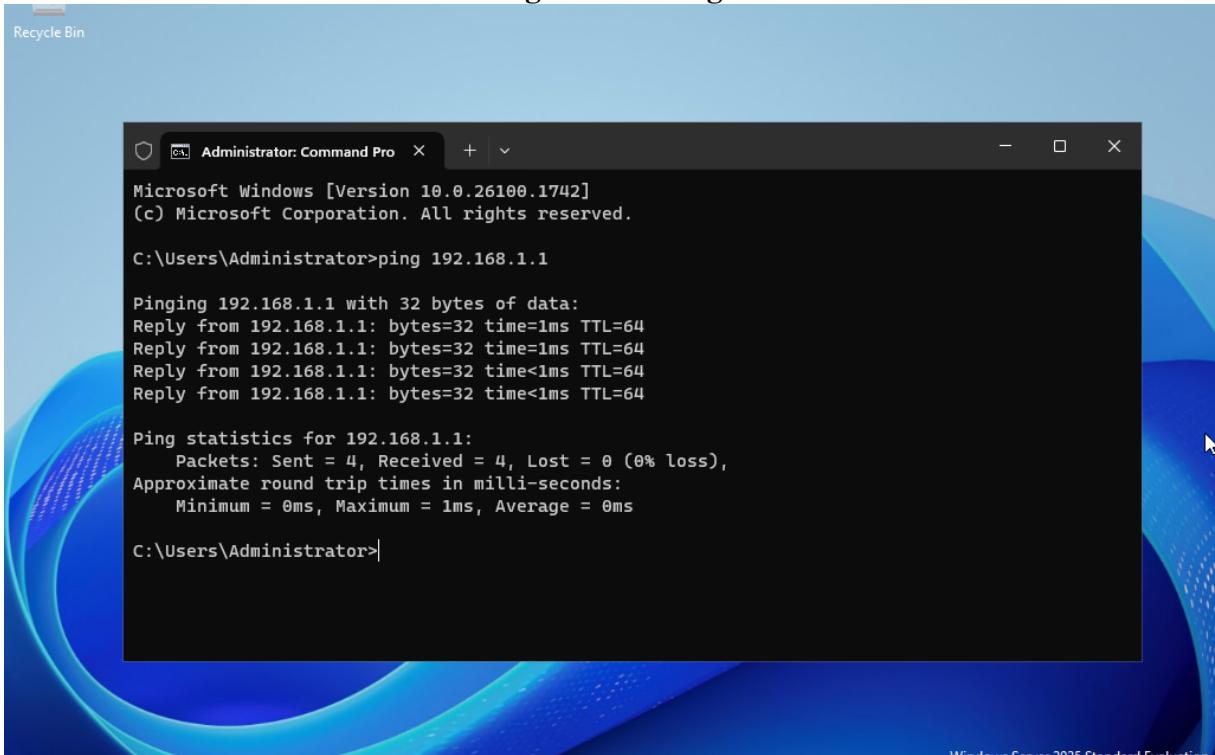
Para realizar as configurações acesei as configurações da Ethernet e defini as opções de IP e DNS para obtenção automática.

#### 2.1.1.5 Teste de Funcionamento e Acesso

No Windows, para validar o funcionamento do servidor DHCP, o acesso foi realizado diretamente pelo usuário, utilizando o IP e DNS automáticos.

Podemos testar a comunicação entre a máquina Windows e a máquina Ubuntu utilizando o comando ping 192.168.1.1 (Figura 20), pois ambas estão conectadas à mesma rede.

**Figura 20 – Ping**



```
Administrator: Command Pro
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
```

**Fonte: Elaborada pelos autores.**

Com o comando ipconfig podemos visualizar o IP (Figura 21), que corresponde ao mesmo IP configurado na máquina server.

**Figura 21 – Resultado "ipconfig"**

Microsoft Windows [Version 10.0.26100.1742]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : exemplo.org  
Link-local IPv6 Address . . . . . : fe80::9915:410e:a15f:61b1%15  
IPv4 Address . . . . . : 192.168.1.51  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1

C:\Users\Administrator>

Windows Server 2025 Standard Evaluation  
Windows License valid for 180 days  
Build 26100.ge\_release.240331-1435

19:30 14/10/2025

**Fonte: Elaborada pelos autores.**

No Ubuntu, após reiniciar a máquina com o comando "sudo service isc-dhcp-server restart", e verificar o status da mesma com "sudo service isc-dhcp-server status", podemos ver (Figura 22) que o servidor está active “(running)”, ou seja, funcionando corretamente.

**Figura 22 – Verificações DHCP**

```
vboxuser@Ubuntu8:~$ sudo service isc-dhcp-server restart
vboxuser@Ubuntu8:~$ sudo service isc-dhcp-server status
● isc-dhcp-server.service - ISC DHCP IPv4 server
  Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-10-15 23:05:36 UTC; 8s ago
    Docs: man:dhcpd(8)
   Main PID: 2565 (dhcpd)
      Tasks: 1 (limit: 3984)
     Memory: 3.8M (peak: 4.1M)
        CPU: 33ms
       CGroup: /system.slice/isc-dhcp-server.service
           └─2565 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf enp0s8

Oct 15 23:05:36 Ubuntu8 dhcpd[2565]: PID file: /run/dhcp-server/dhcpd.pid
Oct 15 23:05:36 Ubuntu8 dhcpd[2565]: Wrote 1 leases to leases file.
Oct 15 23:05:36 Ubuntu8 sh[2565]: Wrote 1 leases to leases file.
Oct 15 23:05:36 Ubuntu8 dhcpd[2565]: Listening on LPF/enp0s8/08:00:27:5b:74:4b/192.168.1.0/24
Oct 15 23:05:36 Ubuntu8 sh[2565]: Listening on LPF/enp0s8/08:00:27:5b:74:4b/192.168.1.0/24
Oct 15 23:05:36 Ubuntu8 sh[2565]: Sending on LPF/enp0s8/08:00:27:5b:74:4b/192.168.1.0/24
Oct 15 23:05:36 Ubuntu8 sh[2565]: Sending on Socket/fallback/fallback-net
Oct 15 23:05:36 Ubuntu8 dhcpd[2565]: Sending on LPF/enp0s8/08:00:27:5b:74:4b/192.168.1.0/24
Oct 15 23:05:36 Ubuntu8 dhcpd[2565]: Sending on Socket/fallback/fallback-net
Oct 15 23:05:36 Ubuntu8 dhcpd[2565]: Server starting service.
```

**Fonte: Elaborada pelos autores.**

### 2.1.2 Serviço AD (Active Directory)

O Servidor AD (Active Directory) na CredValeDoce foi pensado para ser uma estrutura centralizada, que será utilizada para organizar e gerenciar os recursos de rede, como compu-

tadores, grupos, usuários e para o gerenciamento de permissões e políticas de segurança. Isso permite que a cooperativa de crédito tenha mais segurança em relação as suas informações e garante que apenas pessoas autorizadas possam ter acesso a dados sensíveis. Sendo assim o AD facilita a administração da rede, dando mais padronização, agilidade e segurança aos processos internos da CVD.

#### *2.1.2.1 Topologia da Arquitetura*

Nas duas máquinas configuradas foi utilizado o sistema operacional Windows, no servidor utilizou-se o Windows Server 2025 e no cliente utilizou-se o Windows 7 Ultimate, detalhado na Tabela 2.

**Tabela 2 – Máquinas utilizadas para o AD**

Função	Nome da Máquina	IPV4	Papel
Servidor	AD Server	176.16.100.2	Servidor de AD
Cliente	Cliente Windows	172.168.100.20	Usuário

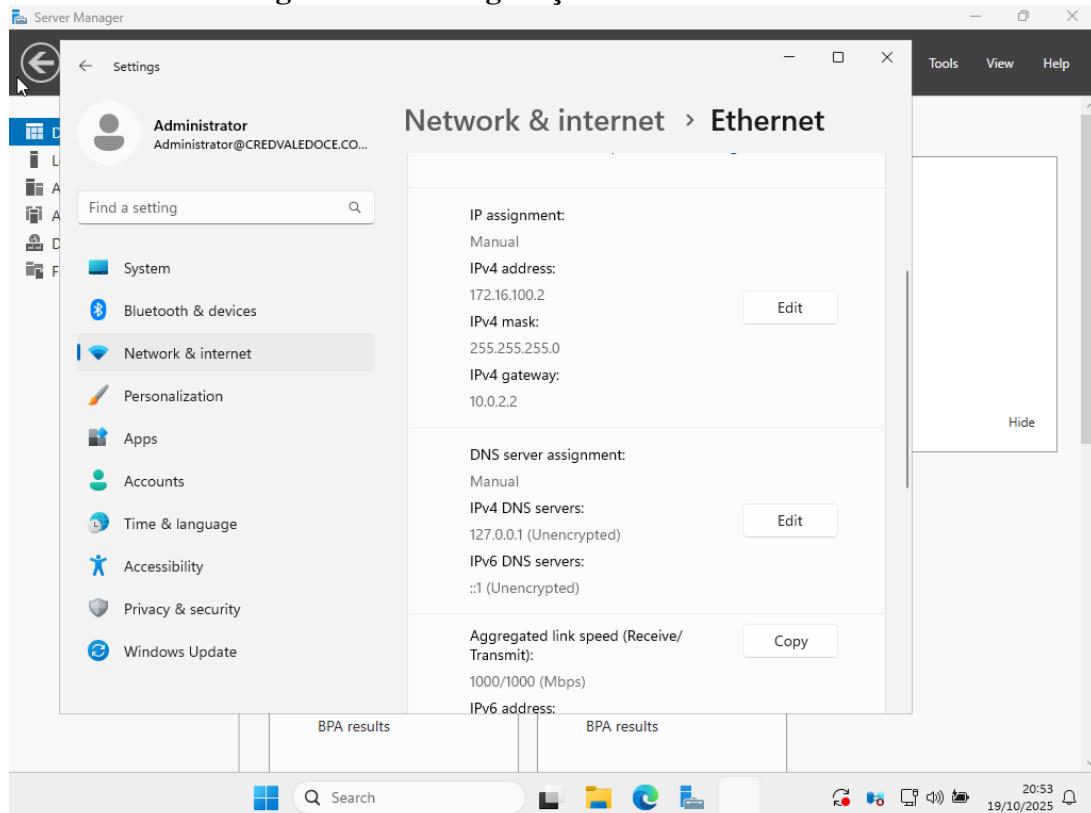
**Fonte:** Elaborada pelos autores.

#### *2.1.2.2 Máquina Virtual*

Foram criadas duas máquinas virtuais locais no Virtual Box, uma para atuar como Servidor AD da Cooperativa de Crédito e uma como cliente. As instâncias foram feitas utilizando o Windows Server 2025 para o servidor, e o Windows 7 Ultimate como usuário que irá se conectar a rede.

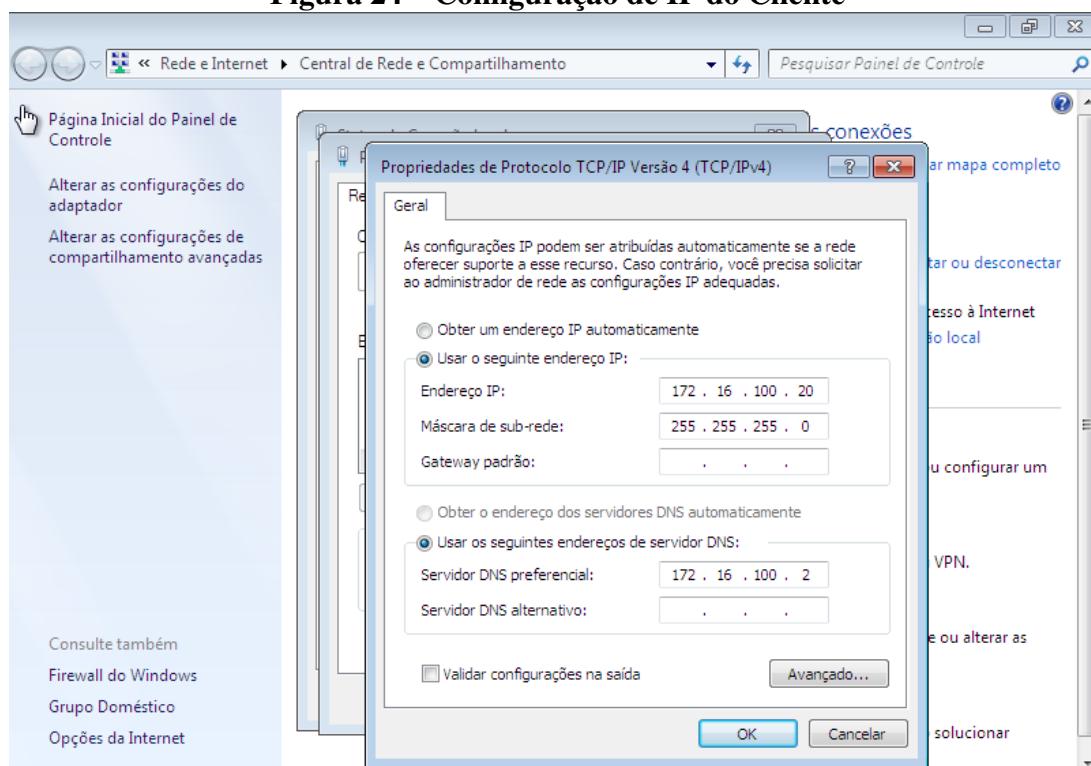
As configurações de IP utilizadas foram IP 172.16.100.2 para o server (Figura 23) e IP 172.16.100.20 para o cliente (Figura 24) e a máscara de sub-rede de ambos foi 255.255.255.0.

**Figura 23 – Configuração de IP do AD Server**



**Fonte:** Elaborada pelos autores.

**Figura 24 – Configuração de IP do Cliente**

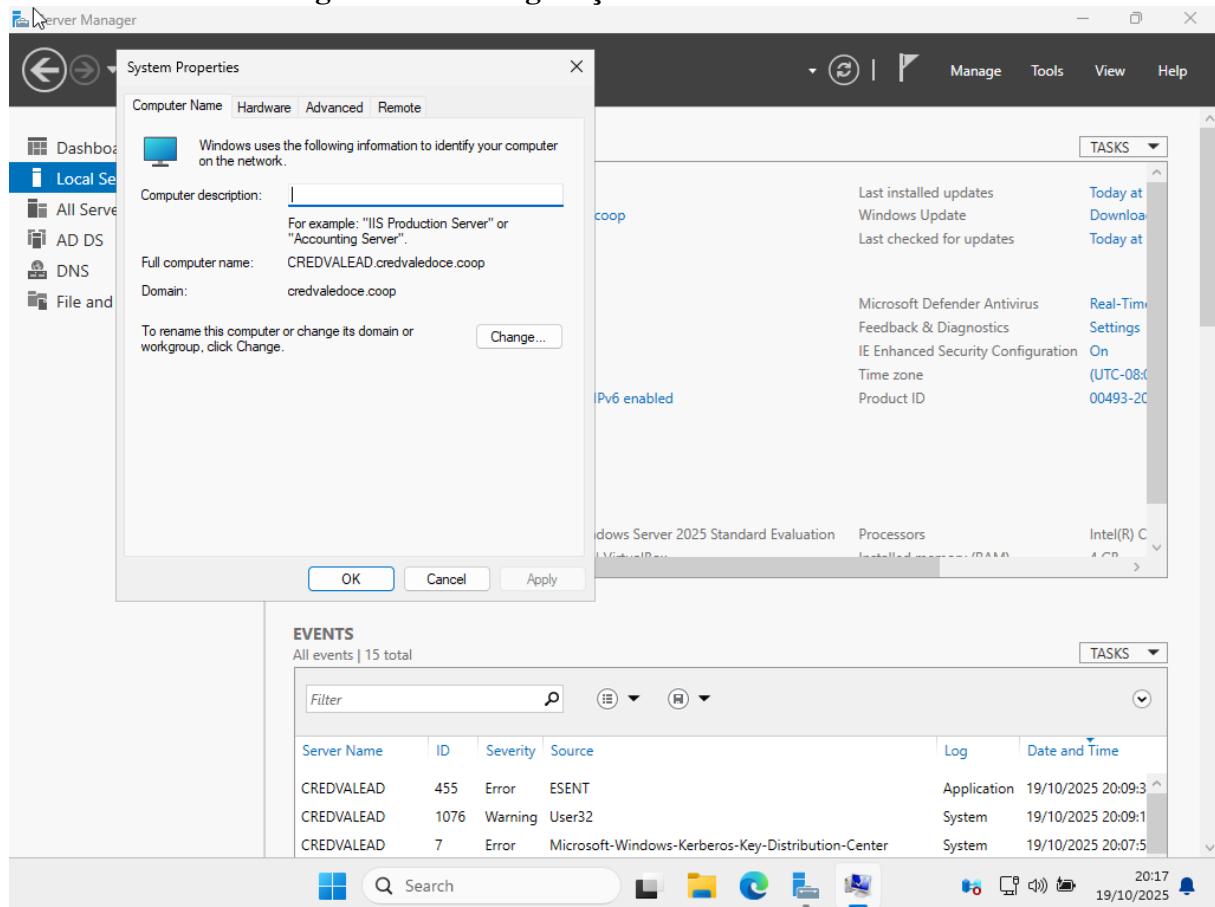


**Fonte:** Elaborada pelos autores.

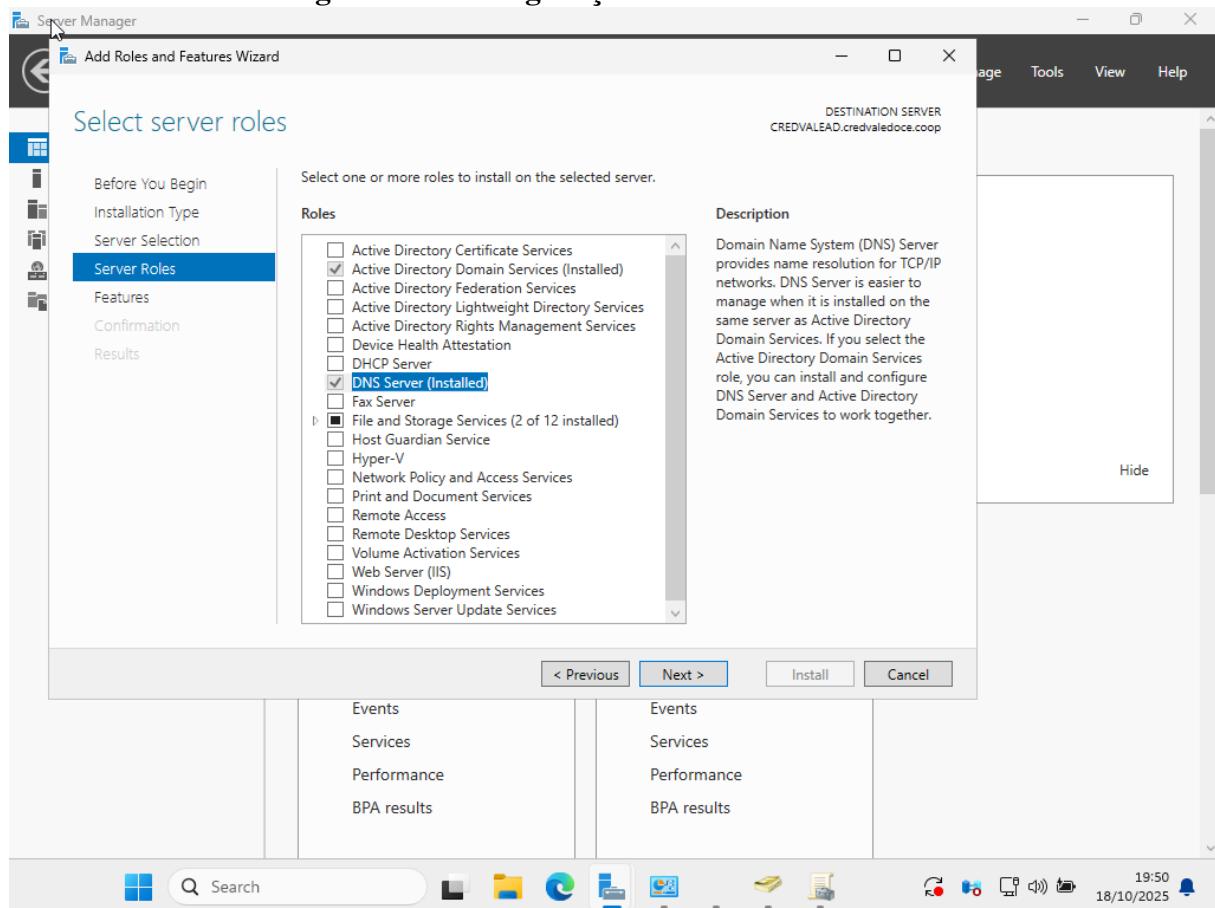
### 2.1.2.3 Instalação e Configuração do Windows Server

Para que fosse possível fazer a configuração é necessário renomear o server (Figura 25) e posteriormente instalar o AD DS no servidor (Figura 26). Mas ele requer que um servidor DNS seja instalado anteriormente. Por isso, a instalação do DNS deve ocorrer antes do AD. Depois foi feita a promoção do servidor a controlador de domínio e o domínio raiz se tornou o credvaledoce.coop.

**Figura 25 – Configurações iniciais do AD Server**



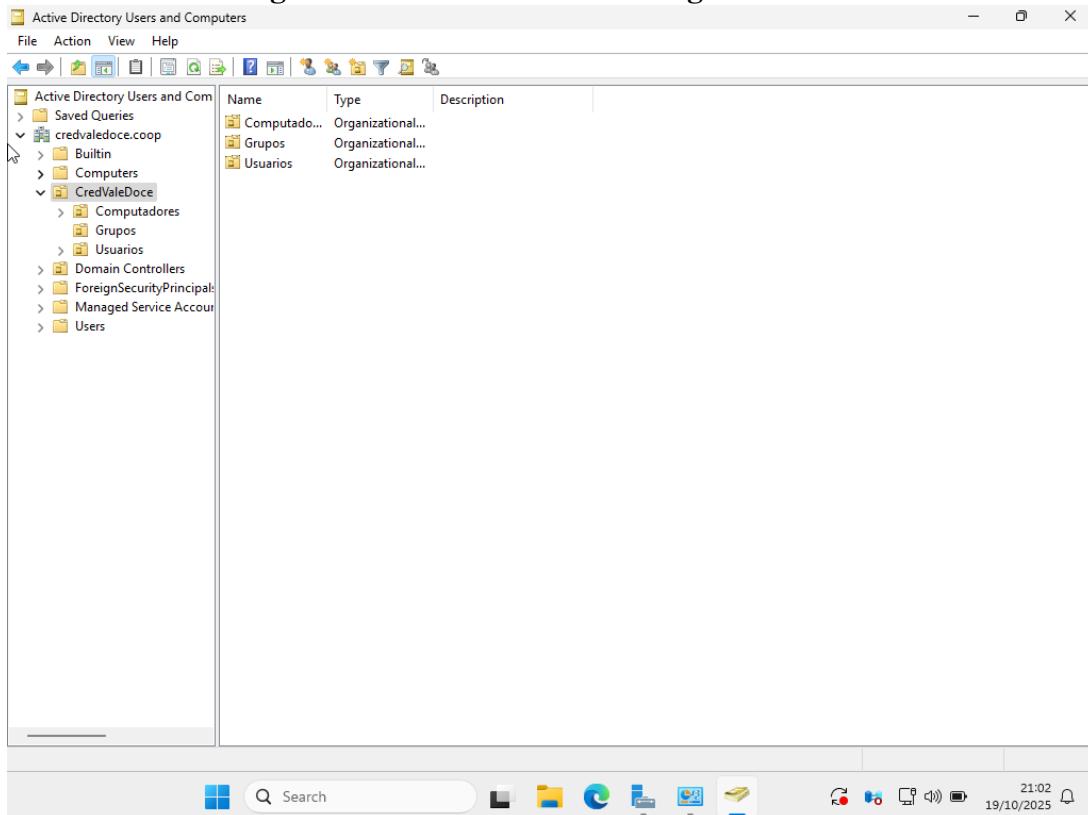
**Fonte:** Elaborada pelos autores.

**Figura 26 – Configurações iniciais do AD Server**

**Fonte:** Elaborada pelos autores.

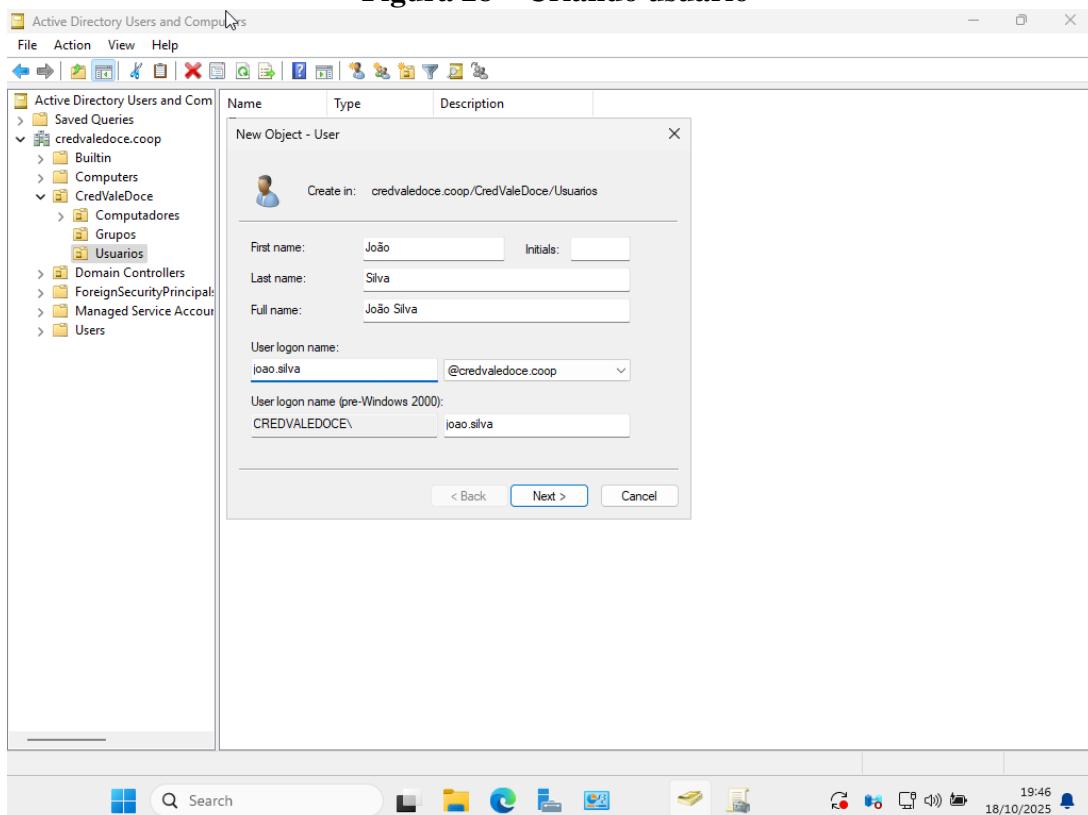
Após as configurações iniciais foi realizada a criação das unidades organizacionais (Figura 27), usuários, como visto na Figura 28, grupos e foi realizado o redirecionamento da pasta padrão de criação dos objetos computadores para a unidade organizacional criada com o comando "redircmp "OU=Computadores, OU=CredValeDoce, DC=credvaledoce, DC=coop no powershell.

**Figura 27 – Criando unidades organizacionais**



Fonte: Elaborada pelos autores.

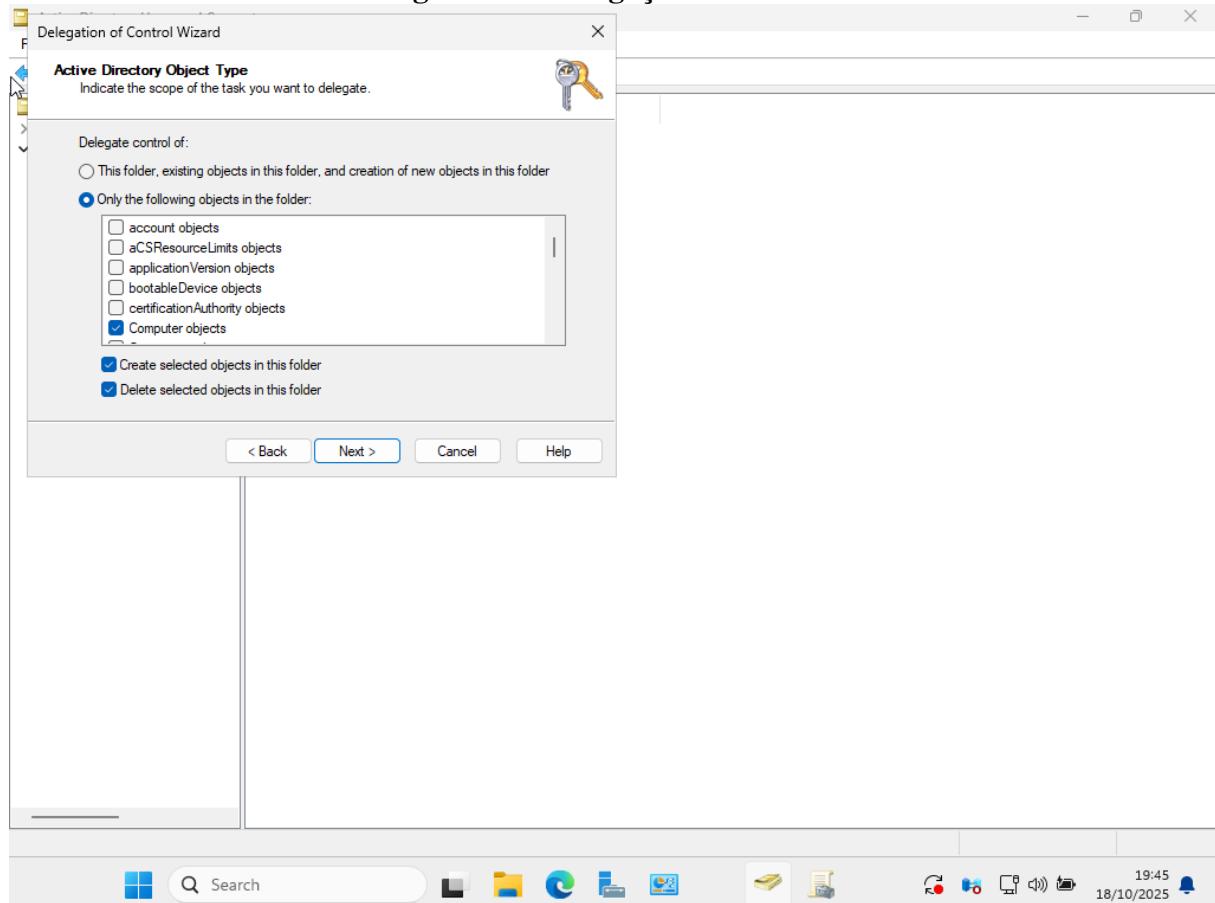
**Figura 28 – Criando usuário**



Fonte: Elaborada pelos autores.

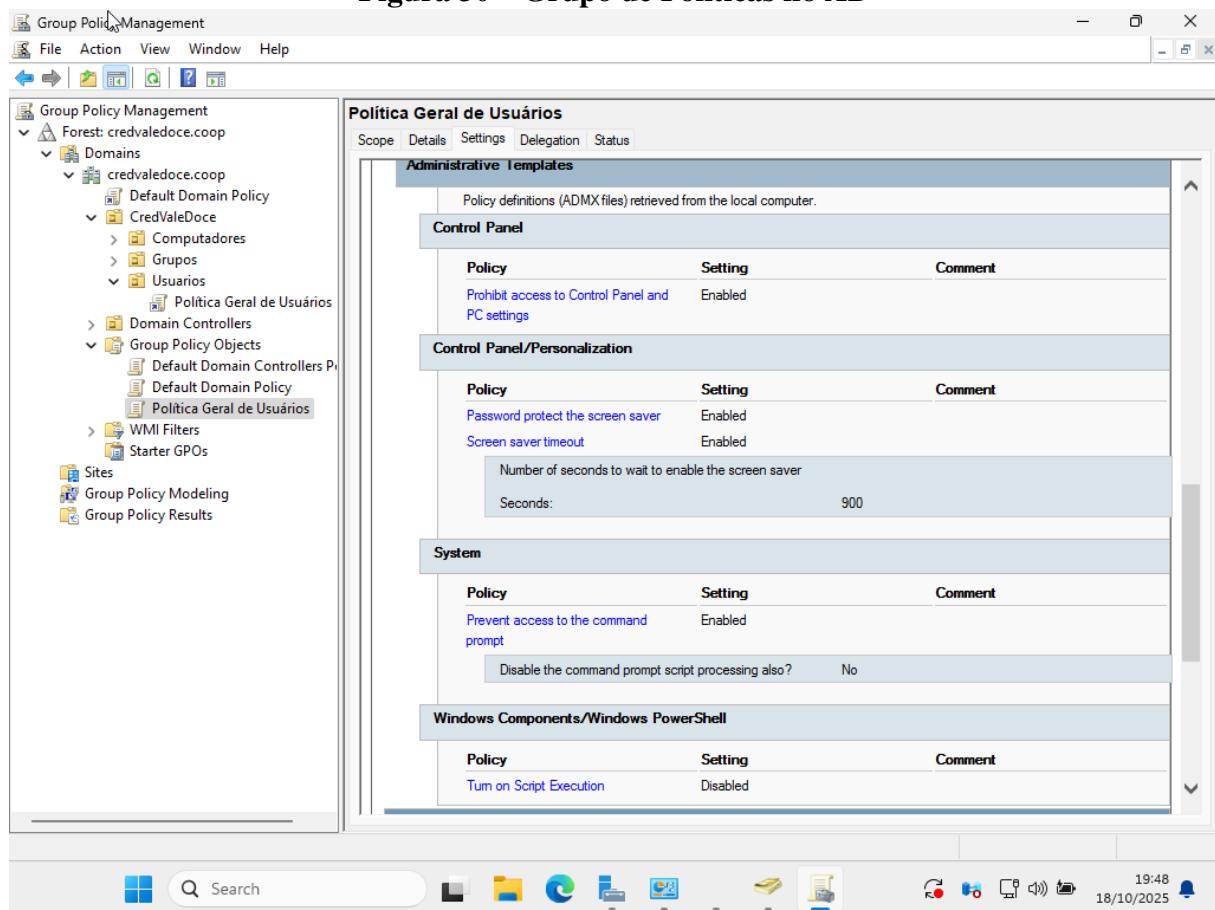
E então foi delegado ao grupo administrador o controle para criar e apagar os objetos de computador irrestritamente, como mostrado na Figura 29.

**Figura 29 – Delegação de controle**



**Fonte:** Elaborada pelos autores.

Por fim foi criado um grupo de políticas padrão que afetará todos os usuários registrados no AD. Na Figura 30 podemos ver todas as políticas aplicadas ao grupo.

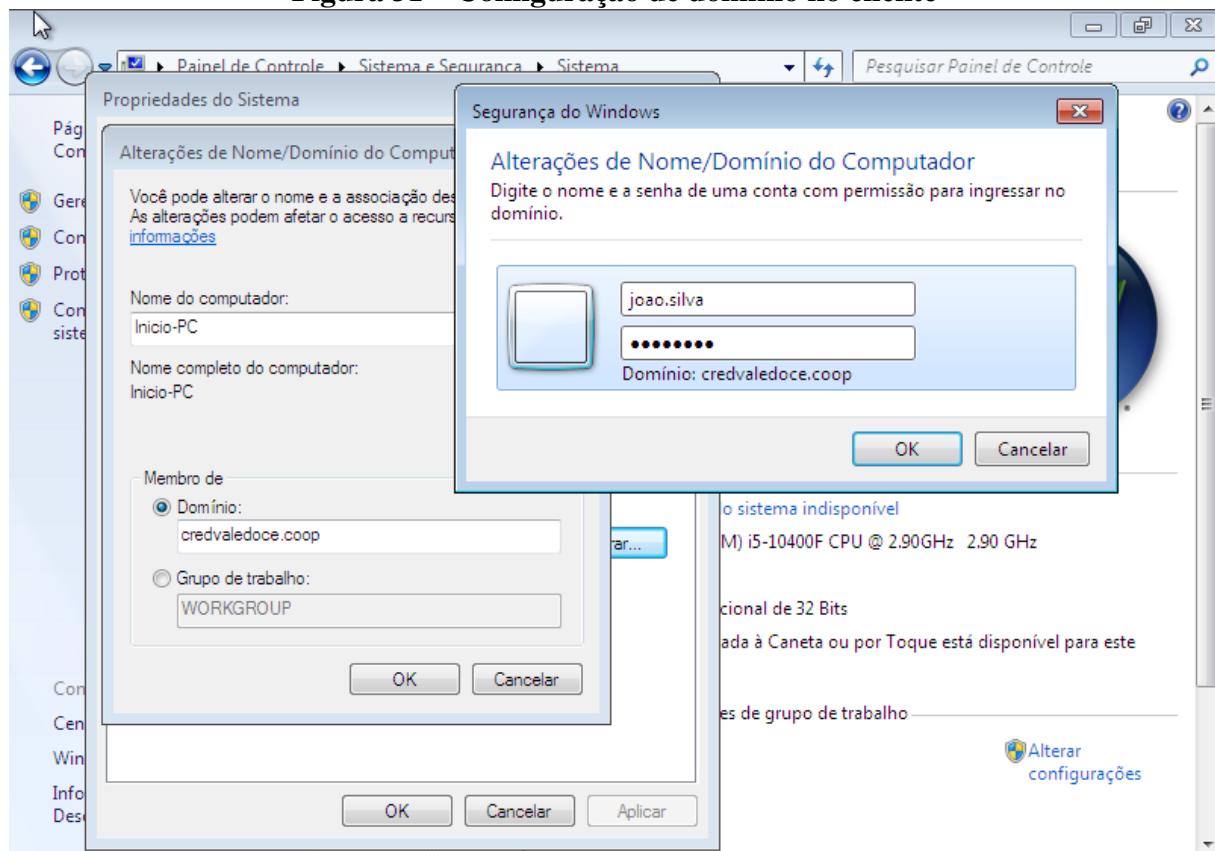
**Figura 30 – Grupo de Políticas no AD**

**Fonte:** Elaborada pelos autores.

#### 2.1.2.4 Teste de Funcionamento e Acesso Usuário Windows 7 Ultimate

Para validar o funcionamento do servidor AD, o teste foi realizado pelo usuário Windows 7 Ultimate, que como podemos observar na Figura 31 foi configurado nele o domínio credvaledoce.coop, logando com o usuário do grupo adm capaz de criar o objeto computador.

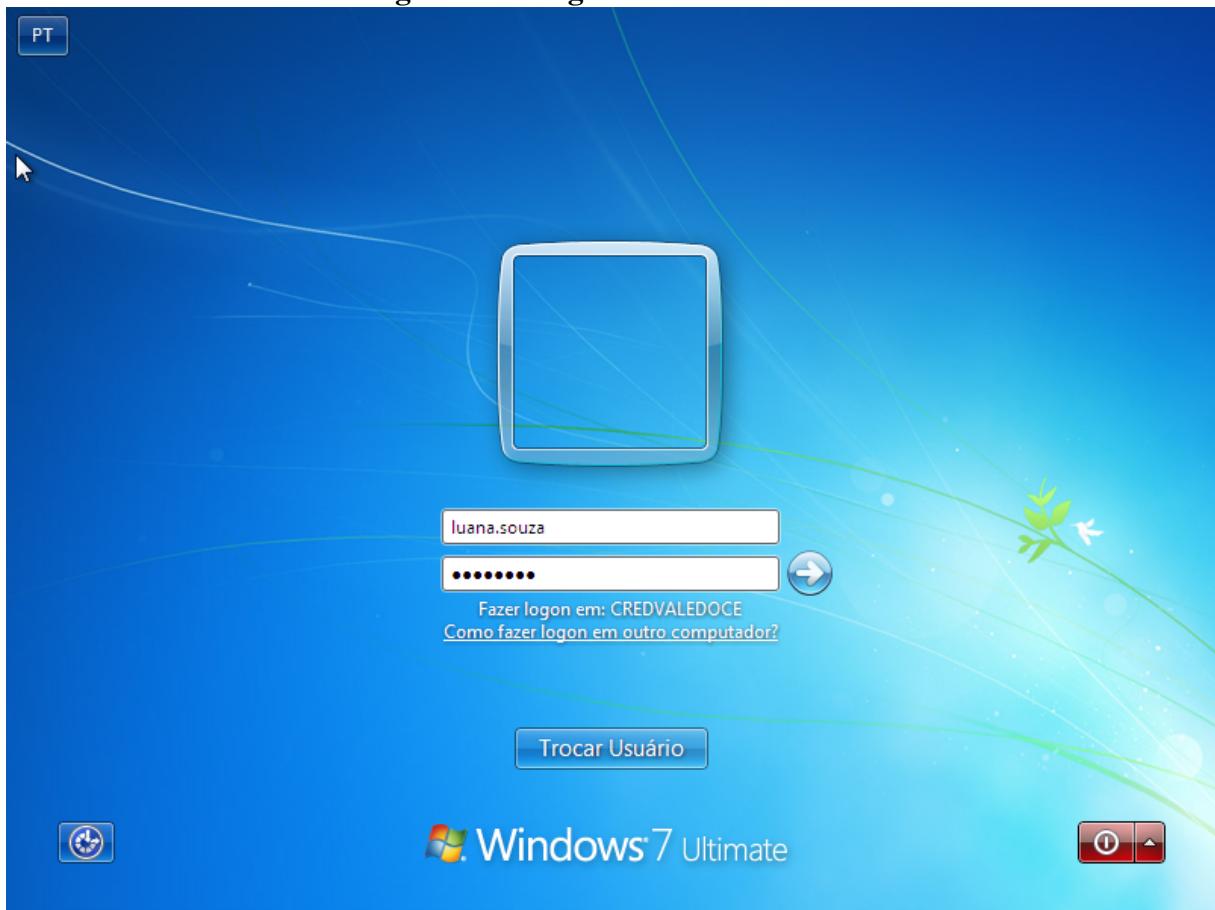
**Figura 31 – Configuração de domínio no cliente**



**Fonte:** Elaborada pelos autores.

Foi realizado o login do usuário na rede, demonstrado na Figura 32.

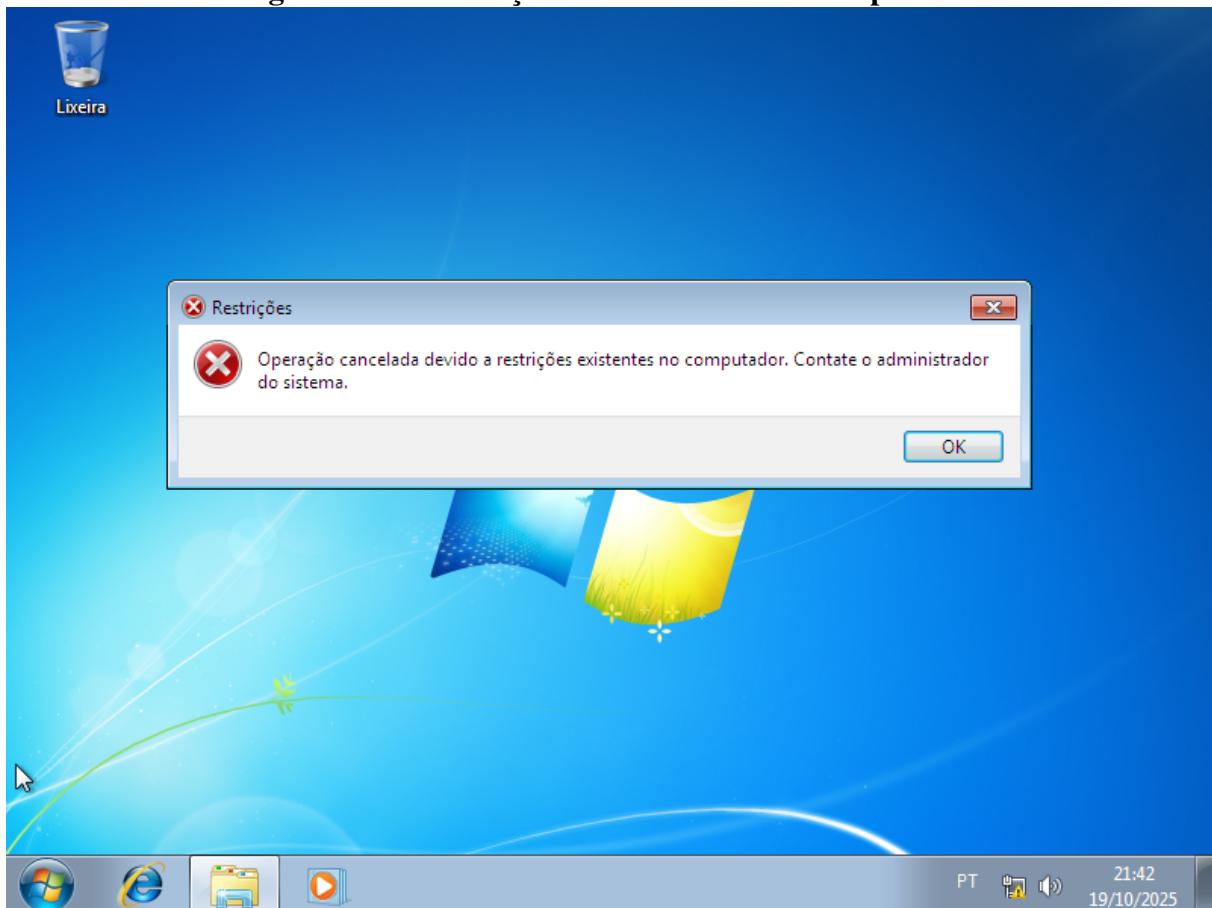
**Figura 32 – Login de usuário no AD**



**Fonte:** Elaborada pelos autores.

Podemos perceber que as políticas de grupo estão em funcionamento porque ele não consegue entrar no painel de controle, visto na Figura 33 pela janela de erro.

**Figura 33 – Verificação do funcionamento das políticas**



**Fonte:** Elaborada pelos autores.

## **2.2 Serviços em Máquinas Virtuais na Nuvem pela AWS**

Na nuvem, foram utilizadas instâncias EC2 da AWS para hospedar os serviços, possibilitando o gerenciamento remoto, a configuração de segurança e o acesso por meio de endereços públicos, simulando um ambiente de produção real.

### **2.2.1 Serviço WEB**

O Servidor Web (Apache HTTP Server) é um serviço responsável por hospedar e disponibilizar páginas e aplicações web acessíveis via navegador.

No projeto da Cooperativa de Crédito, o servidor Web foi ajustado para concentrar o acesso dos funcionários da Matriz e Filiais a um painel de informações institucional.

Através do Apache, é possível publicar sites, dashboards e sistemas internos que operam em rede local ou pela internet, com controle de acesso e fácil manutenção.

### 2.2.1.1 Topologia da Arquitetura

Ambiente configurado em uma instância AWS EC2 t3.micro, executando Ubuntu Server 22.04 LTS, com arquitetura centralizada. Utiliza rede VPC 172.31.0.0/16 e possui acesso liberado para 0.0.0.0/0, permitindo conexões externas durante a fase de testes (POC), descrito na Tabela 3.

**Tabela 3 – Máquina utilizada para o Server WEB**

Função	Nome da Máquina	IPV4 Privado	IPV4 Público	Papel
Servidor	WEB-Server	172.31.23.242	34.227.47.125	Servidor Web

**Fonte:** Elaborada pelos autores.

### 2.2.1.2 Máquina Virtual na Nuvem

Foi criada uma máquina virtual na nuvem (instância EC2) para atuar como Servidor Web da Matriz da Cooperativa de Crédito, com visto na Figura 34. Essa máquina representa o servidor web central da Cooperativa, responsável por disponibilizar informações corporativas e documentos para as filiais de forma online.

A instância foi provisionada na AWS (Amazon Web Services) utilizando o Ubuntu Server 22.04 LTS como sistema operacional.

**Figura 34 – Máquina Servidor Web**

The screenshot shows the AWS Management Console interface for the EC2 service. On the left, there's a navigation sidebar with options like 'Instâncias', 'Eventos', 'Imagens', 'Elastic Block Store', 'Rede e segurança', and 'Balancingo de carga'. The main content area is titled 'Instâncias (1/1) Informações'. It displays a table with one row for the instance 'SERVIDOR-WEB'. The table columns include 'Name' (set to 'SERVIDOR-WEB'), 'ID da Instância' (i-05484593a61ba36fc), 'Estado da instância' (executando), 'Tipo de instância' (t2.micro), 'Verificação de sa...', 'Status do alarm...', 'Zona de dispon...', 'DNS IPv4 público' (34.227.47.125), 'Endereço IP...', and 'IP elástico'. Below the table, there's a detailed view for the instance 'i-05484593a61ba36fc (UbuntuEixo5)'. This view includes tabs for 'Detalhes', 'Status e alarmes', 'Monitoramento', 'Segurança', 'Redes', 'Armazenamento', and 'Tags'. Under the 'Detalhes' tab, sections include 'Resumo da instância' (with fields like 'ID da Instância', 'Endereço IPv6', 'Tipo de nome do host', 'Nome do DNS do recurso privado de resposta', 'Endereço IP atribuído automaticamente', 'Função do IAM', 'Endereço IPv4 público', 'Estado da instância', 'Nome do DNS de IP privado (somente IPv4)', 'Tipo de instância', 'ID da VPC', 'ID da sub-rede', and 'Nome do Grupo do Auto Scaling'), 'Endereços IPv4 privados' (with '172.31.23.242'), 'DNS pública' (with 'ec2-34-236-149-1.compute-1.amazonaws.com'), and 'Endereços IP elásticos'.

**Fonte:** Elaborada pelos autores.

A configuração foi realizada de forma que o Apache hospedasse os arquivos HTML na pasta padrão do serviço /var/www/html, permitindo o acesso via navegador web através do endereço público da instância.

Para fins de prova de conceito (POC), a instância foi configurada com acesso SSH (porta 22) e HTTP (porta 80) liberados no grupo de segurança.

### 2.2.1.3 Instalação e Configuração do Apache

Primeiro a máquina foi atualizada com "sudo apt update && sudo apt upgrade -y", depois o apache2 foi instalado por meio do comando "sudo apt install apache2 -y", então o serviço foi habilitado e iniciado com "sudo systemctl enable apache2" e "sudo systemctl start apache2", respectivamente. E para verificar o funcionamento utiliza-se "sudo systemctl status apache2".

### 2.2.1.4 Configuração do Diretório e Página Web

O Apache, por padrão, utiliza o diretório /var/www/html como raiz do site. Para este projeto, foi mantido o diretório padrão e substituído o arquivo inicial index.html por uma página personalizada(Figura 35). Removendo o arquivo original com "sudo rm /var/www/html/index.html" e criando um novo com "sudo nano /var/www/html/index.html".

**Figura 35 – Conteúdo do index.html**

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Servidor</title>
</head>
<body>
    <h1>Teste Servidor</h1>
</body>
</html>
```

**Fonte:** Elaborada pelos autores.

Foi então permissionado o acesso à pasta com "sudo chown -R www-data:www-data /var/www/html" e "sudo chmod -R 755 /var/www/html". Após as configurações é necessário reiniciar o serviço com "sudo systemctl restart apache2".

### 2.2.1.5 Teste de Funcionamento e Acesso Web

Para validar o funcionamento do servidor, o acesso foi realizado diretamente pelo navegador, utilizando o IP público da instância EC2, <http://34.227.47.125/>. A página HTML personalizada foi exibida corretamente, confirmando o pleno funcionamento do serviço Apache.

### 2.2.1.6 Configuração de Rede e Segurança

A conectividade entre a instância e os usuários externos dependeu das configurações de rede na AWS descritas na Tabela 4.

**Tabela 4 – Grupo de segurança do servidor Web**

Serviço	Porta	Descrição	Origem Permitida
SSH	22	Acesso remoto	0.0.0.0/0
HTTP	80	Acesso web	0.0.0.0/0
ICMP	-	Ping/Teste	0.0.0.0/0

Fonte: Elaborada pelos autores.

Em ambiente de produção, recomenda-se restringir o acesso HTTP a endereços específicos e utilizar HTTPS (porta 443) com certificado SSL.

### 2.2.2 Serviço DNS

O DNS (Domain Name System) é o sistema responsável por traduzir endereços de IP em nomes de domínio. Uma vez que os computadores interpretam apenas números, o DNS atua como uma espécie de "tradutor da internet", sendo um mecanismo muito importante, já que os domínios são mais fáceis de memorizar. Portanto, esse processo é essencial para o funcionamento da internet, pois permite que usuários acessem sites, servidores e serviços de forma simples, sem precisar memorizar sequências de números.

Ao aplicar o comando "nslookup google.com" conseguimos ter acesso aos IPs (Figura 36), apesar de ser legíveis por humanos — como google.com — os endereços numéricos compreendidos pelas máquinas, como 142.251.163.139, o interessante é que ao inserir um IP em um navegador é possível acessar um site da mesma forma que se escreve um domínio.

Figura 36 – Exemplo buscando ip do google.com

The screenshot shows a terminal window on an Ubuntu system. The command entered is 'nslookup google.com'. The output shows the server being 127.0.0.53 and the address being 127.0.0.53#53. It then displays a 'Non-authoritative answer' section, which is highlighted with a red box. This section lists multiple entries for 'google.com' with their respective addresses: 142.251.163.139, 142.251.163.138, 142.251.163.102, 142.251.163.113, 142.251.163.100, 142.251.163.101, 2607:f8b0:4004:c21::65, 2607:f8b0:4004:c21::66, 2607:f8b0:4004:c21::71, and 2607:f8b0:4004:c21::8b. The entire output is shown in a monospaced font.

Fonte: Elaborada pelos autores.

#### 2.2.2.1 Estrutura Hierárquica do DNS

É importante entender como funciona os domínios e como se estrutura sua forma hierárquica demonstrada na Tabela 5. A consulta DNS começa na "raiz", passa pelo "TLD", em seguida pelo "domínio de segundo nível", e por fim chega ao "servidor específico" onde o site está hospedado, de modo que essa hierarquia facilita a organização da internet, permitindo que o DNS direcione corretamente os usuários para os servidores correspondentes.

**Tabela 5 – Hierarquia do DNS**

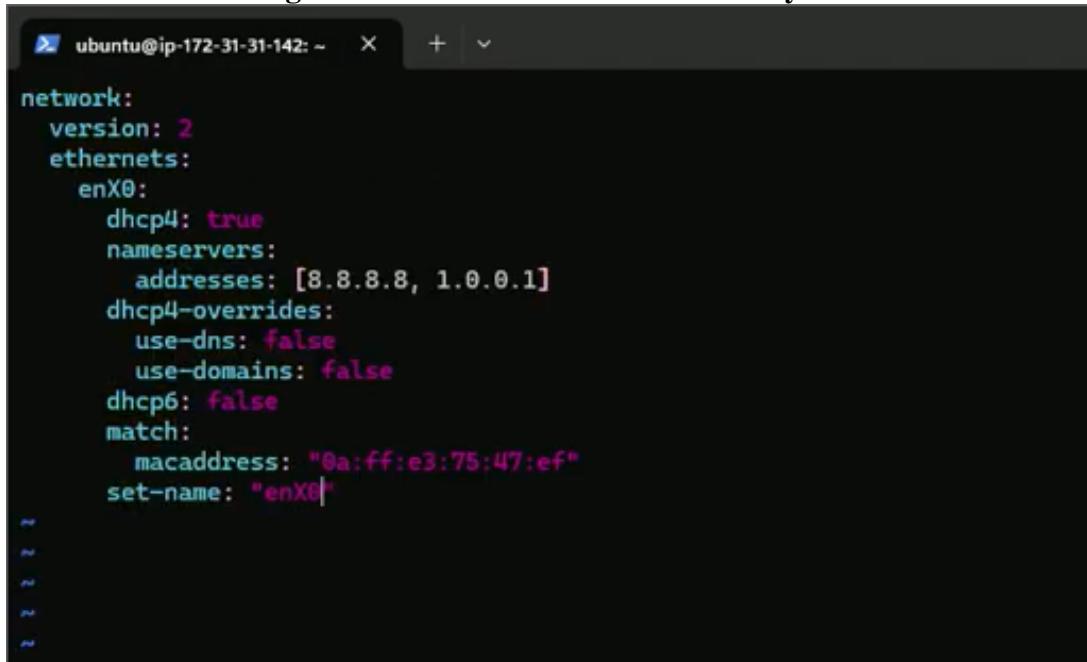
Nível	Exemplo	Descrição/Função
Raíz	.	É o topo da hierarquia. Representado por um ponto final (geralmente oculto). Redireciona consultas aos servidores dos domínios de topo (TLDs).
Domínio de Topo (TLD)	.com, .org, .br	Define a categoria ou país do domínio. Exemplo: .com para comercial, .br para Brasil.
Domínio de Segundo Nível (SLD)	credvaledoce.coop	Nome principal do site, escolhido pelo proprietário. Identifica a organização ou projeto.
Subdomínio	blog.cooperativa.com	Subdivisão do domínio principal. Pode representar diferentes serviços ou seções do mesmo site.
Host / Registro (A ou CNAME)	www.google.com para 142.251.1663.139	Define o nome exato do servidor (máquina) onde o site ou serviço está hospedado. Aponta para um endereço IP.

Fonte: Elaborada pelos autores.

#### 2.2.2.2 A Importância do Netplan na Configuração de Rede

É importante ressaltar que dentro da instância Ubuntu EC2 na AWS, a ferramenta Netplan que é responsável por configurar a rede e o DNS do sistema. Ela garante que a máquina possua conectividade com a internet e que possa responder corretamente às consultas DNS recebidas.

Para visualizar ou editar as configurações, utiliza-se o comando "sudo vim /etc/netplan/50-cloud-init.yaml"(Figura 37).

**Figura 37 – Conteúdo do 50-cloud-init.yaml**


```

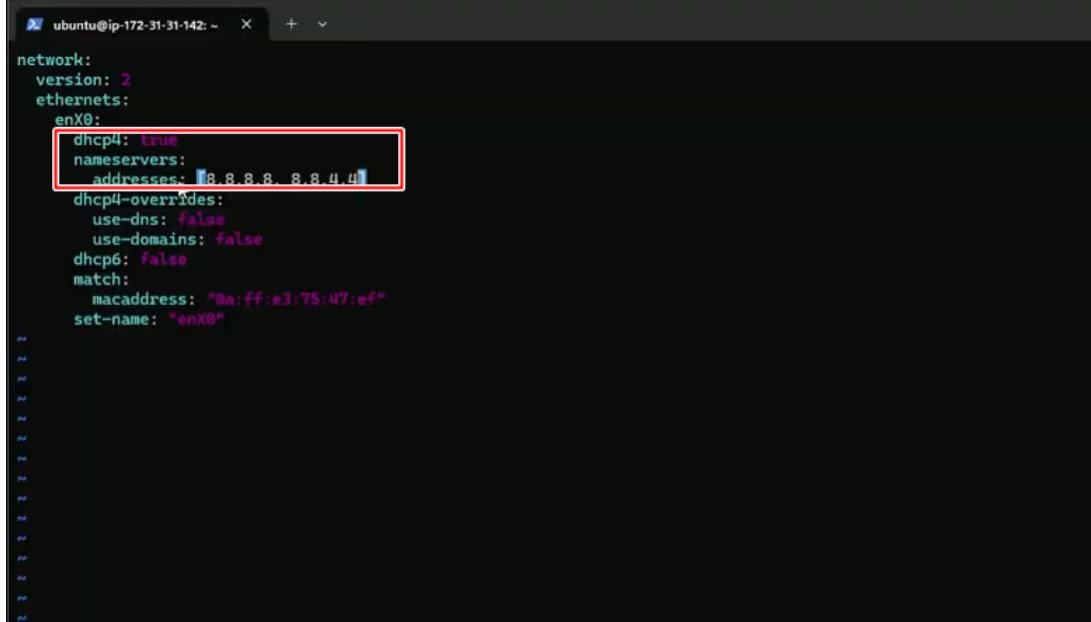
ubuntu@ip-172-31-31-142: ~
network:
  version: 2
  ethernets:
    enX0:
      dhcp4: true
      nameservers:
        addresses: [8.8.8.8, 1.0.0.1]
      dhcp4-overrides:
        use-dns: false
        use-domains: false
      dhcp6: false
      match:
        macaddress: "0a:ff:e3:75:47:ef"
      set-name: "enX0"

```

Fonte: Elaborada pelos autores.

Dentre as instâncias presentes, vale destacar o "dhcp4- Ao deixar somente em "True" a máquina recebe automaticamente todas as configurações de rede incluindo os DNS via DHCP da AWS. Dessa forma, para definir um DNS fixo, poderíamos alterar como na Figura 38.

**Figura 38 – Fixando o DNS**

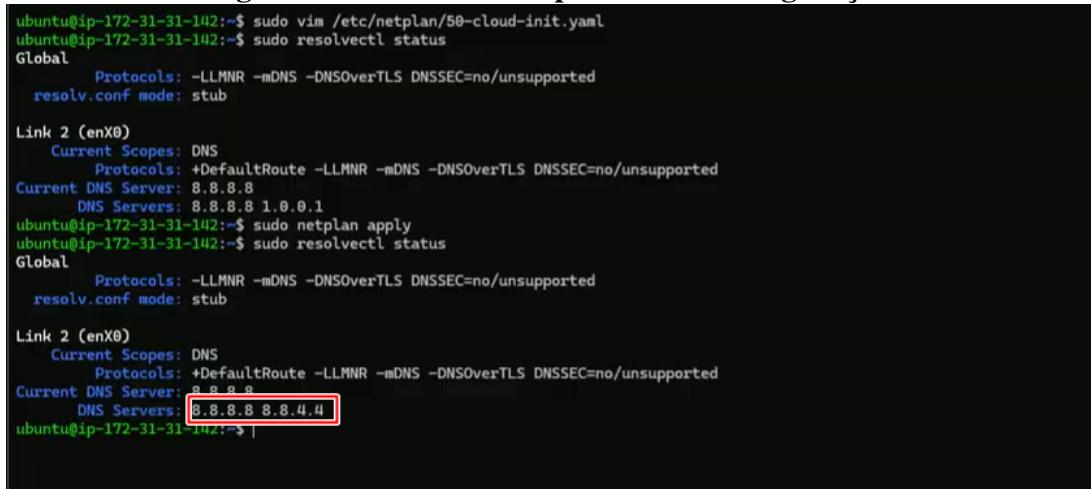


```
ubuntu@ip-172-31-31-142: ~ % 
network:
  version: 2
  ethernets:
    enX0:
      dhcp4: true
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
      dhcp4-overrides:
        use-dns: false
        use-domains: false
      dhcp6: false
      match:
        macaddress: "0a:ff:e3:75:47:ef"
      set-name: "enX0"
~
```

Fonte: Elaborada pelos autores.

Podemos observar na Figura 39 que as mudanças só são aplicadas mediante o comando "sudo netplan apply".

**Figura 39 – Checando e aplicando as configurações**



```
ubuntu@ip-172-31-31-142: ~ $ sudo vim /etc/netplan/50-cloud-init.yaml
ubuntu@ip-172-31-31-142: ~ $ sudo resolvelctl status
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (enX0)
  Current Scopes: DNS
    Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  Current DNS Server: 8.8.8.8
    DNS Servers: 8.8.8.8 1.0.0.1
ubuntu@ip-172-31-31-142: ~ $ sudo netplan apply
ubuntu@ip-172-31-31-142: ~ $ sudo resolvelctl status
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (enX0)
  Current Scopes: DNS
    Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  Current DNS Server: 8.8.8.8
    DNS Servers: 8.8.8.8 8.8.4.4
ubuntu@ip-172-31-31-142: ~ |
```

Fonte: Elaborada pelos autores.

Dessa forma, o Netplan garante que a instância tenha uma rede funcional e possa responder às consultas DNS. de modo que sem ele — ou com uma configuração incorreta — a instância não teria conectividade, e o site não seria acessível, o site não sendo acessível o cliente não tem acesso, mesmo que o DNS esteja configurado corretamente.

Na AWS, as instâncias EC2 recebem automaticamente um DNS interno via DHCP da VPC, o Netplan, por sua vez, gerencia essa rede, aplicando corretamente as configurações de IP e DNS.

### 2.2.3 *Servidor FTP*

O File Transfer Protocol (FTP) é um protocolo padrão para transferência de arquivos entre sistemas, que garante a entrega dos arquivos e permite controle de acesso.

O serviço foi configurado com um servidor utilizando o vsftpd (Very Secure FTP Daemon), e dois clientes, um Ubuntu e um Windows utilizando o FileZilla. Dessa forma foi possível demonstrar a transferência de arquivos entre diferentes sistemas operacionais.

#### 2.2.3.1 *Topologia da Arquitetura*

As instâncias UbuntuSRV01T e UbuntuCliente foram configuradas na AWS EC2, ambas do tipo t2.micro e executando o Ubuntu Server 24.04. Já a máquina local corresponde a um computador pessoal com Windows 11, como descrito na Tabela 6.

**Tabela 6 – Máquinas utilizadas para o FTP**

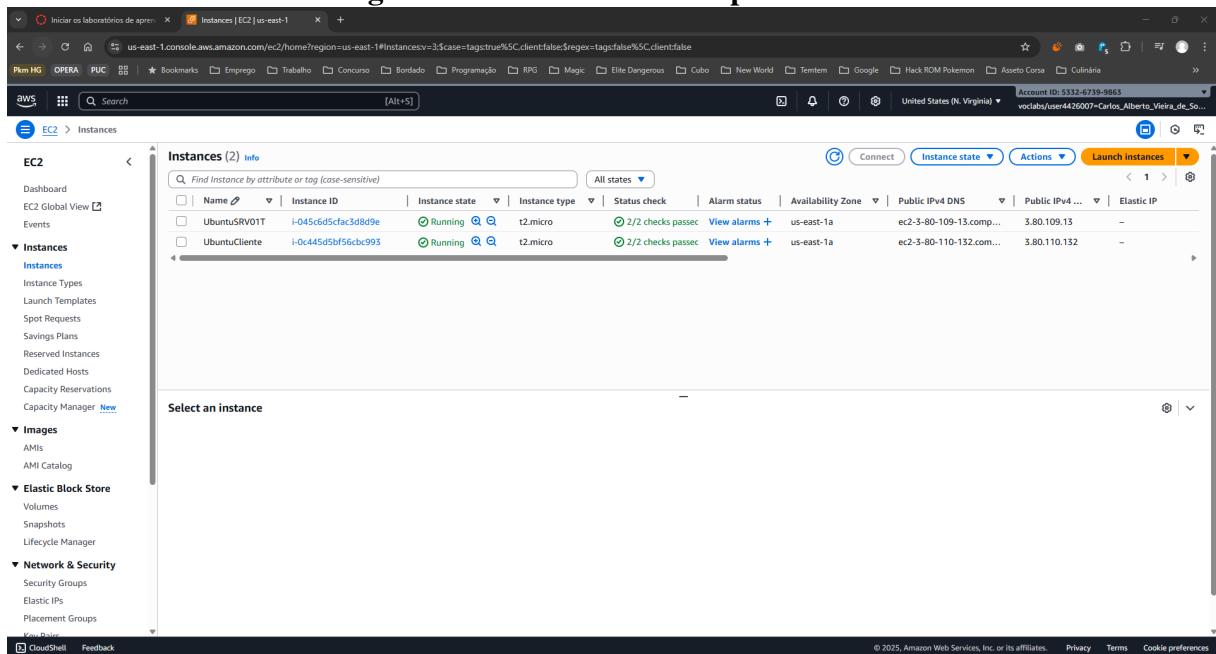
Função	Nome da Máquina	IPV4	Ferramenta
Servidor FTP	UbuntuSRV01T	176.31.29.21	vsftpd
Cliente Ubuntu	UbuntuCliente	176.31.29.222	ftp
Cliente Windows	Máquina local	externo	FileZilla

**Fonte:** Elaborada pelos autores.

#### 2.2.3.2 *Máquinas Utilizadas*

Foram criadas duas máquinas virtuais, utilizando o serviço EC2 na AWS (Amazon WEB Services), para a configuração e testes do serviço FTP. Sendo elas, uma instância server (UbuntuSRV01T) responsável por hospedar o serviço FTP via vsftpd. E uma instância cliente (UbuntuCliente) utilizada para testes de conexão e comandos via terminal (Figura 40).

Além disso foi utilizada um computador pessoal com Windows 11, empregada para validar o acesso via interface gráfica utilizando o cliente FileZilla.

**Figura 40 – Instâncias feitas para o FTP**

**Fonte:** Elaborada pelos autores.

### 2.2.3.3 Configuração do Servidor FTP (UbuntuSRV01T)

Inicialmente a máquina foi atualizada com os comandos "sudo apt update", "sudo apt upgrade" e depois "sudo apt update" novamente. Após a atualização foi instalado o vsftpd com "sudo apt install vsftpd -y" e habilitado para iniciar sempre que a máquina reiniciar com "sudo systemctl enable vsftpd".

Foi realizada a liberação da porta para o SSH (22) para não se perder a conexão com a máquina com "sudo ufw allow ssh", a ativação do firewall com "sudo ufw enable", e por fim a liberação das portas para o ftp, 20, 21, 990, e o intervalo de 30000 a 31000 para o uso do modo passivo com "sudo ufw allow 20,21,990/tcp" e "sudo ufw allow 30000:31000/tcp" (Figura 41).

Por se tratar de uma instância hospedada na AWS, foi necessário liberar as portas no grupo de segurança da instância (Figura 42). O acesso foi permitido a todos (0.0.0.0/0) apenas por se tratar de um ambiente de teste e prova de conceito (POC).

**Figura 41 – Configurações de firewall**

```
ubuntu@ip-172-31-29-21:~$ sudo ufw status
Status: active

To                         Action      From
--                         --         --
22/tcp                      ALLOW       Anywhere
20,21,990/tcp                ALLOW       Anywhere
30000:31000/tcp              ALLOW       Anywhere
22/tcp (v6)                  ALLOW       Anywhere (v6)
20,21,990/tcp (v6)           ALLOW       Anywhere (v6)
30000:31000/tcp (v6)         ALLOW       Anywhere (v6)
```

**Fonte:** Elaborada pelos autores.

**Figura 42 – Configurações do grupo de segurança**

Inbound rules (4)							
	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-096e622d3d9c1c8f5	IPv4	Custom TCP	TCP	30000 - 31000	0.0.0.0/0
<input type="checkbox"/>	-	sgr-019bd47dc009b7f37	IPv4	Custom TCP	TCP	20 - 21	0.0.0.0/0
<input type="checkbox"/>	-	sgr-0a904fd7b4030754	IPv4	SSH	TCP	22	0.0.0.0/0
<input type="checkbox"/>	-	sgr-02abbc56a7e37a53e	IPv4	Custom TCP	TCP	990	0.0.0.0/0

**Fonte:** Elaborada pelos autores.

Foi criado o usuário e a senha (Tabela 7) para a utilização do serviço pela parte cliente com os comandos "sudo useradd srvWeb" e "sudo passwd srvWeb".

**Tabela 7 – Usuários e senhas dos clientes FTP**

Usuário	Senha
srvWeb	234

**Fonte:** Elaborada pelos autores.

Foi realizada então a criação do diretório necessário "sudo mkdir /etc/vsftpd". Utilizou-se o editor VIM para criar e editar o arquivo com os nomes dos usuários autorizados com o comando "sudo vim /etc/vsftpd/user\_list". Ao editar o arquivo é necessário escrever o nome de cada usuário no arquivo, um por linha.

Seguiu-se com a criação e permissionamento das pastas de cada usuário com os comandos "sudo mkdir -p /home/srvWeb/dados", "sudo chown srvWeb:srvWeb /home/srvWeb/-dados" e "sudo chown srvWeb:srvWeb /home/srvWeb".

Ao editar o arquivo de configuração do vsftpd foi retirada a marcação de comentário da linha "write\_enable=YES" que habilita a escrita e upload de arquivos pelos usuários. E foi adicionado ao final do arquivo as linhas explicadas na Tabela 8.

**Tabela 8 – Configuração do vsftpd**

<b>Código</b>	<b>Explicação</b>
userlist_deny=NO userlist_file=/etc/vsftpd/user_list	Somente usuários listados podem acessar. Indica local onde está o arquivo com a lista de usuários permitidos.
tcp_wrappers=NO local_root=/home/srvWeb/dados	Possibilita a listagem de arquivos. Entrega a pasta que deve ser carregada ao logar com o usuário, deve ser indicada para cada usuário criado.
chroot_local_user=YES	Ter uma pasta home para cada usuário logado.
allow_writeable_chroot=YES	Permite ao usuário escrever nesse local.
pasv_enable=YES	Habilita o modo passivo.
pasv_min_port=30000	Indica o inicio do intervalo de portas destinadas para o modo passivo.
pasv_max_port=31000	Indica o fim do intervalo de portas destinadas para o modo passivo.
pasv_address=18.212.252.103	Aponta o ip da máquina do servidor.

**Fonte:** Elaborada pelos autores.

O ip colocado no "pasv\_address" foi o público para que fosse encontrado por máquinas fora da rede que o servidor se encontra. Por padrão no EC2 esse ip sempre é alterado ao reiniciar a instância. Logo, nesse ambiente de teste devemos nos atentar de alterar esse valor sempre que ele mudar para que tudo funcione normalmente.

Por fim o serviço necessita ser reiniciado com "sudo systemctl restart vsftpd"

#### 2.2.3.4 Configuração e testes do Cliente (UbuntuCliente e Máquina local)

No cliente ubuntu foi realizada apenas a atualização da máquina com "sudo apt update", "sudo apt upgrade" e "sudo apt update". E então foi feita a conexão com o servidor com "ftp 18.212.252.103". Com a conexão concluída é solicitada o login e senha do usuário, após a validação foi testado a listagem com "ls" e criação de diretório com "mkdir Teste" (Figura 43).

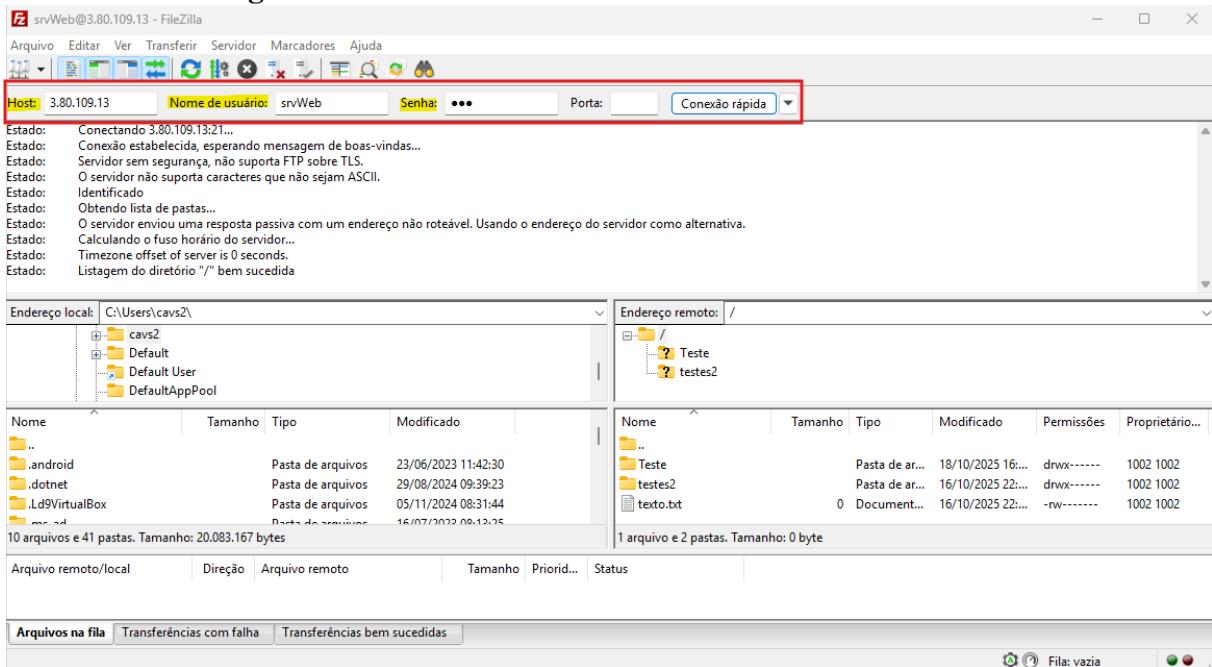
**Figura 43 – Resultado dos testes FTP no cliente ubuntu**

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30246|)
150 Here comes the directory listing.
drwx----- 2 1002 1002 4096 Oct 17 01:09 testes2
-rw----- 1 1002 1002 0 Oct 17 01:10 texto.txt
226 Directory send OK.
ftp> mkdir Teste
257 "/Teste" created
ftp>
```

**Fonte:** Elaborada pelos autores.

Após a instalação do software Filezilla é necessário indicar, nos campos destacados na Figura 44, o ip do servidor, login e senha do usuário. Com, a conexão estabelecida as pastas e arquivos do diretório serão listados e poderão ser manipulados.

**Figura 44 – Resultado dos testes FTP no cliente Windows**



**Fonte: Elaborada pelos autores.**

## 2.2.4 Serviço NFS (Network File System)

O Network File System (NFS) é um protocolo que permite o compartilhamento de arquivos em rede de forma transparente, possibilitando que diretórios e arquivos localizados em um servidor sejam acessados por clientes como se estivessem em seus próprios sistemas locais.

No contexto da Cooperativa, foi configurada uma arquitetura em que a Matriz atua como servidor NFS (NFS Server) e as Filiais atuam como clientes NFS (NFS Clients).

Dessa forma, todos os arquivos gerados ou modificados nas filiais são armazenados centralmente na matriz, garantindo padronização, sincronização e transparência de acesso.

Além disso, o uso do NFS reduz a duplicação de dados, centraliza o armazenamento e facilita o controle de versões e backups corporativos.

Para a configuração, foi estabelecida a conexão via SSH com a instância EC2 “NSF-Server” (Ubuntu Server 22.04 LTS, tipo t3.micro) hospedada na AWS.

### 2.2.4.1 Topologia da Arquitetura do Serviço NFS

Nessa configuração foi adotado o Tipo: Centralizado, com a Rede VPC: 172.31.0.0/16, com acesso permitido: 0.0.0.0/0 (devendo ser considerado apenas para Proof of Concept).

(POC)/testes). A distribuição dos IPS após o instanciamento na EC2, estão identificadas a seguir, na Tabela 9:

**Tabela 9 – Identificação das Instâncias do Serviço de NFS**

Função	Nome da Instância	IPv4 Privado	Papel
Matriz	NFS-Server	172.31.31.204	Servidor NFS
Filial 1	NFS-Filial-1	172.31.23.111	Cliente NFS
Filial 2	NFS-Filial-2	172.31.28.50	Cliente NFS
Filial 3	NFS-Filial-3	172.31.22.140	Cliente NFS
Filial 4	NFS-Filial-4	172.31.19.147	Cliente NFS
Filial 5	NFS-Filial-5	172.31.25.100	Cliente NFS

Fonte: Elaborada pelos autores

As máquinas virtuais criadas, denominadas como instâncias do tipo EC2 utilizando o serviço de computação em nuvem da AWS (Amazon Web Services), podem ser identificadas na Figura 45:

**Figura 45 – Instâncias criadas no EC2 da AWS**

Name	Instance ID	State	Type	Status checks	Alarm status	Availability Zone	Region
SRV_Ubuntu01	I-05a81bd8cf5f530f5	Running	t2.micro	2/2 checks passed	+ View alarms	us-east-1c	ec
NFS-SVR-Matriz	I-080ee7fa54dc9b122	Running	t3.micro	3/3 checks passed	+ View alarms	us-east-1c	ec
NFS-Filial-2	I-03fffb8a31f8de9892	Running	t3.micro	3/3 checks passed	+ View alarms	us-east-1c	ec
NFS-Filial-3	I-0026d32e82244c229	Running	t3.micro	3/3 checks passed	+ View alarms	us-east-1c	ec
NFS-Filial-1	I-016d768d68cc48ec9	Running	t3.micro	3/3 checks passed	+ View alarms	us-east-1c	ec
NFS-Filial-5	I-0b06342f9bd15f253	Running	t3.micro	3/3 checks passed	+ View alarms	us-east-1c	ec
NFS-Filial-4	I-08648e4cf698a5d75	Running	t3.micro	3/3 checks passed	+ View alarms	us-east-1c	ec

Fonte: Elaborada pelos autores

#### 2.2.4.2 Configuração do Serviço NFS no Servidor (Matriz)

Uma vez instanciada a NFS-Matriz, foi realizada a sua configuração via terminal, fazendo sua conexão com SSH. Feita a conexão, a instalação seguiu com os seguintes comandos:

Configuração do Kernel:

- sudo apt update
- sudo apt install nfs-kernel-server -y

Em seguida, foi criado o diretório que será compartilhado com as filiais:

- sudo mkdir -p /mnt/nfs\_share
- sudo chown nobody:nogroup /mnt/nfs\_share

- sudo chmod 777 /mnt/nfs\_share

Com o diretório criado, ele foi então configurado para permitir acesso aos clientes da rede interna (VPC 172.31.0.0/16). Para isso, o arquivo de configuração /etc(exports) foi editado e acrescida a seguinte linha:

- sudo nano /etc(exports)

Dentro do exports foi acrescida uma linha:

- /mnt/nfs\_share 172.31.0.0/16(rw,sync,no\_subtree\_check)

Essa configuração permite que toda a faixa de IPs 172.31.0.0 possam acessar os arquivos, podendo ler e escrever (rw). O sync estabele que os arquivos são escritos ou alterados serão gravados imediatamente no disco. O (no-subtree-check), evita checagens desnecessárias de subdiretórios, melhorando o desempenho.

Após a configuração, as alterações foram aplicadas e o serviço exportado com os comandos:

- sudo exportfs -ra
- sudo exportfs -v

Para fins de prova de conceito (POC), foram liberadas no Security Group da AWS as portas necessárias para funcionamento do NFS, conforme Tabela 10.

**Tabela 10 – Portas configuradas no Security Group da AWS**

Protocolo	Porta	Serviço
TCP/UDP	2049	NFS
TCP/UDP	111	RPCBind
TCP	22	SSH
ICMP	-	Echo Request/Reply

**Fonte: Elaborada pelos autores**

Em ambiente de produção, recomenda-se restringir o acesso à faixa interna da VPC e aplicar autenticação por host, garantindo maior segurança à comunicação entre matriz e filiais.

#### *2.2.4.3 Configuração do Serviço NFS no Cliente (Filial 1)*

Por limitação de tempo e escopo do projeto, a configuração foi demonstrada apenas na Filial 1. As demais filiais podem replicar a configuração.

Já com a instância NFS-Filial-1 criada EC2, foi feita a conexão em um novo terminal e sua configuração se deu da seguinte forma:

Instalação do cliente NFS

- sudo apt update
- sudo apt install nfs-common -y

Posteriormente, foi criado o diretório local onde o compartilhamento remoto será montado:

- sudo mkdir /mnt/nfs\_client

O diretório compartilhado pela matriz foi montado utilizando o comando:

- sudo mount -t nfs 172.31.31.204:/mnt/nfs\_share /mnt/nfs\_client

Para verificar se o compartilhamento foi montado corretamente, utilizou-se:

- df -h | grep nfs

O retorno confirmou a montagem e o acesso ao diretório remoto, validando o funcionamento do serviço.

- 172.31.31.204:/mnt/nfs\_share 6.8G 2.0G 4.8G 30 /mnt/nfs\_client

#### 2.2.4.4 Testes de Compartilhamento de Arquivos - NFS

Para validar o funcionamento do sistema de arquivos distribuído, foi criado um arquivo no servidor da matriz, usando o seguinte comando visualizado na Figura 46:

**Figura 46 – Teste de Escrita de um arquivo .txt na Matriz**

```
odair — ubuntu@ip-172-31-31-204: ~ -- ssh -i odair_si_1.pem ubuntu@ec2-54-242-132-148.compute-1.amazonaws....  
[ubuntu@ip-172-31-31-204:~]$ echo -e "Manual Quatro de uso do NFS da Cred Vale Doce\n\nDefinições\nInstruções de uso\nBenefícios" | sudo tee /mnt/nfs_share/manual14_nfs.txt  
Manual Quatro de uso do NFS da Cred Vale Doce  
  
Definições  
Instruções de uso  
Benefícios  
ubuntu@ip-172-31-31-204:~$
```

**Fonte: Elaborada pelos autores**

Em seguida, o mesmo arquivo foi acessado a partir da filial, conforme Figura 47:

**Figura 47 – Teste de Leitura na Filial 1 do arquivo criado na Matriz**

```
odair — ubuntu@ip-172-31-23-111: ~ -- ssh -i odair_si_1.pem ubuntu@ec2-54-210-74-118.compute-1.amazonaws.co...
[ubuntu@ip-172-31-23-111:~]$ cat /mnt/nfs_client/manual4_nfs.txt
Manual Quatro de uso do NFS da Cred Vale Doce

Definições
Instruções de uso
Benefícios
ubuntu@ip-172-31-23-111:~$
```

**Fonte:** Elaborada pelos autores

O conteúdo retornado foi idêntico ao arquivo original, demonstrando a transparência e sincronização imediata do NFS.

De modo complementar, foi realizado o teste inverso — criação de um arquivo a partir da filial e leitura na matriz:

Criação do arquivo .txt na Filial 1, conforme a Figura 48:

**Figura 48 – Teste de Escrita do arquivo na Filial 1**

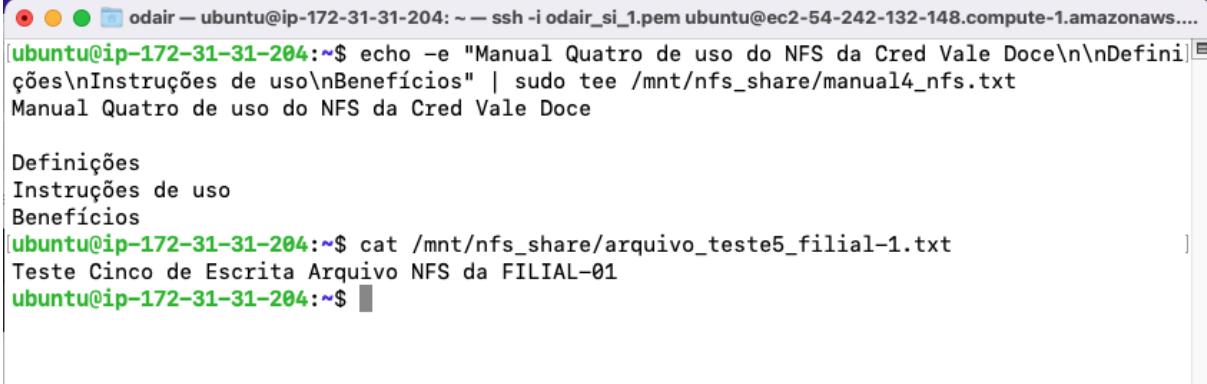
```
odair — ubuntu@ip-172-31-23-111: ~ -- ssh -i odair_si_1.pem ubuntu@ec2-54-210-74-118.compute-1.amazonaws.co...
[ubuntu@ip-172-31-23-111:~]$ cat /mnt/nfs_client/manual4_nfs.txt
Manual Quatro de uso do NFS da Cred Vale Doce

Definições
Instruções de uso
Benefícios
[ubuntu@ip-172-31-23-111:~]$ echo "Teste Cinco de Escrita Arquivo NFS da FILIAL-01" | sudo tee /mnt/nfs_client/ arquivo teste5_filial-1.txt
Teste Cinco de Escrita Arquivo NFS da FILIAL-01
ubuntu@ip-172-31-23-111:~$
```

**Fonte:** Elaborada pelos autores

Leitura pela Matriz do arquivo criado na Filial 1, conforme a Figura 49:

**Figura 49 – Teste de Leitura pela Matriz do arquivo escrito na Filial 1**



```
odair — ubuntu@ip-172-31-31-204: ~ — ssh -i odair_si_1.pem ubuntu@ec2-54-242-132-148.compute-1.amazonaws....  
[ubuntu@ip-172-31-31-204:~]$ echo -e "Manual Quatro de uso do NFS da Cred Vale Doce\n\nDefinições\nInstruções de uso\nBenefícios" | sudo tee /mnt/nfs_share/manual4_nfs.txt  
Manual Quatro de uso do NFS da Cred Vale Doce  
  
Definições  
Instruções de uso  
Benefícios  
[ubuntu@ip-172-31-31-204:~]$ cat /mnt/nfs_share/ arquivo teste5_filial-1.txt  
Teste Cinco de Escrita Arquivo NFS da FILIAL-01  
[ubuntu@ip-172-31-31-204:~$ ]
```

**Fonte:** Elaborada pelos autores

A presença do arquivo no diretório do servidor confirmou o compartilhamento bidirecional e a integridade da comunicação entre as instâncias.

#### *2.2.4.5 Considerações sobre o NFS na Cred Vale Doce*

A implementação do Network File System (NFS) na arquitetura proposta proporciona centralização dos dados corporativos, redução de redundâncias e facilidade de manutenção de backups.

Além disso, o serviço garante:

- Transparência de acesso: os usuários das filiais acessam diretórios remotos como se fossem locais;
- Consistência de dados: todas as unidades visualizam o mesmo conjunto de arquivos atualizados;
- Escalabilidade: novas filiais podem ser integradas facilmente ao sistema;
- Padronização operacional: assegura uniformidade nos processos de armazenamento e compartilhamento de documentos.

Dessa forma, o NFS contribui diretamente para a eficiência operacional e tecnológica da Cred Vale Doce, alinhando-se à proposta de integração total entre matriz e filiais por meio de uma infraestrutura de rede segura, centralizada e de fácil gerenciamento.

#### *2.2.5 Serviço de Banco de Dados (PostgreSQL)*

O PostgreSQL, comumente abreviado como "Postgres", é um sistema de gerenciamento de banco de dados relacional a objetos (ORDBMS) de código aberto, conhecido por sua confiabilidade, flexibilidade e suporte a padrões técnicos abertos.

Entre suas principais características estão o suporte a tipos de dados relacionais e não relacionais, como JSON, além de recursos avançados como chaves estrangeiras, triggers, views, procedimentos armazenados, funções agregadas e suporte a múltiplas linguagens de programação, incluindo Python, Java, C e Ruby.

#### *2.2.5.1 Topologia da Arquitetura*

Ambiente configurado em uma instância AWS EC2 do tipo t3.small, executando Ubuntu Server 24.04 LTS, com arquitetura centralizada, descrito na Tabela 11. Utiliza a rede VPC 172.31.0.0/16 e possui acesso liberado para 0.0.0.0/0, permitindo conexões externas durante a fase de testes (POC).

**Tabela 11 – Máquina utilizada para o banco de dados**

Função	Nome da Máquina	IPV4 Privado	IPV4 Público	Papel
Servidor	Ubuntu_Server	172.31.27.40	3.87.77.159	PostgresSQL

**Fonte:** Elaborada pelos autores.

#### *2.2.5.2 Máquina Virtual na Nuvem*

Foi criada uma máquina virtual na nuvem (instância EC2) para atuar como Servidor PostgresSQL da Matriz da Cooperativa de Crédito. Essa máquina representa o servidor web central da Cooperativa, responsável por disponibilizar informações corporativas e documentos para as filiais de forma online.

A instância foi provisionada na AWS (Amazon Web Services) utilizando o Ubuntu Server 24.04 LTS (Figura 50) como sistema operacional, dentro da mesma VPC (Virtual Private Cloud) que conecta as demais filiais.

**Figura 50 – Instância utilizada para o banco de dados**

**Fonte:** Elaborada pelos autores

Por se tratar de um banco de dados SQL, onde as informações mais sensíveis se residem, o foco é sempre ideal realizar uma configuração que limite o acesso a maquina virtual com o banco de dados. Porém, para fins de prova de conceito (POC), a instância foi configurada com acesso SSH (porta 22) e HTTP (porta 5432) liberados no grupo de segurança como visto na Figura 51.

**Figura 51 – Grupo de segurança da instância do banco de dados**

▼ Regras de entrada

Regras de filtro				
Nome	ID da regra do grupo de ...	Intervalo de p...	Protocolo	Origem
-	sgr-0b71dfab1301aeb0c	22	TCP	0.0.0.0/0
-	sgr-094d2edb8f673520d	5432	TCP	0.0.0.0/0

▼ Regras de saída

Regras de filtro				
Nome	ID da regra do grupo de ...	Intervalo de p...	Protocolo	Destino
-	sgr-0d06fb4d207517e3d	5432	TCP	0.0.0.0/0
-	sgr-0eddcc67e5f17ce69	Todos	Todos	0.0.0.0/0

**Fonte:** Elaborada pelos autores

### 2.2.5.3 Instalação e Configuração do PostgreSQL

Atualize a lista de pacotes do sistema com o comando "sudo apt update && sudo apt upgrade -y". Instale o PostgreSQL e os componentes adicionais com "sudo apt install postgresql postgresql-contrib".

Após a instalação, verifique o status do serviço para garantir que o serviço está ativo e em execução com "sudo systemctl status postgresql". Para iniciar o serviço e habilitá-lo para iniciar automaticamente ao ligar o sistema, utilize o comando "sudo systemctl start postgresql && sudo systemctl enable postgresql".

Acesse o prompt do PostgreSQL como o usuário administrador com "sudo -i -u postgres psql". Para criar um novo usuário (role), use comando SQL "CREATE ROLE novo\_usuario WITH LOGIN PASSWORD 'sua\_senha'". Caso queira trocar a senha do usuário postgres ou de qualquer outro usuário basta executar o comando "ALTER USER nome\_usuario WITH PASSWORD nova\_senha;".

Para criar um banco de dados, é preciso executar o seguinte comando "CREATE DATABASE meu\_banco OWNER nome\_usuario".

#### *2.2.5.4 Configuração do Diretório e comunicação para o Banco de Dados*

Para realizar a configuração para acesso remoto, primeiramente é preciso acessar o arquivo de configuração do postgresql que se localiza na pasta /etc/postgresql/18/main.

Para editar o arquivo postgresql.conf, é preciso utilizar o seguinte comando "sudo nano /etc/postgresql/14/main/postgresql.conf". Altere a linha "listen\_addresses = 'localhost'" para "listen\_addresses = '\*'".

O segundo arquivo a ser editado é nomeado de pg\_hba.conf e para acessá-lo, é preciso executar o seguinte comando "sudo nano /etc/postgresql/14/main/pg\_hba.conf". Após acessar o arquivo, insira a seguinte linha no final dele "host all all 0.0.0.0/0 md5".

Com todas essas alterações implementadas, reinicie o PostgreSQL "sudo systemctl restart postgresql".

#### *2.2.5.5 Teste de Funcionamento e Acesso Web*

Para validar o funcionamento do servidor, o acesso foi realizado de duas formas, utilizando um terminal (Figura 53) de uma máquina que simulava a de administração de alguma filial da empresa e pela interface gráfica, com o PgAdmin4 (Figura 52).

**Figura 52 – PgAdmin4**

The screenshot shows the PgAdmin4 interface. On the left is the Object Explorer pane, which lists servers, databases, tables, and other database objects. In the center is the Query Editor pane, displaying a SQL query and its results. The query is:

```

1. SELECT * FROM public.funcionarios
2. ORDER BY id DESC LIMIT 100
3.

```

The results table has four columns: id, nome, cargo, and filial\_id. The data is:

id	nome	cargo	filial_id
1	Mariana Almeida	Gerente de Agência	3
2	Patrícia Costa	Caixa	2
3	Lucas Mendes	Gerente de Agência	2
4	Fernanda Lima	Analista de Crédito	1
5	Roberto Andrade	Gerente Geral	1

**Fonte: Elaborada pelos autores**

**Figura 53 – Terminal**

```

ubuntu@ip-172-31-27-40:~$ sudo -u postgres psql
psql (16.10 (Ubuntu 16.10-0ubuntu0.24.04.1))
Type "help" for help.

postgres=# \c credvaledoce
You are now connected to database "credvaledoce" as user "postgres".
credvaledoce=# SELECT * FROM public.funcionarios
ORDER BY id DESC LIMIT 100;
   id  |    nome     |         cargo          | filial_id
-----+-----+-----+-----+
      5 | Mariana Almeida | Gerente de Agência | 3
      4 | Patrícia Costa | Caixa | 2
      3 | Lucas Mendes | Gerente de Agência | 2
      2 | Fernanda Lima | Analista de Crédito | 1
      1 | Roberto Andrade | Gerente Geral | 1
(5 rows)

credvaledoce=#

```

**Fonte: Elaborada pelos autores**

Os dados dos usuários criados estão listados na Tabela 12.

**Tabela 12 – Dados de usuários do banco de dados**

Nome de Usuário	Senha	Descrição	Banco de Dados de Acesso
postgres	CredVerde_31	Usuário padrão/root do Postgressql	Todos
admin	ModoPet.05	Usuário Administrador do Postgressql	credvaledoce
teste	teste1234	Usuário criado somente para testes de conexões, não possuindo nenhum acesso aos banco de dados	Nenhum

**Fonte:** Elaborada pelos autores.

#### 2.2.5.6 Configuração de Rede e Segurança

A conectividade entre a instância e os usuários externos dependeu das configurações de rede na AWS visto na Tabela 13.

**Tabela 13 – Máquina utilizada para o banco de dados**

Serviço	Porta	Descrição	Origem Permitida
SSH	22	Acesso remoto	0.0.0.0/0
HTTP	5432	Acesso PostgreSQL	0.0.0.0/0

**Fonte:** Elaborada pelos autores.

Em ambiente de produção, recomenda-se restringir o acesso do Banco de dados a endereços específicos e utilizar sempre a criptografia de senhas e dados sensíveis.

## 3 GERÊNCIA E MONITORAMENTO DE AMBIENTES DE REDE

### 3.1 Monitoramento em Máquinas Virtuais Locais

As máquinas virtuais locais foram utilizadas para criar um ambiente controlado, ideal para testes e simulações de rede. Nelas, o Zabbix teve um papel essencial, sendo responsável por monitorar o desempenho e o consumo de recursos de cada máquina. Por meio dessa ferramenta, foi possível observar o funcionamento dos serviços em tempo real, detectar possíveis falhas e manter a estabilidade do sistema. O uso do Zabbix é importante porque garante maior eficiência, confiabilidade e controle sobre os ambientes virtuais, tornando o processo de gerenciamento e análise muito mais preciso.

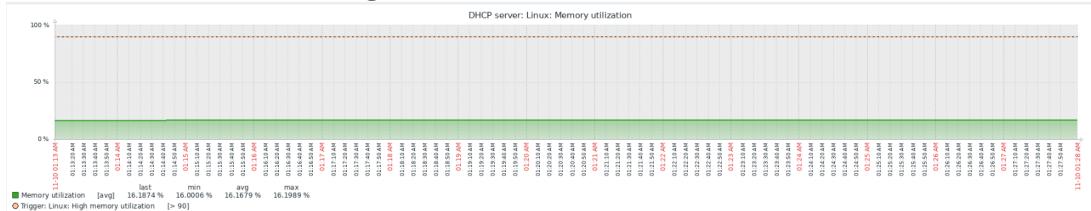
### 3.1.1 Servidor DHCP ( Dynamic Host Configuration Protocol )

O Zabbix foi utilizado para monitorar o funcionamento do DHCP (Dynamic Host Configuration Protocol), um protocolo que automatiza a atribuição de endereços IP e outras configurações de rede aos dispositivos conectados. Essa automação evita conflitos de endereçamento e facilita o gerenciamento da infraestrutura. No projeto, o Zabbix Agent foi implementado junto a uma máquina Linux Ubuntu Server configurada como servidor DHCP, possibilitando acompanhar em tempo real o desempenho do serviço e garantir uma distribuição eficiente e estável dos endereços na rede.

#### 3.1.1.1 Monitoramento da Infraestrutura

No monitoramento de memória RAM (Figura 54) é possível perceber que ele é baixo e estável, sem variações significativas, sem risco de esgotamento da memória e está suficiente para sua carga atual.

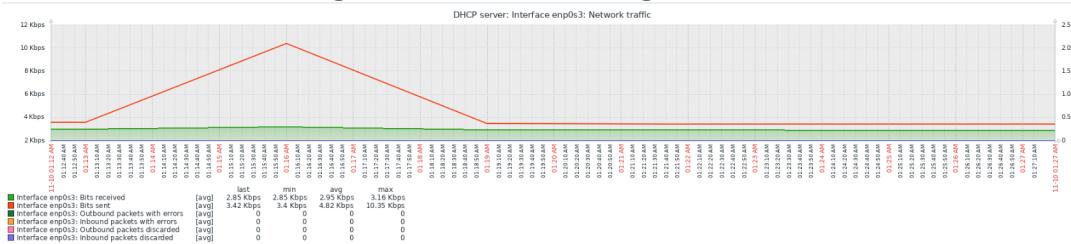
**Figura 54 – DHCP Uso de RAM**



**Fonte:** Elaborada pelos autores

A Figura 56 mostra o gráfico de interface de rede e indica que está funcionando normalmente, com baixa utilização e sem erros, o pico no inicio do gráfico provavelmente foi causado pela inicialização do servidor.

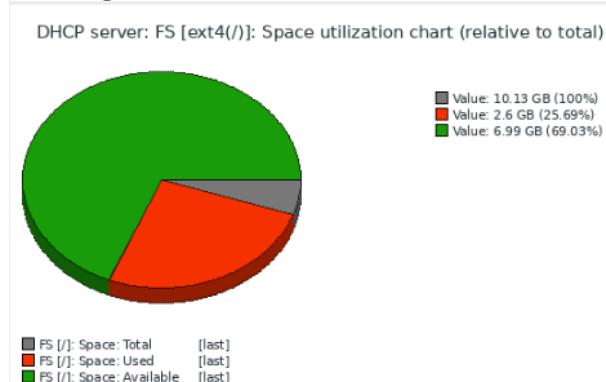
**Figura 56 – DHCP Tráfego de Rede]**



Fonte: Elaborada pelos autores

No gráfico de armazenamento da Figura 57 podemos observar que o servidor DHCP ainda tem bastante espaço disponível, cerca de 70% do espaço total, e o uso atual é 25%, mostrando que seu esgotamento não é algo iminente e não há necessidade de limpeza ou expansão.

**Figura 57 – DHCP Armazenamento**



Fonte: Elaborada pelos autores

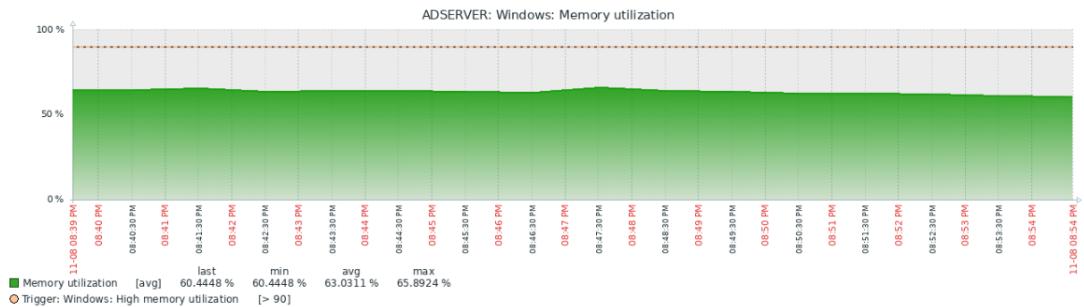
### 3.1.2 Servidor AD ( Active Directory )

O monitoramento e a gerência de ambientes de rede são componentes fundamentais para garantir o desempenho, a disponibilidade e a segurança de sistemas de rede, por isso foram feitos os testes para o serviço AD (Active Directory) da CREDIVALE DOCE. Esse serviço está localizado em um ambiente virtual local, possibilitando integrar ferramentas de monitoramento, como foi utilizado no caso o Zabbix Appliance, com o serviço de diretório, AD, para obter uma visão centralizada e eficiente da infraestrutura do serviço. O ambiente é composto por duas máquinas virtuais principais, o Zabbix Appliance, responsável pelo monitoramento e coleta de métricas dos dispositivos, servidores e serviços da rede. Ele é uma solução pronta para uso que já vem com o sistema operacional e o Zabbix Server pré-instalados hospedado no VirtualBox. E o Servidor AD (Active Directory) no Windows Server, responsável pelo gerenciamento de usuários, autenticação, políticas de grupo e demais funções de diretório hospedado no VirtualBox.

#### 3.1.2.1 Monitoramento da Infraestrutura

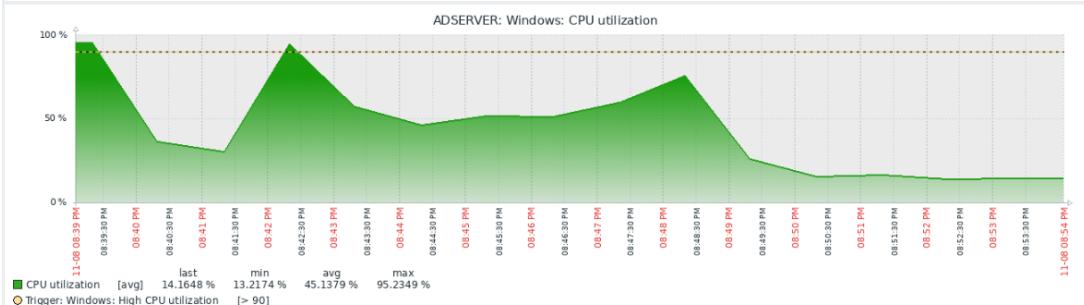
O Zabbix utiliza um agente instalado no host Windows para coletar dados detalhados, como disponibilidade de serviços, utilização de recursos e status de processos do sistema. Alertas e triggers são configurados para notificar administradores em caso de falhas ou degradação de desempenho. Dessa forma, os itens de monitoramento mais importantes para serem considerados quanto ao AD Server são o uso de memória RAM, o espaço de armazenamento e o consumo de CPU. No gráfico de utilização de memória (Figura 58) é possível perceber que a utilização da mesma não chegou em pontos críticos e se manteve estável, mostrando a estabilidade no serviço. Já no gráfico de utilização de CPU (Figura 59) houveram picos e quedas se mantendo mais estável para o final do gráfico, esses picos podem sinalizar uma sobrecarga devido a inicialização do Windows que depois se estabiliza à medida que o tempo passa.

**Figura 58 – AD Uso de Memória RAM**



**Fonte:** Elaborada pelos autores

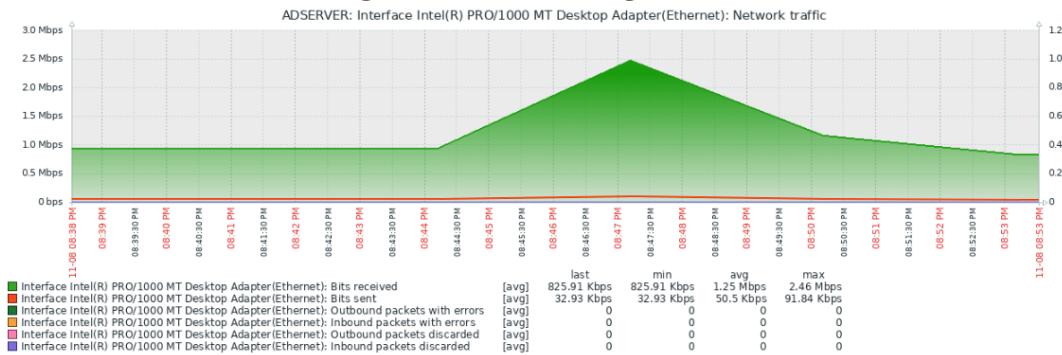
**Figura 59 – AD Uso de CPU**



**Fonte:** Elaborada pelos autores

O gráfico de tráfego de rede (Figura 60) mostrou que não houveram perdas de pacotes ou retransmissões anormais o que demonstra que a comunicação está funcionando corretamente, o tráfego está normal para um AD Server e o pico que houve no gráfico pode demonstrar um momento de maior demanda da rede, o que acompanha o uso normal de um server, um pico controlado e uma queda progressiva.

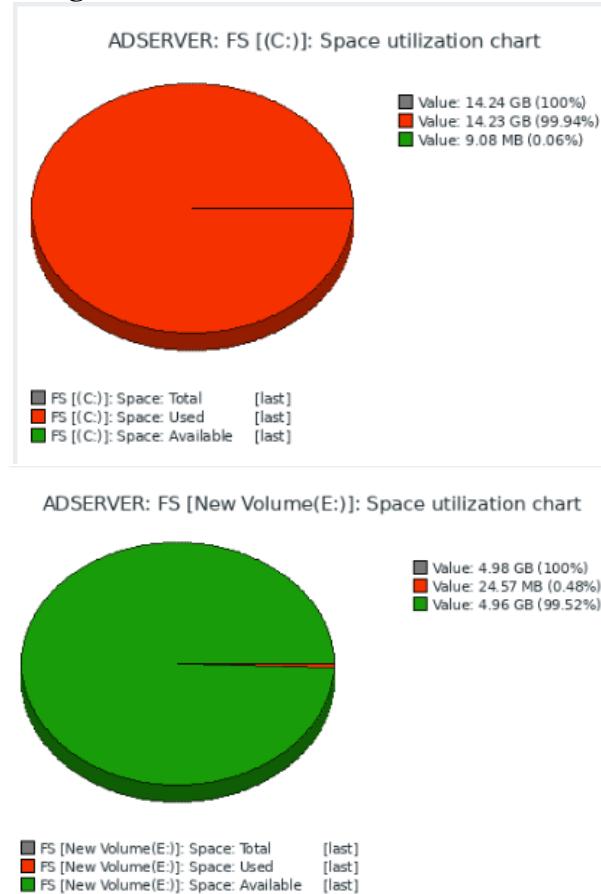
**Figura 60 – AD Tráfego de Rede**



Fonte: Elaborada pelos autores

Os gráficos de uso de espaço (Figura 61) apesar de demonstrar que o uso está no máximo, foi acrescentado uma memória extra para o melhor funcionamento da aplicação.

**Figura 61 – AD Armazenamento Disco 1**



Fonte: Elaborada pelos autores

### 3.1.2.2 Considerações Finais

A combinação do Zabbix Appliance com um servidor AD em um ambiente virtual local cria uma solução robusta de monitoramento e administração de rede. Essa arquitetura permite que os administradores mantenham total controle sobre os recursos, sem depender de serviços externos, e ainda aproveitem a flexibilidade de um ambiente virtualizado. Ao monitorar conti-

nuamente o Active Directory e os demais componentes da infraestrutura, a equipe de TI pode agir proativamente, prevenindo falhas, otimizando o desempenho e garantindo a disponibilidade dos serviços essenciais da rede corporativa.

### 3.2 Monitoramento em Máquinas Virtuais na AWS ( Amazon Web Service )

Para o ambiente em nuvem da AWS foi criada uma nova instância na EC2 para instalar e hospedar o servidor Zabbix que monitora todas as outras máquinas dos outros serviços. No frontend foi configurado um dashboard para unificar todos os gráficos em um só local, foi definido que os dados relevantes para todos os serviços seriam colocados cada um em um gráfico apenas, sendo eles a disponibilidade do agente, o uso de memória RAM e o uso de CPU.

Na Figura 62 é possível ver a disponibilidade do agente em cada máquina, o valor retornado para o monitor Zabbix é do tipo 0 ou 1, sendo 0 o agente não está respondendo e 1 significando que o cliente na máquina monitorada está funcional. Com isso foi configurado para que ao receber o valor 0 faça com que a cor de fundo fique vermelha e com o valor 1 fique verde, fazendo assim que fique intuitivo e de rápida assimilação a informação sobre a disponibilidade do monitoramento.

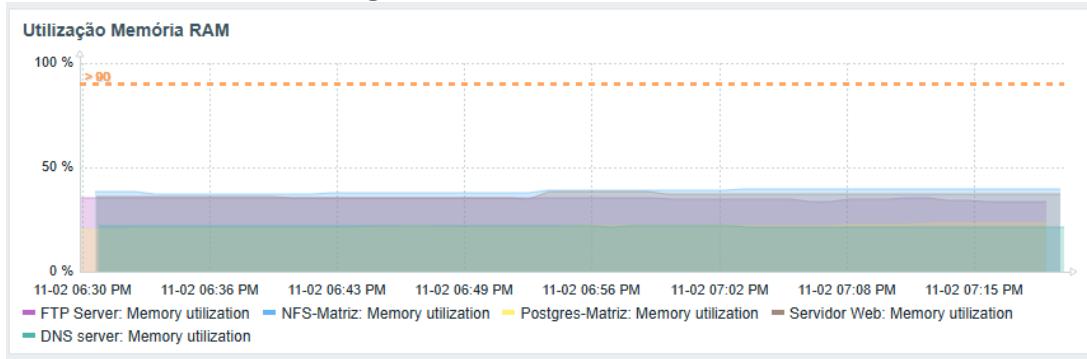
**Figura 62 – Disponibilidade dos Agentes - AWS**



**Fonte:** Elaborada pelos autores

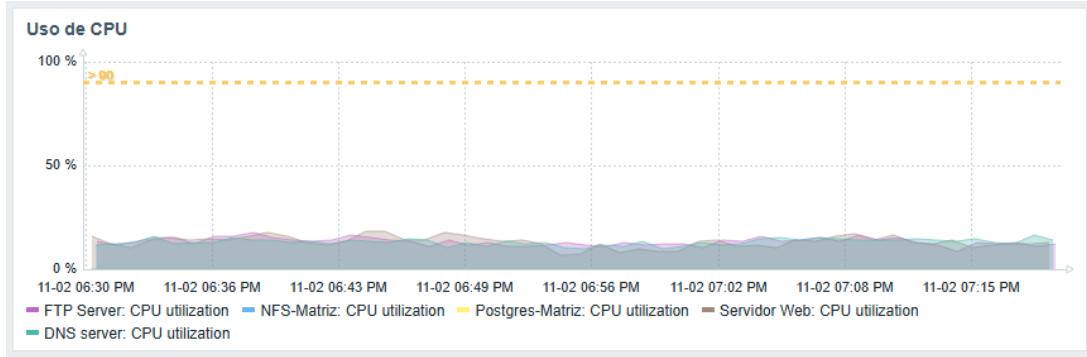
Para o uso da memória RAM e CPU foi escolhido mostrar os dados em um gráfico de linha em que o uso em porcentagem é representado no eixo y, e o eixo x representa o tempo. Podemos visualizar nas Figuras 63 e 64 que para todas as máquinas o uso de RAM e CPU foram suficientemente constantes no período monitorado, indicando que a carga sobre as máquinas não estavam sendo preocupantes. Também é possível visualizar no gráfico uma linha superior de gatilho para valores superiores a 90%, com ele é possível configurar alarmes de diversas maneiras para que ao atingir um valor tão alto o responsável tenha conhecimento do ocorrido e possa buscar outros dados para interpretar a fim de diagnosticar o problema e tomar ações para solucioná-lo.

**Figura 63 – Uso de RAM - AWS**



Fonte: Elaborada pelos autores

**Figura 64 – Uso de CPU - AWS**

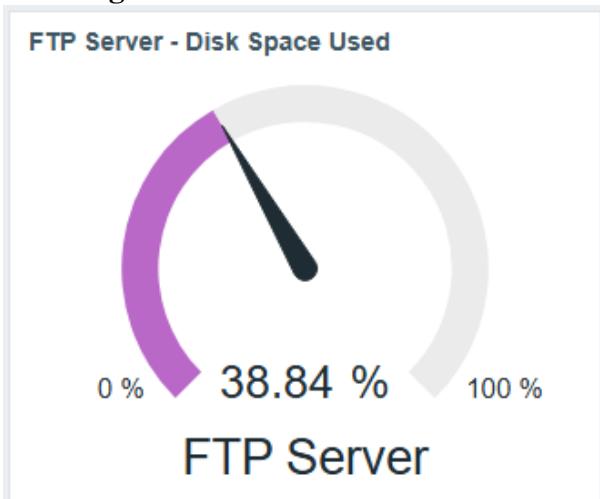


Fonte: Elaborada pelos autores

### 3.2.1 Servidor FTP ( *File Transfer Protocol* )

Pelo servidor de FTP ser responsável por transferir e armazenar os arquivos foram selecionados o espaço utilizado do disco e o tráfego de rede para serem monitorados por julgar como os dados mais relevantes para o serviço.

No gráfico mostrado pela Figura 65 podemos ver que o armazenamento está apenas 38,84% utilizado, esse valor é aceitável pois ainda está longe de atingir o limite do disco. Este gráfico é importante para conseguir identificar rapidamente a necessidade de rever políticas de armazenamento, ou mais comumente, a necessidade de expansão na capacidade do disco da máquina.

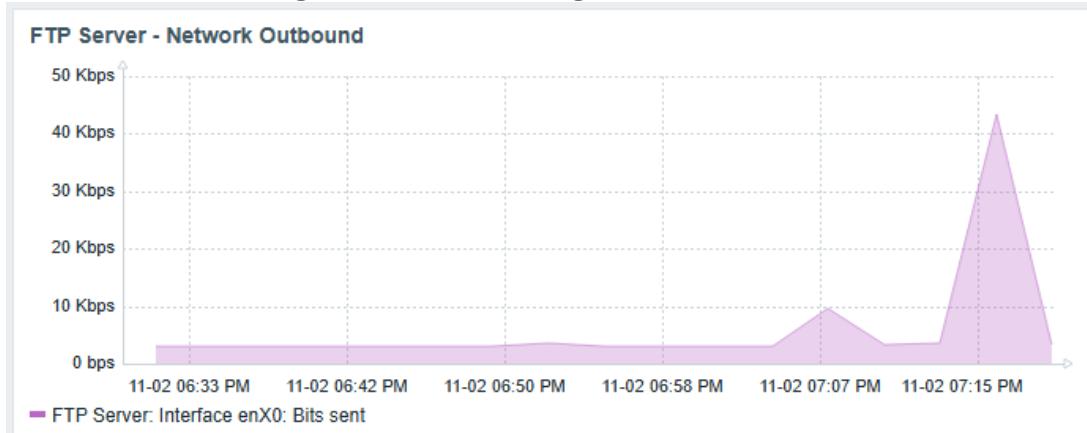
**Figura 65 – FTP Armazenamento**

Fonte: Elaborada pelos autores

Já na Figura 66 podemos visualizar o tráfego de rede de entrada e na Figura 67 o tráfego de saída da máquina, eles indicam principalmente quando estão acontecendo transferências de arquivos, por meio desses dados pode-se tirar informações como horário em que a máquina é mais utilizada, valor que ela necessidade de banda para funcionar sem ter problemas, até também momentos de anormalidades que podem ser referentes a mau uso, ou algum ataque, por exemplo. No gráfico de entrada, Figura 66, o único pico, que chega a um uso de 8 Mpbs, representa um momento em que foi enviado um arquivo maior para a máquina que está hospedando o serviço, já no gráfico de saída, Figura 67, os picos apresentados podem significar os momentos em que arquivos foram transferidos para uma ou mais máquinas clientes.

**Figura 66 – FTP Tráfego de Rede de Entrada**

Fonte: Elaborada pelos autores

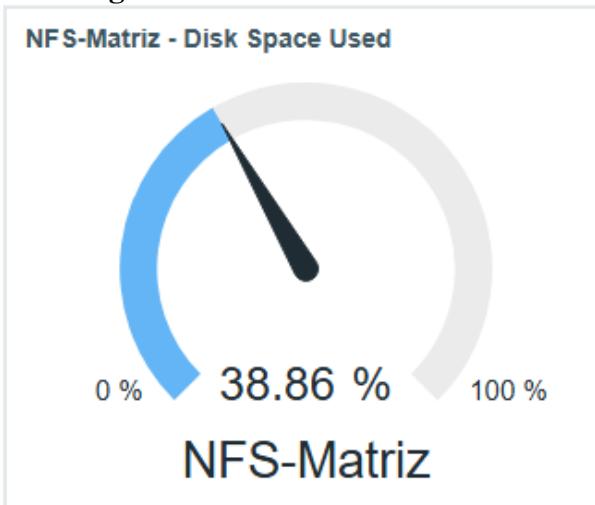
**Figura 67 – FTP Tráfego de Rede de Saída**

Fonte: Elaborada pelos autores

### 3.2.2 Servidor NFS ( Network File System )

Os gráficos apresentados nas Figuras 68, 69 e 70 referem-se ao monitoramento do serviço NFS (Network File System) configurado na instância do EC2 da AWS, responsável por prover o compartilhamento de arquivos entre os ambientes da matriz e da nuvem. O monitoramento foi realizado por meio do Zabbix Agent, com base nos indicadores Disk Space Used, Disk Read Rate (r/s) e Disk Write Rate (w/s), que permitem avaliar respectivamente a ocupação do volume, as operações de leitura e as operações de escrita por segundo no disco utilizado pelo NFS.

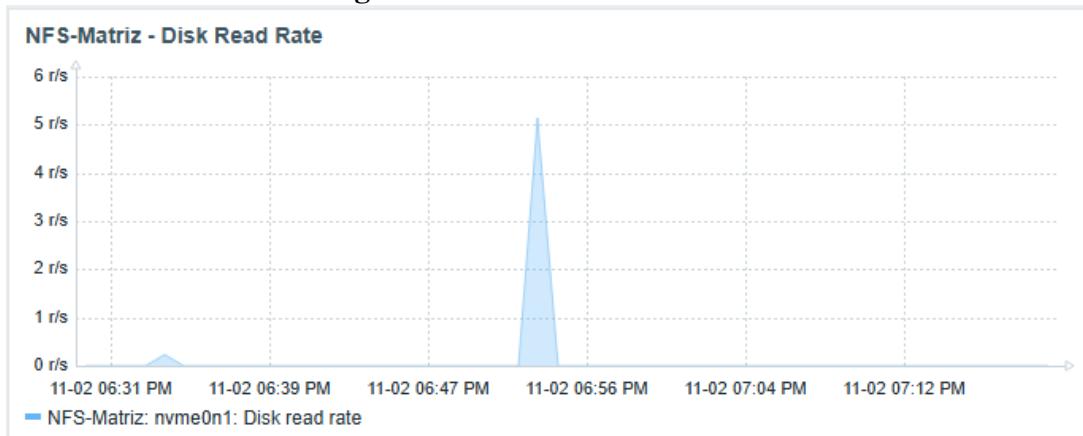
No gráfico da Figura 68 (NFS-Matriz – Disk Space Used), o percentual de utilização do volume em disco encontra-se em 38,86%, valor considerado dentro dos limites seguros de operação. Essa taxa indica que o ambiente ainda dispõe de ampla capacidade livre para armazenamento e expansão, sem risco imediato de esgotamento do espaço disponível. O indicador demonstra estabilidade e ausência de crescimento abrupto no consumo de espaço, evidenciando o uso controlado e consistente do armazenamento associado ao serviço NFS.

**Figura 68 – NFS Armazenamento**

Fonte: Elaborada pelos autores

Na sequência, o gráfico da Figura 69 (NFS-Matriz – Disk Read Rate) apresenta a taxa média de leitura durante o período de monitoramento em torno de 0,2 r/s, com picos de 5 r/s registrados durante períodos de maior demanda. As variações observadas refletem o acesso de múltiplos clientes à estrutura de diretórios compartilhados, mantendo-se, contudo, dentro dos parâmetros operacionais esperados. Não foram identificadas interrupções nem períodos prolongados de inatividade, indicando estabilidade nas operações de leitura.

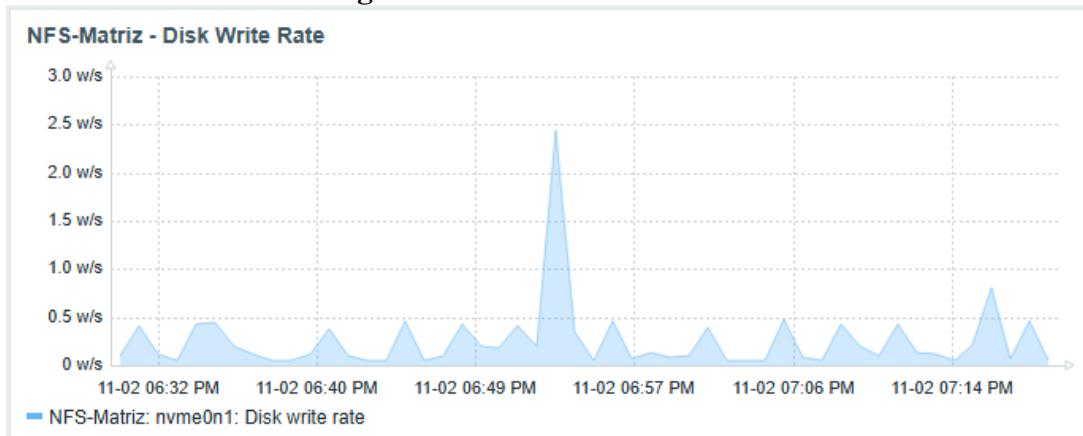
**Figura 69 – NFS Leitura de Disco**



Fonte: Elaborada pelos autores

Por fim, o gráfico da Figura 70 (NFS-Matriz – Disk Write Rate) demonstra comportamento semelhante, com média de 0,3 w/s e picos de 2,5 w/s correspondentes a momentos de escrita simultânea. O padrão de oscilação é característico do NFS em ambiente multiusuário, refletindo operações regulares de atualização de arquivos. O desempenho de escrita manteve-se estável durante todo o monitoramento.

**Figura 70 – NFS Escrita de Disco**



Fonte: Elaborada pelos autores

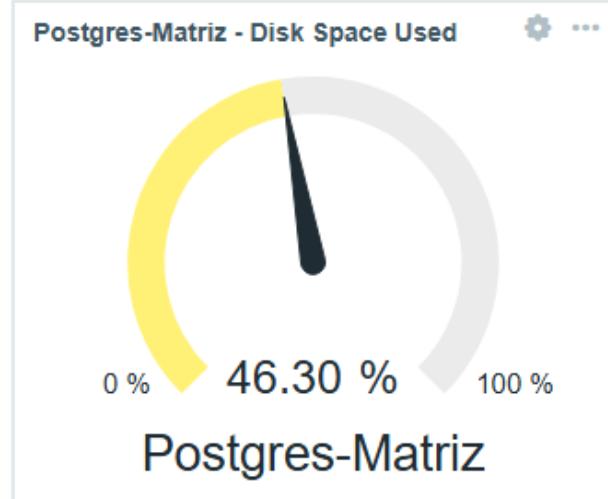
Em síntese, o serviço NFS operando em uma instância AWS apresenta desempenho estável, com utilização de disco de 38,86% e taxas de leitura e escrita coerentes com a carga de trabalho aplicada. Não foram observados gargalos, saturações ou anomalias de uso, confirmado a eficiência e a confiabilidade do serviço no ambiente de nuvem.

### 3.2.3 Servidor Banco de Dados ( Postgresql )

Os gráficos apresentados nas Figuras 71, 72 e 73 referem-se ao monitoramento do serviço PostgreSQL, que é um gerenciador de banco de dados relacional com o foco na segurança e escalabilidade para a empresa. Foi configurado utilizando uma instância do EC2 da AWS, é um sistema responsável por armazenar os dados da matriz em nuvem. O monitoramento foi realizado por meio do Zabbix Agent, com base nos indicadores Disk Space Used, Disk Utilization e Disk Network (Kbps), que permitem avaliar respectivamente a ocupação do volume, a utilização do espaço de armazenamento pelo PostgreSQL e a quantidade de dados trafegados durante um período de tempo.

No gráfico da Figura 71 (Postgres-Matriz – Disk Space Used), mostra a proporção do espaço total em disco que está atualmente sendo utilizado pelo servidor. O valor destacado é de 46,30%. O espaço em disco é um recurso crítico para qualquer servidor de banco de dados. Se o disco encher, o PostgreSQL pode parar de funcionar, resultando em indisponibilidade do serviço, falhas em transações e possivelmente corrupção de dados. Um uso de 46,30% indica que pouco menos da metade da capacidade total do disco está sendo utilizada. Isso é geralmente considerado uma situação saudável e segura, pois há espaço suficiente disponível para crescimento futuro, operações de manutenção (como backups, vacuums, etc.) e picos não planejados no uso.

**Figura 71 – Banco de Dados Armazenamento**

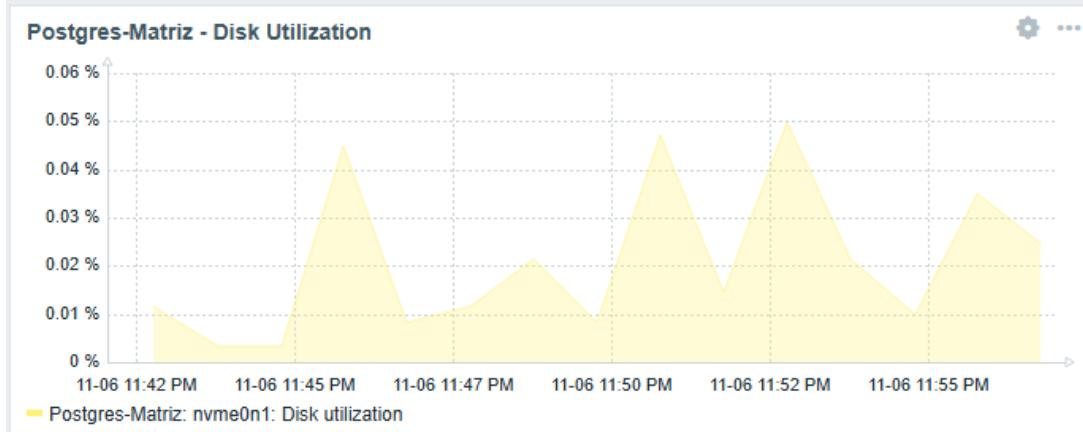


**Fonte:** Elaborada pelos autores

Na sequência, o gráfico da Figura 72 (Postgres-Matriz – Disk Utilization) é um gráfico que demonstra a taxa de utilização do disco (I/O – operações de leitura e escrita) ao longo do tempo. Os valores são muito baixos, variando entre 0.01% e 0.08%. A utilização do disco (I/O) mede o quanto ativo e sobrecarregado o subsistema de armazenamento está. Mesmo com espaço livre, um disco com I/O muito alto (100% de utilização) pode se tornar um gargalo, tornando o sistema lento, pois as operações ficam na fila aguardando para serem lidas ou escritas. Os valores extremamente baixos (menos de 0,1%) indicam que o servidor não está sob pressão de I/O. O disco está respondendo rapidamente às solicitações, sem formar filas. Isso é ideal

para o desempenho do banco de dados, especialmente para o PostgreSQL, que é intensivo em operações de disco.

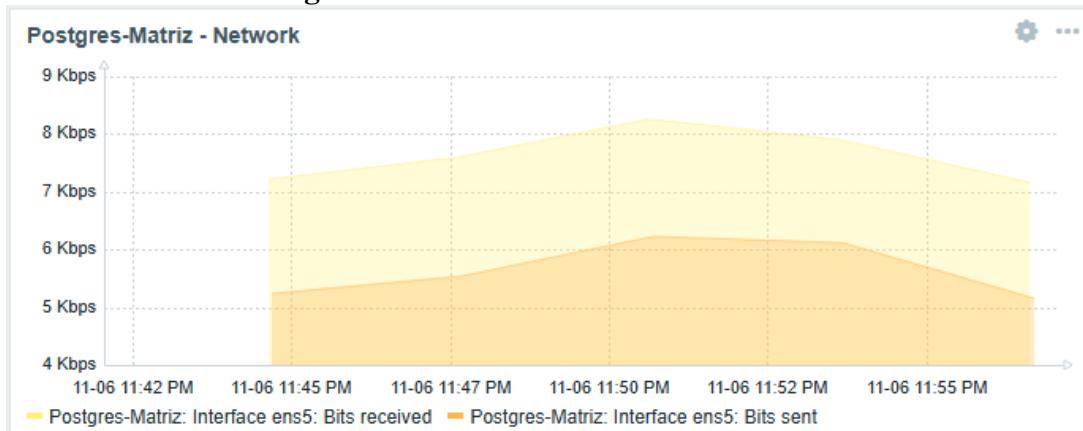
**Figura 72 – Banco de Dados Uso de Disco**



**Fonte:** Elaborada pelos autores

Por fim, o gráfico da Figura 73 (Postgres-Matriz – Network) que monitora o tráfego de rede do servidor, especificamente a taxa de transferência de dados nas interfaces de rede ens6 (dados recebidos) e ens5 (dados enviados). A unidade de medida é Kbps (Kilobits por segundo), e o pico mostrado é de aproximadamente 8 Kbps. A rede é o canal de comunicação do servidor de banco de dados com suas aplicações clientes e outros serviços. É crucial monitorar para identificar gargalos de comunicação, picos de tráfego anormais (que podem indicar um ataque ou problema na aplicação) ou para planejamento de capacidade. Um tráfego na casa de poucos Kbps é considerado muito baixo. Isso sugere que, no momento do monitoramento, o servidor estava lidando com uma carga de trabalho leve ou praticamente ociosa em termos de comunicação de rede. Não há congestionamento ou gargalo de rede. Para um servidor de banco de dados em produção sob carga normal, esperariam-se valores significativamente mais altos (Mbps ou até Gbps).

**Figura 73 – Banco de Dados Uso de Rede**



**Fonte:** Elaborada pelos autores

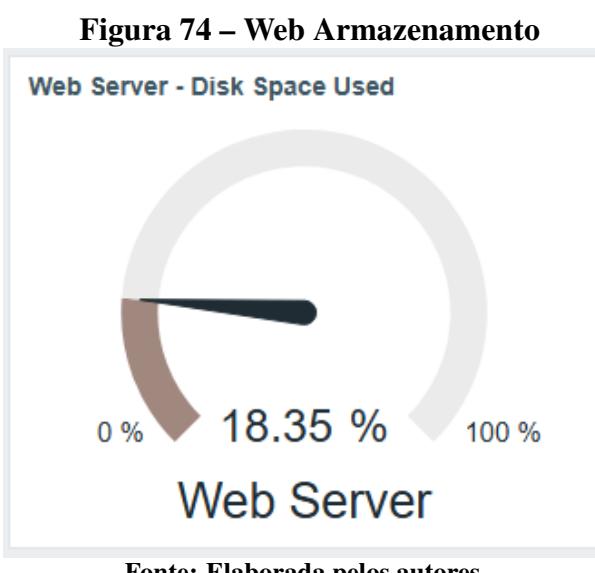
Com base nos dados monitorados, o servidor Postgres-Matriz está em um estado extremamente saudável e sem pressão em todos os recursos críticos analisados:

Disco: Tem espaço mais que suficiente (46,30% usado) e não sofre com lentidão de I/O (utilização abaixo de 0,1%). Rede: O tráfego é mínimo, indicando que não há uma carga pesada de consultas ou transferência de dados no momento. Esta é uma situação ideal, indicando que há uma grande margem para crescimento na carga de trabalho sem que o servidor enfrente problemas de desempenho imediatos. A monitorização contínua é essencial para detectar quando esses números começarem a aumentar para níveis que exijam atenção.

### 3.2.4 Servidor WEB

A Figura 74, 75 e 76 apresentam o monitoramento do Serviço Web, responsável por hospedar e disponibilizar aplicações corporativas por meio de um servidor dedicado. Esse serviço tem como principal função garantir o acesso estável, rápido e seguro aos sistemas web da organização, sendo essencial para o funcionamento contínuo das aplicações. O monitoramento foi realizado utilizando o Zabbix Agent, com base em três indicadores principais: Disk Space Used, Response Time e Falhas, que permitem acompanhar, respectivamente, o uso de armazenamento, o tempo médio de resposta da aplicação e a ocorrência de erros no serviço.

O gráfico da Figura 74 (Web Server – Disk Space Used) indica que 18,35% do espaço total em disco está sendo utilizado no servidor. Esse valor representa uma baixa taxa de ocupação, o que demonstra que há capacidade de armazenamento suficiente para o funcionamento do serviço e para futuras expansões. O monitoramento desse parâmetro é essencial, pois garante que o ambiente continue operando com segurança, evitando riscos de indisponibilidade causados por saturação do disco ou falhas na gravação de arquivos temporários e logs.

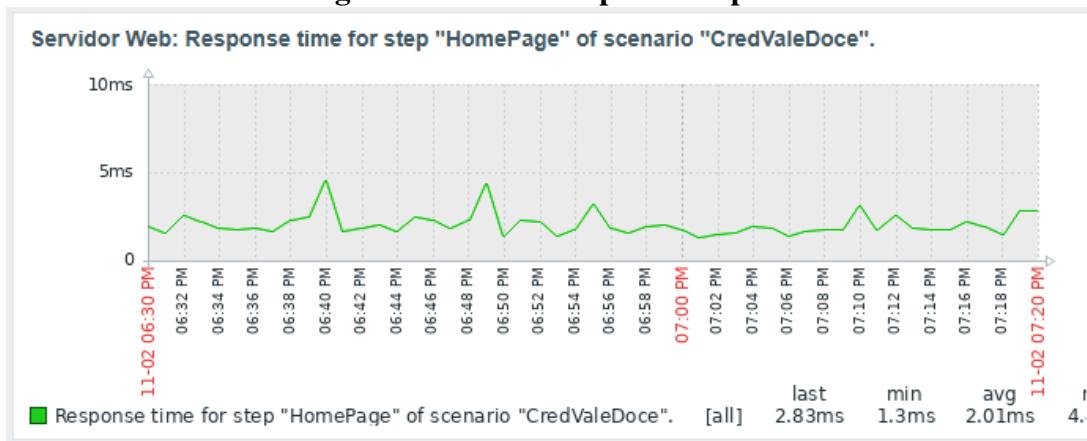


Fonte: Elaborada pelos autores

Já o gráfico Servidor Web – Response time for step "HomePage" of scenario "CredValeDoce" na Figura 75 apresenta o tempo de resposta da aplicação web durante o período de monitoramento. Os valores observados variam entre 1,3 ms e 2,83 ms, com média de 2,01 ms, indicando excelente desempenho e estabilidade. A constância da linha verde demonstra que o

servidor respondeu de forma rápida e uniforme às requisições simuladas, sem picos de lentidão, refletindo um ambiente otimizado e com boa capacidade de processamento.

**Figura 75 – Web Tempo de Resposta**



**Fonte:** Elaborada pelos autores

Por fim, o gráfico Servidor Web – Falhas na Figura 76 exibe a ocorrência de erros no cenário “CredValeDoce”. Nota-se um pequeno registro de falha pontual por volta das 11h13, que rapidamente foi normalizada, não havendo reincidências após esse horário. A baixa frequência e rápida recuperação indicam que o evento foi isolado e sem impacto significativo sobre a disponibilidade do serviço.

**Figura 76 – Web Número de Falhas**



**Fonte:** Elaborada pelos autores

Com base na análise dos três indicadores apresentados, conclui-se que o Serviço Web encontra-se em excelente estado operacional, apresentando desempenho estável e eficiente, com tempo médio de resposta de aproximadamente 2 ms, demonstrando agilidade no processamento das requisições; ocupação de disco de apenas 18,35%, indicando ampla capacidade disponível para o crescimento e manutenção das operações; apenas uma falha pontual registrada, rapidamente normalizada, sem impacto perceptível na disponibilidade ou estabilidade do serviço.

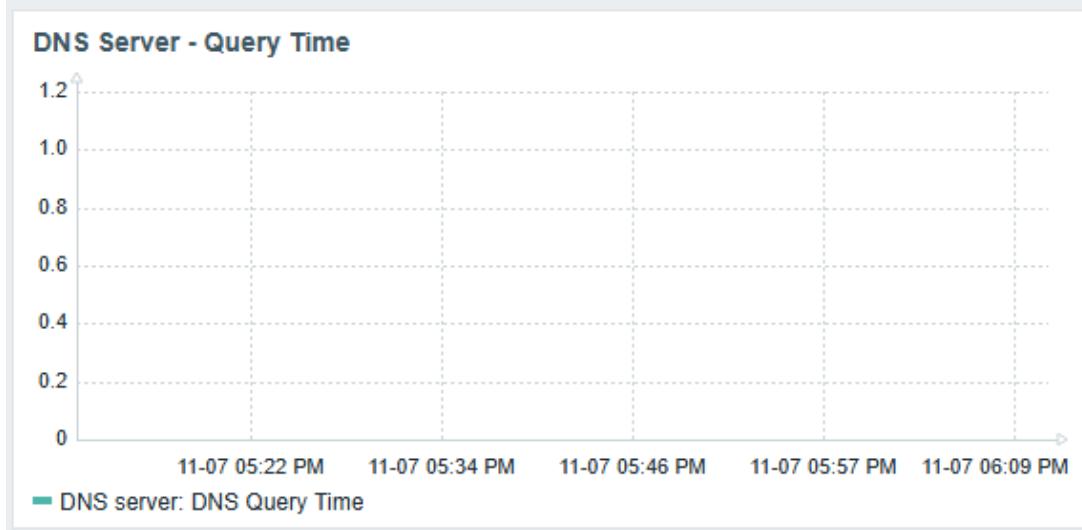
Em síntese, o ambiente web monitorado apresenta condições ideais de operação, com bom desempenho, baixo consumo de recursos e alta confiabilidade. Recomenda-se apenas a continuidade do monitoramento periódico, garantindo a detecção precoce de eventuais variações de desempenho e a manutenção da estabilidade observada.

### 3.2.5 Servidor DNS (*Domain Name Server*)

Foi realizado o monitoramento do serviço DNS (Domain Name System) hospedado na instância AWS EC2, utilizando o Zabbix Agent para coleta de métricas de desempenho e disponibilidade. Como o DNS tem papel essencial na rede, sendo responsável por traduzir nomes de domínio em endereços IP, logo, os usuários podem consultar os serviços sem a necessidade de utilizar e decorar endereços numéricos.

O gráfico Query Time na Figura 77 expõe o tempo médio de resposta das consultas DNS durante o período monitorado. Desse modo, observa-se que os valores permaneceram próximos de 0 ms, com variação mínima, indicando excelente desempenho do servidor. Logo, esse resultado evidencia que o serviço DNS está resolvendo os nomes de domínio de forma rápida e estável, sem atrasos perceptíveis ou falhas de comunicação.

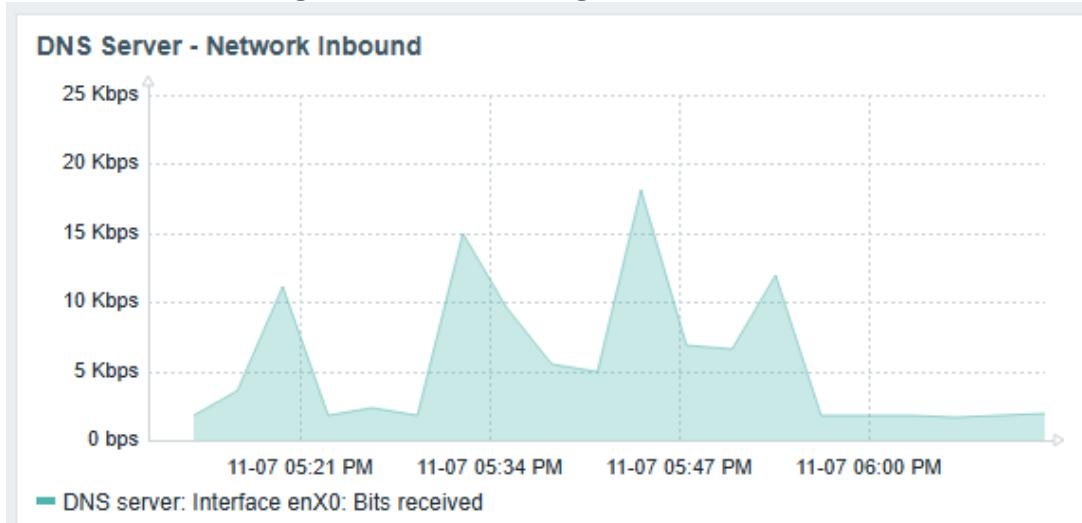
**Figura 77 – DNS Query Time**



**Fonte:** Elaborada pelos autores

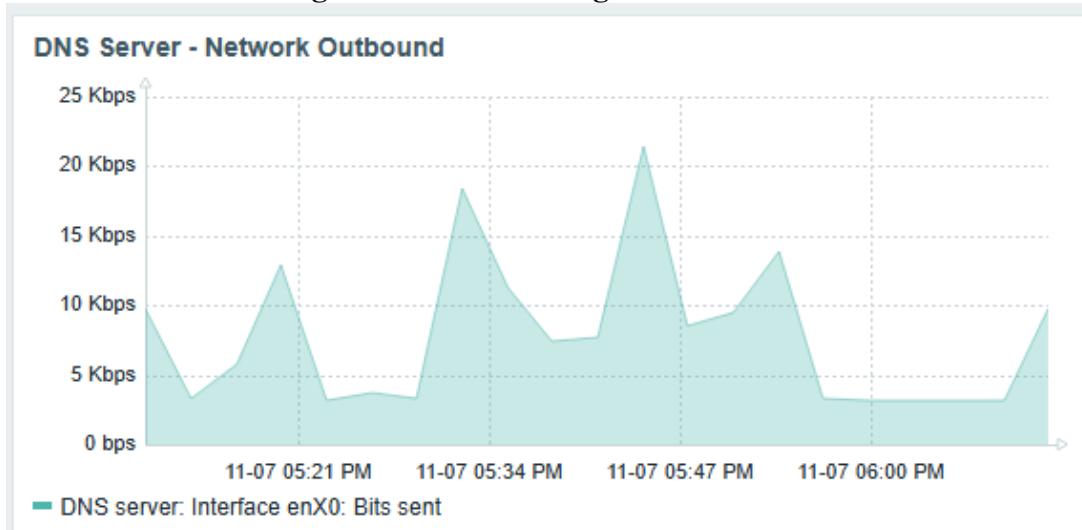
Os gráficos de Network Inbound e Network Outbound, nas Figuras 78 e 79 respectivamente, indicam o fluxo de dados recebidos e enviados pela interface de rede da instância DNS. Verifica-se uma atividade de rede constante, e como observado com picos variando entre 5 Kbps e 25 Kbps, o que demonstra que o servidor está sendo acessado regularmente e processando consultas em diferentes momentos. Desse modo, a alternância entre os valores de entrada e saída é esperada e representa o ciclo natural de recebimento de consultas (Inbound) e envio de respostas (Outbound).

**Figura 78 – DNS Tráfego de Rede Entrada**



Fonte: Elaborada pelos autores

**Figura 79 – DNS Tráfego de Rede Saída**



Fonte: Elaborada pelos autores

Portanto, o monitoramento do servidor DNS apresentou excelente estabilidade e desempenho, com tempo médio de resposta próximo de zero e tráfego de rede coerente com o volume de consultas. Esses resultados confirmam que o serviço está corretamente configurado, operando dentro dos padrões esperados e garantindo alta disponibilidade para os demais sistemas dependentes da resolução de nomes. Dessa forma, o Zabbix se mostrou uma ferramenta eficaz para acompanhar a performance do DNS, permitindo detectar possíveis falhas de rede ou lentidão antes que impactem o ambiente. O comportamento observado reforça a confiabilidade da configuração e a eficiência da infraestrutura implementada na AWS.

## 4 MECANISMOS E POLÍTICAS DE SEGURANÇA

### 4.1 Política de segurança da informação Cred Vale Doce

Com o objetivo de criar um ambiente seguro na Cred Vale Doce, foi elaborado o documento de Política de Segurança da Informação (PSI), que estabelece procedimentos, normas e diretrizes voltados à proteção dos dados da instituição. A PSI promove a conscientização sobre a importância da segurança entre todos os colaboradores, garantindo que cada pessoa compreenda seu papel na preservação das informações.

A política tem como finalidade assegurar a confidencialidade, integridade e disponibilidade das informações, bem como garantir a conformidade com as legislações e regulamentações aplicáveis. Seu escopo abrange todos os cooperados, colaboradores, parceiros e terceirizados que tenham acesso à rede da Cred Vale Doce.

Ao estabelecer diretrizes claras, a PSI fortalece a transparência, aumenta a eficiência operacional, contribui para a prevenção e gestão de crises, melhora a experiência dos usuários e reforça a confiança de todos. Assim, assegura-se que os dados estejam sempre disponíveis e protegidos quando necessário.

Mas apesar da implementação da Política de Segurança da Informação ser um passo muito importante na administração e segurança dos dados, ela sozinha não é o suficiente para garantir que os parâmetros listados em seu conteúdo sejam seguidos. Por isso, a cooperativa visa assegurar a adesão dos colaboradores através de diversas estratégias e do monitoramento, promovendo a internalização, aperfeiçoamento, o cumprimento e a sustentabilidade das práticas de segurança.

Das ações que a Cred Vale Doce implementa, destaca-se a construção de uma cultura organizacional, que envolve comunicação clara das normas, através da própria PSI, da cartilha de acesso seguro, de panfletos e da própria comunicação da empresa, visando incorporar valores associados à segurança, à ética e à responsabilidade coletiva. Essa cultura institucional também é reforçada por meio de discursos institucionais, exemplos de liderança e mecanismos formais de incentivo ao comportamento seguro.

A cooperativa também investe em processos de capacitação, não ficando apenas na transmissão de informações. Programas educativos, treinamentos práticos, simulações e atividades de sensibilização, são feitos periodicamente para garantir um ambiente seguro para todos e reforçar uma cultura de prevenção. Como o evento Hunting Week que está citado no item 4.3 deste documento. O uso de metodologias ativas de aprendizagem, como essas citadas acima, podem aumentar a retenção de conhecimento e o engajamento dos colaboradores. Há também processos de comunicação interna onde são criados múltiplos canais para facilitar a disseminação de informações e o feedback dos colaboradores. Alguns exemplos são comunicados periódicos, murais digitais, reuniões de equipe e espaços de diálogo contribuem para que todos sempre se mantenham atualizados.

Mas apenas a cultura da empresa, os processos de capacitação e comunicação ativa e passiva não são o suficientes para reforçar uma questão tão importante como a segurança da informação e de redes. Sendo assim, o monitoramento e avaliação se fazem necessários, pois eles permitem identificar o grau de conformidade e os pontos de melhoria. Por isso, são feitas auditorias internas, checklists operacionais, análises de incidentes e indicadores de desempenho que são ferramentas essenciais para verificar a aplicação das diretrizes e assegurar que as práticas estejam alinhadas aos padrões estabelecidos. A cooperativa possui também mecanismos de responsabilização e reconhecimento, tendo uma definição clara de consequência caso as normas sejam descumpridas e a valorização e reconhecimento no caso delas serem seguidas corretamente.

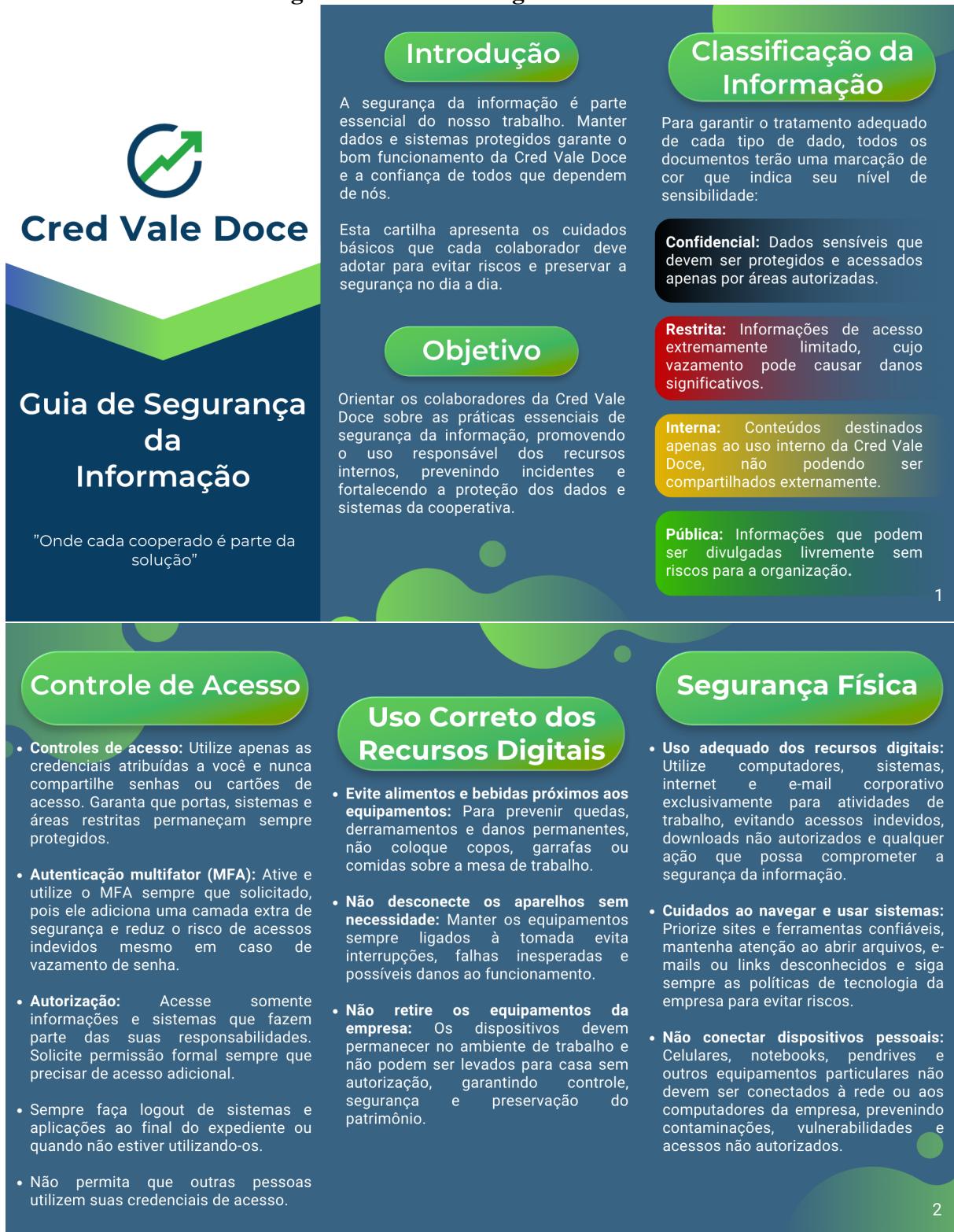
Dessa forma, é possível perceber que é imprescindível promover a participação ativa dos colaboradores na construção, revisão e aprimoramento das diretrizes. Garantir que as informações da política de segurança sejam efetivamente seguidas exige uma abordagem multidimensional. Somente por meio da articulação entre cultura organizacional, capacitação contínua, monitoramento rigoroso, comunicação eficaz, mecanismos de incentivo e participação coletiva é possível alcançar níveis elevados de conformidade, protegendo a segurança de todos.

Link para a PSI: [Política de Segurança da Informação](#)

#### **4.2 Cartilha de acesso seguro Cred Vale Doce**

A Cartilha de Acesso Seguro da Cred Vale Doce ( Figura 80 e 81 ), que será impressa em formato de livreto, foi desenvolvida com o objetivo de promover um ambiente mais protegido para todos. O material é destinado tanto aos cooperados quanto aos colaboradores e ao público em geral interessado no tema. A Cred Vale Doce busca garantir um sistema seguro e de fácil compreensão para todos os usuários, incentivando uma postura mais proativa e consciente sobre a importância do papel de cada um na proteção das informações. Dessa forma, a cartilha contribui para fortalecer a segurança e ampliar a cultura de responsabilidade no uso dos sistemas.

**Figura 80 – DNS Tráfego de Rede Saída**



**Cred Vale Doce**

**Guia de Segurança da Informação**

"Onde cada cooperado é parte da solução"

**Controle de Acesso**

- Controles de acesso:** Utilize apenas as credenciais atribuídas a você e nunca compartilhe senhas ou cartões de acesso. Garanta que portas, sistemas e áreas restritas permaneçam sempre protegidos.
- Autenticação multifator (MFA):** Ative e utilize o MFA sempre que solicitado, pois ele adiciona uma camada extra de segurança e reduz o risco de acessos indevidos mesmo em caso de vazamento de senha.
- Autorização:** Acesse somente informações e sistemas que fazem parte das suas responsabilidades. Solicite permissão formal sempre que precisar de acesso adicional.
- Sempre faça logout de sistemas e aplicações ao final do expediente ou quando não estiver utilizando-os.**
- Não permita que outras pessoas utilizem suas credenciais de acesso.**

**Introdução**

A segurança da informação é parte essencial do nosso trabalho. Manter dados e sistemas protegidos garante o bom funcionamento da Cred Vale Doce e a confiança de todos que dependem de nós.

Esta cartilha apresenta os cuidados básicos que cada colaborador deve adotar para evitar riscos e preservar a segurança no dia a dia.

**Objetivo**

Orientar os colaboradores da Cred Vale Doce sobre as práticas essenciais de segurança da informação, promovendo o uso responsável dos recursos internos, prevenindo incidentes e fortalecendo a proteção dos dados e sistemas da cooperativa.

**Classificação da Informação**

Para garantir o tratamento adequado de cada tipo de dado, todos os documentos terão uma marcação de cor que indica seu nível de sensibilidade:

- Confidencial:** Dados sensíveis que devem ser protegidos e acessados apenas por áreas autorizadas.
- Restrita:** Informações de acesso extremamente limitado, cujo vazamento pode causar danos significativos.
- Interna:** Conteúdos destinados apenas ao uso interno da Cred Vale Doce, não podendo ser compartilhados externamente.
- Pública:** Informações que podem ser divulgadas livremente sem riscos para a organização.

**Uso Correto dos Recursos Digitais**

- Evite alimentos e bebidas próximos aos equipamentos:** Para prevenir quedas, derramamentos e danos permanentes, não coloque copos, garrafas ou comidas sobre a mesa de trabalho.
- Não desconecte os aparelhos sem necessidade:** Manter os equipamentos sempre ligados à tomada evita interrupções, falhas inesperadas e possíveis danos ao funcionamento.
- Não retire os equipamentos da empresa:** Os dispositivos devem permanecer no ambiente de trabalho e não podem ser levados para casa sem autorização, garantindo controle, segurança e preservação do patrimônio.

**Segurança Física**

- Uso adequado dos recursos digitais:** Utilize computadores, sistemas, internet e e-mail corporativo exclusivamente para atividades de trabalho, evitando acessos indevidos, downloads não autorizados e qualquer ação que possa comprometer a segurança da informação.
- Cuidados ao navegar e usar sistemas:** Priorize sites e ferramentas confiáveis, mantenha atenção ao abrir arquivos, e-mails ou links desconhecidos e siga sempre as políticas de tecnologia da empresa para evitar riscos.
- Não conectar dispositivos pessoais:** Celulares, notebooks, pendrives e outros equipamentos particulares não devem ser conectados à rede ou aos computadores da empresa, prevenindo contaminações, vulnerabilidades e acessos não autorizados.

**Fonte: Elaborada pelos autores**

**Figura 81 – DNS Tráfego de Rede Saída**

### Recuperação em Desastres e Respostas a Incidentes

- **Plano de Contingência:** Deve ser mantido um plano de contingência para garantir que as operações possam ser retomadas rapidamente em caso de interrupção.
- **Backup:** Os dados críticos devem ser regularmente copiados e armazenados em locais seguros para garantir sua recuperação.
- **Reportar qualquer anomalia imediatamente:** Qualquer falha, lentidão incomum ou comportamento suspeito deve ser comunicado à equipe responsável assim que identificado.
- **Seguir as instruções da TI durante incidentes:** Em situações de risco, é importante cumprir as orientações para ajudar na contenção e evitar que o problema se agrave.

### Responsabilidades do Colaborador

- Apoiar o processo de recuperação: Após o incidente, seguir os procedimentos de restauração e adotar as medidas preventivas atualizadas ajuda a reduzir futuras ocorrências.
- Tratar dados **Confidenciais e Restritos** com máxima proteção.
- Não compartilhar informações fora dos canais autorizados.
- Solicitar permissão antes de acessar dados de outro setor.
- Reportar imediatamente qualquer suspeita de acesso indevido.
- Cumprir as leis, regulamentos e normas aplicáveis relacionados a segurança da informação: Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), Marco Civil da Internet (Lei nº 12.965/2014) e Normativos do Banco Central do Brasil e do Conselho Monetário Nacional.

### Papel dos Colaboradores

- **Participação essencial:** Cada pessoa tem um papel fundamental na proteção das informações da Créd Vale Doce, adotando práticas seguras no dia a dia e seguindo as orientações estabelecidas.
- **Engajamento contínuo:** Buscar conhecer e cumprir as políticas internas fortalece a segurança e reduz riscos para toda a organização.
- **Conscientização e treinamento:** É importante acompanhar nosso programa de conscientização e participar dos treinamentos de segurança, mantendo-se atualizado sobre procedimentos, boas práticas e novas ameaças.



### Penalidades e Infrações

- **Descumprimento das políticas de segurança:** Violações das regras estabelecidas podem resultar em advertências, registros formais e outras medidas disciplinares previstas pela empresa.
- **Uso indevido de equipamentos ou informações:** Ações que coloquem dados, sistemas ou patrimônio em risco podem gerar penalidades mais severas, conforme a gravidade.
- **Reincidência ou infrações graves:** Casos repetidos ou condutas que causem prejuízo à organização podem levar a sanções maiores, seguindo as normas internas e a legislação aplicável.

Para mais informações acesse:



### Viu algo suspeito?

Qualquer irregularidade deve ser reportada assim que percebida.

### Fiquem sempre de olho!

Prestem atenção a nossas diretrizes e normas na nossa política de segurança da informação para se manter sempre atualizado. A segurança de todos é uma responsabilidade nossa.

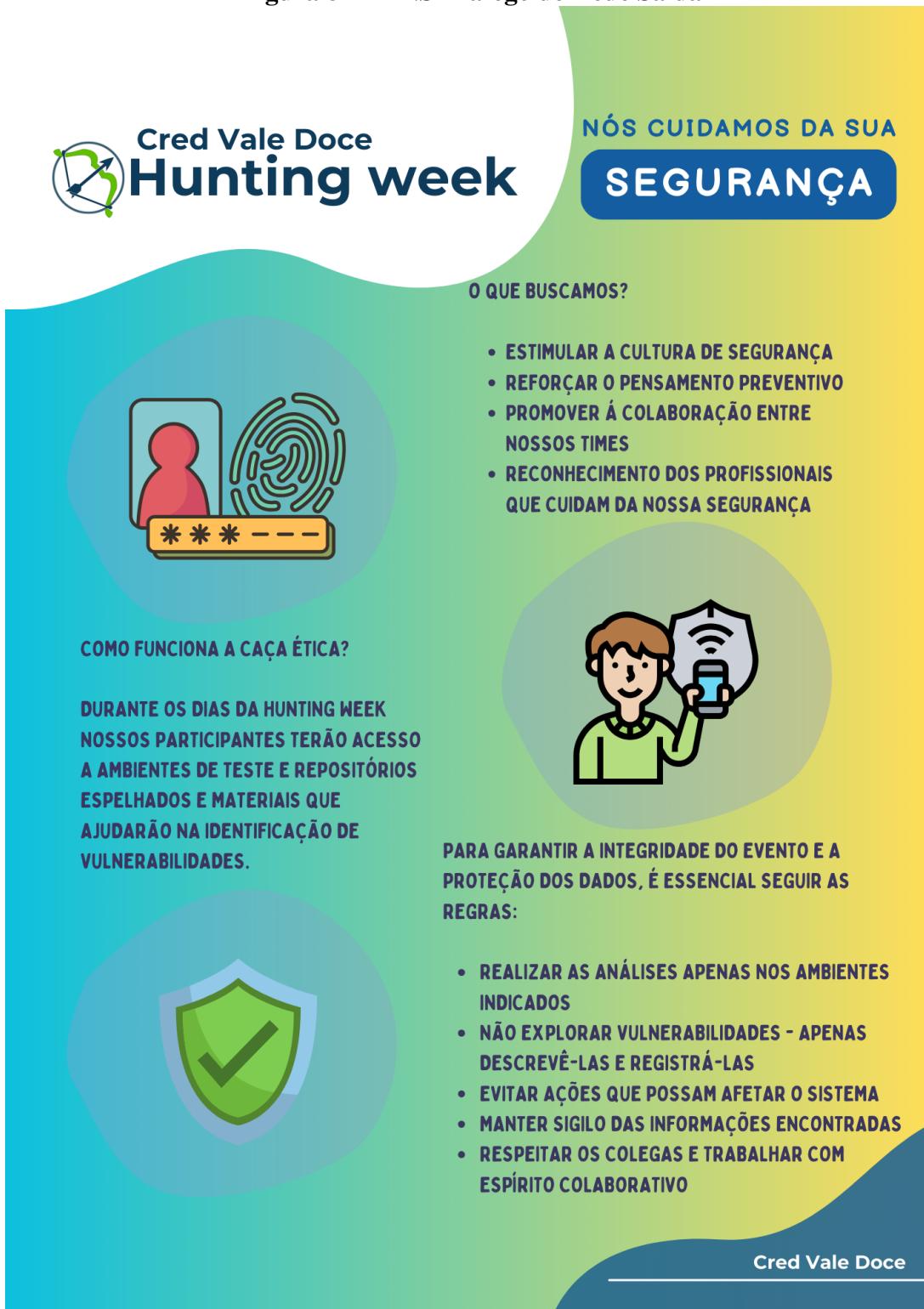


**Fonte: Elaborada pelos autores**

#### **4.3 Evento Cred Vale Hunting Week**

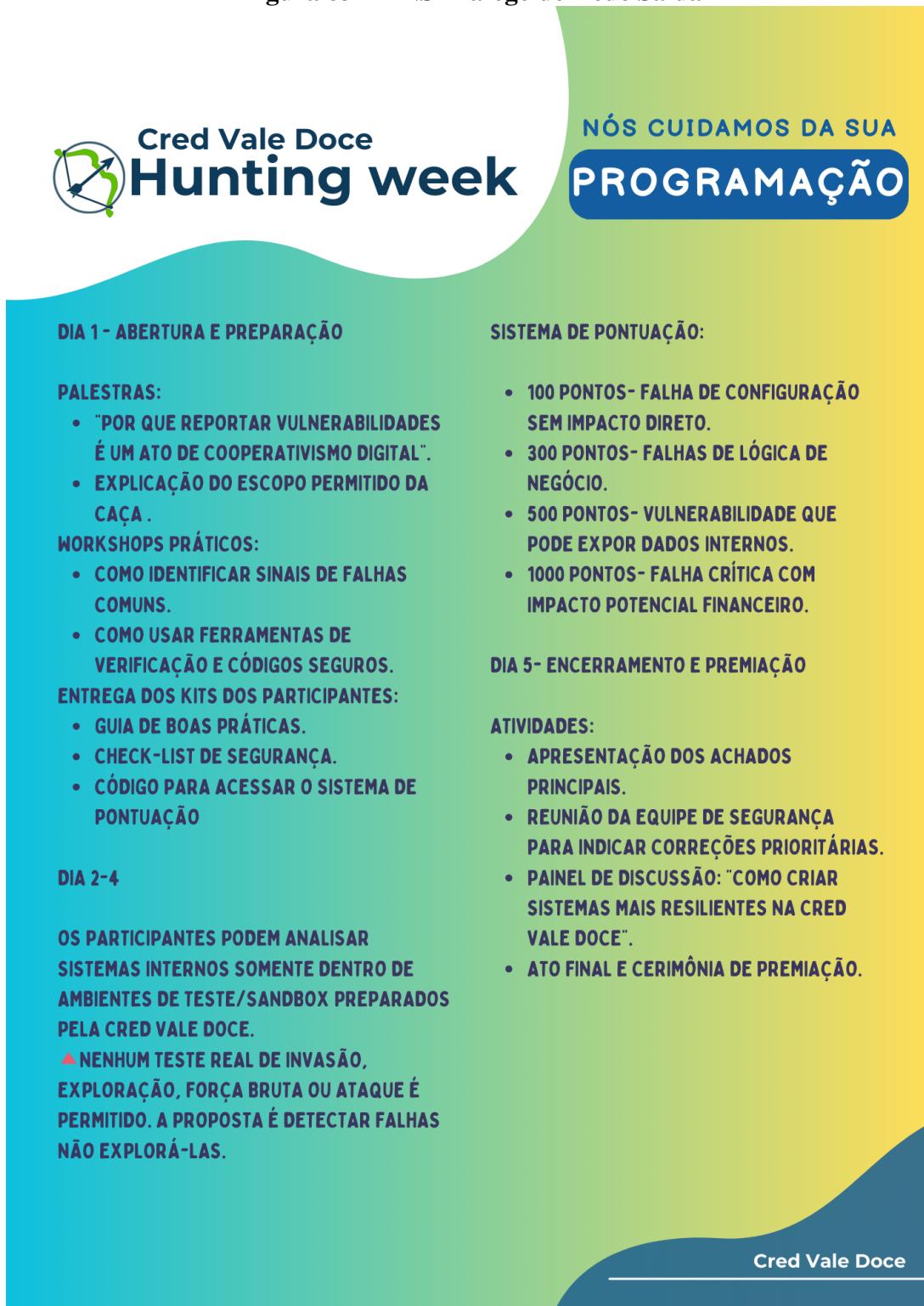
A Cred Vale Doce Hunting Week é um evento semestral promovido pela Cred Vale Doce com o objetivo de criar um ambiente controlado, educativo e gamificado que mantenha os colaboradores, principalmente os da área de TI, atualizados e engajados nas questões de segurança da informação. Cada edição tem duração de cinco dias e conta com um sistema de pontuação, ambientes controlados e a produção de materiais e relatórios técnicos. Esses conteúdos contribuem para aprimorar a segurança da cooperativa, atualizar planos de ação, avaliar impactos e definir melhorias nos processos internos. Dessa forma, o evento visa contribuir para a redução de riscos à segurança, o aumento do engajamento das equipes, o fortalecimento da cultura de reporte responsável e uma maior promoção da integração entre os membros do time. Com isso, espera-se obter sistemas mais estáveis, confiáveis e seguros. As figuras 82, 83 e 84 mostram uma programação de uma edição do evento.

**Figura 82 – DNS Tráfego de Rede Saída**



Fonte: Elaborada pelos autores

Figura 83 – DNS Tráfego de Rede Saída



Fonte: Elaborada pelos autores

**Figura 84 – DNS Tráfego de Rede Saída**



Fonte: Elaborada pelos autores

## 4.4 Análise de vulnerabilidade

Tomando como referência o OWASP Top 10 (2021), são apresentadas abaixo as vulnerabilidades de segurança mais relevantes que podem afetar a rede da Cred Vale Doce. Essas vulnerabilidades devem ser cuidadosamente analisadas para que sejam adotadas as medidas de prevenção adequadas (OWASP FOUNDATION, 2021d).

### 4.4.1 A01:2021 – *Broken Access Control*

O controle de acesso falho, representa um desafio comum enfrentado por muitas instituições na atualidade. Quando o assunto é ambientes financeiros, qualquer falha que permita a um usuário acessar informações ou funções além do permitido podem gerar fraudes, vazamento de dados de clientes, manipulação de contas ou exposição de dados sigilosos, regulados ou sensíveis. Como a cooperativa possui múltiplos perfis, aumenta a complexidade e fica mais suscetível a erros. É necessário ficar atento para que na Cred Vale Doce, não surjam problemas como o risco de funcionários de diferentes filiais ou setores acessarem dados indevidos, alterações de limites, taxas ou informações internas de maneira incorreta, vazamento de dados sensíveis por APIs sem controle adequado e usuários com permissões limitadas obterem acesso administrativo indevido (OWASP FOUNDATION, 2021a).

Para evitar essas situações, é fundamental restringir o acesso a documentos como configuração padrão, permitindo exceções apenas para arquivos públicos. É essencial também que o controle de acesso seja baseado em papéis com perfis bem definidos e não confiar apenas no front-end para limitar as ações dos usuários, toda permissão deve ser validada no servidor. Outra ação é impedir que o mesmo usuário execute fluxos completos que possam gerar fraude, como abrir e aprovar uma transação. Devem haver restrições rigorosas nas APIs e verificações de permissões a cada endpoint. Os controles de acesso devem assegurar que somente os proprietários dos dados possam visualizá-los, modificá-los ou copiá-los, sem presumir que qualquer usuário possui essas permissões. Além disso, em caso de múltiplas tentativas de acesso com falhas, o sistema deve emitir um alerta ao administrador, reforçando a segurança.

Além disso, tendo em vista a segurança de seus cooperados, a cooperativa também pode implementar o bloqueio de acesso a contas de outros cooperados, assegurar o controle de acesso diferenciado por filial e garantir que somente auditoria possa acessar dados consolidados da cooperativa inteira.

### 4.4.2 A02:2021 – *Cryptographic Failures*

Como as cooperativas lidam frequentemente com informações sensíveis, o uso de criptografia torna-se indispensável. Ela é essencial para proteger dados bancários, credenciais e

transações. Falhas nela podem expor números de conta, dados pessoais, extratos, chaves de API, tokens de autenticação, etc, além de ser uma exigência regulatória para instituições financeiras. Entre os problemas que podem ocorrer na transmissão desses dados estão a utilização de versões desatualizadas de Segurança da Camada de Transporte (TLS), uso de protocolos fracos, vazamento de chaves privadas de comunicação entre sistemas, emprego de criptografia fraca em VPNs internas e o armazenamento inadequado de dados dos cooperados (OWASP FOUNDATION, 2021b).

Para evitar falhas desse tipo, é fundamental ter uma criptografia forte, desabilitando protocolos e suites fracas, implementando chaves protegidas em HSM ou cofres de segredo. Também é importante implementar chaves com ciclo de vida definido, acesso restrito e mecanismos de revogação. Outro aspecto que deve ser levado em consideração é classificar corretamente os dados, identificar quais são sensíveis e armazená-los somente quando estritamente necessário, garantindo sempre que sua criptografia esteja atualizada e segura. Além disso, é importante manter atualizados os algoritmos, chaves e protocolos de segurança, aplicar controles compatíveis com o nível de sensibilidade das informações, utilizar criptografia autenticada e realizar verificações independentes para assegurar a eficácia das configurações adotadas. A criptografia deve ser obrigatória para dados de conta, CPF, extratos e tokens de transação e a proteção deve ser forte para as integrações, como o PIX, e para sistemas internos.

#### ***4.4.3 A07:2021 – Identification and Authentication Failures***

Para evitar que usuários não autorizados se autentiquem ou que contas legítimas sejam comprometidas, é necessário proteger dados sensíveis e as transações financeiras. Essas falhas de identificação e autenticação podem representar vulnerabilidades significativas porque uma única falha de autenticação pode comprometer dados, fundos e a confiança na cooperativa. Uma cooperativa de crédito lida com dados pessoais sensíveis, informações e transações financeiras, e quando há falhas na identificação ou autenticação o sistema não verifica corretamente se o usuário é quem diz ser, pode acabar permitindo que senhas, tokens ou sessões sejam explorados e ocorra o bypass de login. Outros riscos possíveis são controles de autenticação inconsistentes entre filiais, uso de senhas fracas ou compartilhadas e falhas em sistemas responsáveis pelo gerenciamento de dados dos cooperados. Essas falhas são críticas porque permitem que um atacante obtenha acesso a contas de cooperados ou sistemas internos, podendo gerar fraudes, roubo de dados e prejuízos financeiros (OWASP FOUNDATION, 2021c).

Para mitigar esses problemas, é recomendável adotar autenticação multifator sempre que possível e obrigatória para logins de colaboradores internos, acesso de cooperados ao internet/mobile banking e aprovação de transações críticas. Também é importante eliminar completamente o uso de credenciais padrões, especialmente para contas administrativas. As senhas devem ser fortes e as políticas devem ser rígidas como o comprimento mínimo de 12 caracteres, combinando letras, números e símbolos, a expiração de senha deve ser baseada em risco,

deve ocorrer o bloqueio temporário após tentativas falhas, e deve ser proibida a reutilização de senhas anteriores. As sessões e autenticações também devem ser controladas, devendo ocorrer a expiração automática após inatividade, o logout obrigatório em mudanças de senha ou transações críticas, a detecção de comportamentos suspeitos, alertas devem acontecer em tentativas de login incomuns e deve ocorrer a revisão e bloqueio automático de contas com padrões suspeitos.

Para a recuperação e redefinição de conta segura devem ser seguidos processos de redefinição de senha com verificação de múltiplos fatores, evitar que perguntas de segurança frágeis sejam feitas como “nome da mãe” ou “cidade natal” do indivíduo e devem ser registradas e auditadas todas as alterações de credenciais que forem feitas. Sempre devem ser feitos também o monitoramento e a auditoria de tentativas de login falhas, logins simultâneos incomuns, padrões de autenticação suspeitos, e a auditoria deve ser sempre feita para contas privilegiadas e eventos críticos e deve haver a integração com sistema de antifraude para alertar operações suspeitas. A autenticação de dois fatores deve ser obrigatória para acesso a dados de cooperados, aprovação de transações financeiras, as tentativas de login por agência ou IP devem ser limitadas, a autenticação deve ser reforçada para sistemas integrados como o PIX e os logs devem ser detalhados para auditoria interna e compliance BACEN.

## 5 DESENVOLVIMENTO WEB BACK-END

Para colocar em prática as normas de segurança e aprimorar o funcionamento interno da Cred Vale Doce, criamos uma aplicação web, com um Back-end bem organizado para assegurar que os dados da empresa sejam gerenciados de forma segura e eficaz. A aplicação foi desenvolvida em php juntamente com React (Javascript), está rodando em um servidor Apache hospedado em uma instância na EC2 da AWS, ela pode ser acessada por meio do endereço "http://[Ip Público da Instância]/cooperativa/" a partir dos dispositivos que possuem permissões de acesso. A máquina virtual foi preparada para hospedar os serviços de backend com php, frontes com Javascript e banco de dados com PostgreSQL. O sistema foi idealizado para reunir toda a administração de dados em um só lugar, funcionando como uma ferramenta essencial para a organização e o controle das atividades da cooperativa.

A base dessa estrutura é o "Sistema de Gestão da Cooperativa" (Figura 85), um painel administrativo que une os setores mais importantes da instituição. Como pode ser visto na interface abaixo, o Back-end controla o acesso a partes específicas, permitindo que os usuários com permissão gerenciem de forma simples as Unidades, Funções, Setores e Colaboradores. Essa divisão em partes torna a navegação mais fácil e garante a organização para que cada aspecto da cooperativa seja administrado de maneira separada e organizada.

**Figura 85 – DNS Tráfego de Rede Saída**

**Fonte:** Elaborada pelos autores

Além da visão macro sobre o sistema, o desenvolvimento do back-end teve seu foco na funcionalidade detalhada de cada módulo, implementando operações completas de criação, leitura, atualização e exclusão (CRUD) de dados. Um exemplo prático dessa implementação é o módulo de Filiais mostrado na Figura 86, que faz parte do Sistema de Gestão da Cooperativa, foi criado para gerenciar de maneira centralizada todas as unidades físicas da Cred Vale Doce. Esse componente possibilita o registro, a modificação e a organização em nível hierárquico das diversas localidades de atuação da cooperativa, assegurando que as informações se mantenham coerentes em toda a rede.

O módulo tem como objetivo principal fornecer uma visão unificada da estrutura física da organização, permitindo o controle detalhado de cada unidade e facilitando a gestão operacional distribuída. Seu escopo inclui desde a matriz principal até as filiais regionais, criando um mapa organizacional completo da presença territorial da cooperativa. Através deste módulo, a cooperativa implementa mecanismos de controle e padronização que garantem a uniformidade operacional entre todas as unidades, além de fornecer dados essenciais para tomadas de decisão estratégicas sobre expansão e otimização da rede física. O sistema permite ainda a integração com outros módulos, como o de funcionários, facilitando a alocação de recursos humanos de acordo com a localização geográfica.

A interface também disponibiliza botões de ação intuitivos ("Editar" e "Excluir") e a opção de adicionar novas unidades ("+ Nova Filial"), evidenciando a capacidade do sistema de processar requisições dinâmicas e manter o banco de dados da Cred Vale Doce sempre íntegro e atualizado.

**Figura 86 – DNS Tráfego de Rede Saída**

The screenshot shows a table titled "Filiais" (Branches) with the following data:

ID	Nome	Cidade	Ações
2	Filial 1 - Cidade A	Cidade A	<button>Editar</button> <button>Excluir</button>
3	Filial 2 - Cidade B	Cidade B	<button>Editar</button> <button>Excluir</button>
5	Filial 3 - Cidade D	João Monlevade	<button>Editar</button> <button>Excluir</button>
1	Matriz - Cooperativa Vale do Créditos	Cidade Polo	<button>Editar</button> <button>Excluir</button>

[+ Nova Filial](#)

**Fonte: Elaborada pelos autores**

Dessa forma, o desenvolvimento da aplicação está funcional, as outras páginas que aparecem como cards na primeira imagem foram criadas, porém possuem a mesma formatação e estruturação igual a da segunda imagem, sendo assim, páginas com funcionalidades parecidas. Cada módulo desenvolvido incorpora princípios de usabilidade, segurança e integridade de dados, trabalhando em conjunto com as políticas de segurança da informação para criar um ambiente gerencial confiável e eficiente.

Por meio da implementação de sistemas integrados e padronizados é possível garantir a consistência das informações organizacionais, a rastreabilidade das operações e a eficiência na gestão dos recursos, contribuindo para o fortalecimento institucional e para a melhoria contínua dos serviços oferecidos pela cooperativa.

## REFERÊNCIAS

OPPENHEIMER, P. **Projeto de redes top-down**: um enfoque de análise de sistemas para o projeto de redes empresariais. Rio de Janeiro: Campus, 1999.

OWASP FOUNDATION. **A01:2021 – Broken Access Control**. 2021. Disponível em: <[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)>. Acesso em: 24 de nov. 2025.

OWASP FOUNDATION. **A02:2021 – Cryptographic Failures**. 2021. Disponível em: <[https://owasp.org/Top10/A02\\_2021-Cryptographic\\_Failures/](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/)>. Acesso em: 24 de nov. 2025.

OWASP FOUNDATION. **A07:2021 – Identification and Authentication Failures**. 2021. Disponível em: <[https://owasp.org/Top10/A07\\_2021-Identification\\_and\\_Authentication\\_Failures/](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)>. Acesso em: 24 de nov. 2025.

OWASP FOUNDATION. **OWASP Top 10 - 2021**. 2021. Disponível em: <[https://owasp.org/Top10/A00\\_2021\\_Introduction/](https://owasp.org/Top10/A00_2021_Introduction/)>. Acesso em: 24 de nov. 2025.