



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

Projeto da infraestrutura de rede - Cooperativa Bancária CoopCred

Ítalo Fideles Vieira do Nascimento¹
Jully Anne Roman Palhano Dutra²
Lucas Moraes Barcelos³
Pedro Henrique Nunes Alves⁴
Victor Hugo Vasquez da Silva⁵
Vinícius Pereira Coelho⁶
Fábio Leandro Rodrigues Cordeiro⁷

Resumo

A evolução tecnológica nas instituições financeiras exige ambientes de rede cada vez mais robustos, seguros e bem estruturados. Observa-se, no entanto, que a ausência de documentação técnica pode comprometer a manutenção e a escalabilidade desses ambientes. Justifica-se, portanto, a necessidade de descrever de forma clara e objetiva os recursos de rede adotados pela CoopCred. Este trabalho tem como objetivo apresentar a infraestrutura de rede da instituição, detalhando os componentes físicos e lógicos envolvidos, sua topologia, os padrões utilizados e as medidas de segurança implementadas. Para tanto, foram realizadas análises de campo, levantamento de equipamentos e estudo das políticas de segurança em vigor. Os resultados obtidos revelam uma rede estruturada com base em boas práticas de TI, utilizando equipamentos atualizados e políticas eficazes de proteção de dados. Conclui-se que a documentação apresentada contribui significativamente para a gestão do ambiente de rede, oferecendo suporte a futuras expansões, auditorias e ações de melhoria contínua.

Palavras-chave: infraestrutura de rede; segurança da informação; topologia de rede; documentação técnica; CoopCred;

*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.

¹Aluno(a) do Programa de Graduação em Sistemas de Informação – ifvnascimento@sga.pucminas.br.

²Aluno(a) do Programa de Graduação em Sistemas de Informação – jarpdutra@sga.pucminas.br.

³Aluno(a) do Programa de Graduação em Sistemas de Informação – lucas.barcelos.1439634@sga.pucminas.br.

⁴Aluno(a) do Programa de Graduação em Sistemas de Informação – pedro.alves.1460908@sga.pucminas.br.

⁵Aluno(a) do Programa de Graduação em Sistemas de Informação – vhvsilva@sga.pucminas.br.

⁶Aluno(a) do Programa de Graduação em Sistemas de Informação – vinicius.coelho.1404638@sga.pucminas.br.

⁷Professor(a) do Programa de Graduação em Sistemas de Informação – fabioleandro@pucminas.br.

Abstract

Technological advancements in financial institutions demand increasingly robust, secure, and well-structured network environments. However, the lack of technical documentation may hinder the maintenance and scalability of such environments. Therefore, it is essential to clearly and objectively describe the network resources adopted by CoopCred. This paper aims to present the institution's network infrastructure by detailing the physical and logical components involved, its topology, the standards applied, and the implemented security measures. Field analysis, equipment surveys, and the study of current security policies were conducted to support the development of this work. The results show a structured network based on IT best practices, utilizing up-to-date equipment and effective data protection policies. It is concluded that the presented documentation contributes significantly to network management, providing support for future expansions, audits, and continuous improvement actions.

Keywords: network infrastructure; information security; network topology; technical documentation; CoopCred;

1 INTRODUÇÃO

Este documento tem como finalidade apresentar a infraestrutura de rede da CoopCred, detalhando os recursos físicos e lógicos envolvidos, sua topologia, os padrões adotados e as medidas de segurança implementadas. A proposta é fornecer uma visão clara e técnica do ambiente atual, servindo como base para manutenção, expansão e auditorias futuras.

1.1 Apresentação Institucional e Diretrizes Estratégicas

A CoopCred - Cooperativa de Crédito de Minas Gerais foi fundada com o objetivo de oferecer soluções financeiras acessíveis e seguras para seus cooperados. Com sede na cidade de Uberaba - MG, a cooperativa expandiu suas atividades e hoje conta com cinco filiais distribuídas em cidades próximas, consolidando-se como uma instituição confiável no setor financeiro. Atualmente, a empresa possui um quadro de 350 funcionários, que atuam para garantir a qualidade e eficiência dos serviços prestados.

As filiais da CoopCred estão localizadas nas seguintes cidades:

- Filial 1: Patos de Minas - MG
- Filial 2: Poços de Caldas - MG
- Filial 3: Montes Claros - MG
- Filial 4: Governador Valadares - MG
- Filial 5: Sete Lagoas - MG

Missão: Prover serviços financeiros de qualidade, garantindo segurança, transparência e acessibilidade aos cooperados, promovendo o desenvolvimento econômico e social das comunidades atendidas.

Visão: Ser referência no setor de cooperativas de crédito em Minas Gerais, destacando-se pela inovação tecnológica, segurança e eficiência nos serviços prestados aos cooperados.

1.2 Justificativa do Projeto

Com o constante crescimento da CoopCred e a expansão de suas atividades para diversas regiões de Minas Gerais, torna-se essencial garantir que a infraestrutura de rede acompanhe as demandas operacionais e tecnológicas da cooperativa. A rede corporativa, tanto em sua camada física quanto lógica, precisa estar preparada para suportar o tráfego de dados de forma segura, eficiente e escalável.

Segundo Tanenbaum e Wetherall (Tanenbaum; Wetherall, 2011), uma rede de computadores bem estruturada é a base para o funcionamento confiável de sistemas distribuídos, especialmente em organizações com múltiplas unidades. Complementando esse ponto de vista, Stallings (Stallings, 2014) destaca que a segurança da informação deve ser tratada como um elemento essencial da arquitetura de rede, prevenindo acessos não autorizados, interrupções de serviço e perdas de dados.

Além disso, a necessidade de conformidade com normas e regulamentações, como a Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018), exige que a CoopCred adote práticas de governança e segurança baseadas em padrões reconhecidos internacionalmente. Entre eles, destaca-se a norma ISO/IEC 27001 (ABNT, 2013), que estabelece requisitos para sistemas de gestão da segurança da informação.

Cavalcanti (Cavalcanti, 2021) ressalta que o planejamento de uma infraestrutura de rede moderna deve considerar não apenas conectividade e desempenho, mas também escalabilidade, resiliência frente a falhas e capacidade de resposta a incidentes. Esse tipo de abordagem estruturada possibilita não apenas o atendimento às demandas atuais, mas também a preparação para futuras expansões e adoção de novas tecnologias.

Este projeto visa não apenas descrever a situação atual da rede da CoopCred, mas também embasar futuras decisões relacionadas à modernização tecnológica, à implementação de políticas de segurança mais robustas e ao suporte a auditorias internas e externas. Dessa forma, busca-se alinhar a infraestrutura de TI com os objetivos estratégicos da organização, garantindo a continuidade dos negócios com eficiência, segurança e conformidade.

1.3 Objetivo

Este projeto visa desenvolver a infraestrutura de rede para a CoopCred, garantindo a conectividade confiável entre a matriz e as filiais, além de oferecer serviços internos essenciais para o funcionamento seguro e eficiente da instituição.

A infraestrutura será projetada para suportar os serviços financeiros da cooperativa, incluindo operações bancárias internas, sistemas de transações online, comunicação entre unidades e segurança dos dados. Para isso, serão implementadas segmentações de rede, políticas de segurança e redundância para minimizar falhas, assegurando alta disponibilidade e proteção das informações sensíveis da instituição.

1.4 Objetivos específicos

- Documentar a infraestrutura de rede da CoopCred, proporcionando uma visão clara de sua composição atual;
- Servir como base para manutenção, expansão e auditoria da rede corporativa;

- Garantir o alinhamento com as melhores práticas de TI e segurança da informação;
- Apoiar o time técnico em tomadas de decisão estratégicas e operacionais;

1.5 Estrutura Organizacional da CoopCred

A distribuição dos colaboradores da CoopCred está organizada entre a matriz e as filiais, conforme ilustrado na Tabela 1. A matriz, localizada em Uberaba - MG, conta com 150 funcionários. As cinco filiais, situadas em diferentes cidades do interior de Minas Gerais, possuem 40 colaboradores cada, totalizando 350 funcionários em toda a empresa.

1.6 Departamentos Principais

- **Administração e Finanças** – Gerencia os investimentos, orçamentos e estratégias financeiras.
- **TI e Infraestrutura** – Responsável pela segurança digital, servidores, redes e suporte técnico.
- **Atendimento e Relacionamento** – Equipe de suporte ao cliente e serviços bancários presenciais.
- **Crédito e Financiamento** – Avaliação e concessão de empréstimos e financiamentos.
- **Segurança e Compliance** – Monitoramento de fraudes, auditorias e regulamentações financeiras.

Tabela 1 – Distribuição dos Funcionários por Setor e Unidade

| Setor | Matriz (Uberaba) | Cada Filial | Total |
|--------------------------|------------------|-------------|------------|
| Diretoria Executiva | 5 | 0 | 5 |
| Gerência e Administração | 20 | 5 | 45 |
| TI e Infraestrutura | 25 | 5 | 50 |
| Atendimento e Caixa | 50 | 20 | 150 |
| Crédito e Financiamento | 30 | 7 | 65 |
| Segurança e Compliance | 20 | 3 | 35 |
| Total | 150 | 40 | 350 |

Fonte: Elaborado pelos autores (2025).

1.7 Principais Serviços da CoopCred

Produtos Financeiros

- Conta Corrente e Conta Poupança – Para cooperados realizarem depósitos, pagamentos e movimentações.
- Empréstimos e Financiamentos – Linhas de crédito com taxas reduzidas para pessoas físicas e empresas.
- Crédito Rural e Empresarial – Apoio ao setor agrícola e pequenos negócios.
- Cartões de Crédito – Opções de cartão com benefícios exclusivos para cooperados.

Serviços Bancários

- PIX, TED e DOC – Transferências rápidas e seguras.
- Boletos e Pagamentos – Emissão e pagamento de contas.
- Investimentos e Previdência – Planos de investimento e aposentadoria.
- Seguro e Consórcios – Proteção financeira para cooperados.

Canais de Atendimento

- Agências Físicas – Atendimento presencial na matriz e nas 5 filiais.
- Aplicativo e Internet Banking – Acesso remoto aos serviços bancários.
- Central de Atendimento – Suporte telefônico e via chat.

1.8 Esboço da Proposta de Projeto de Redes

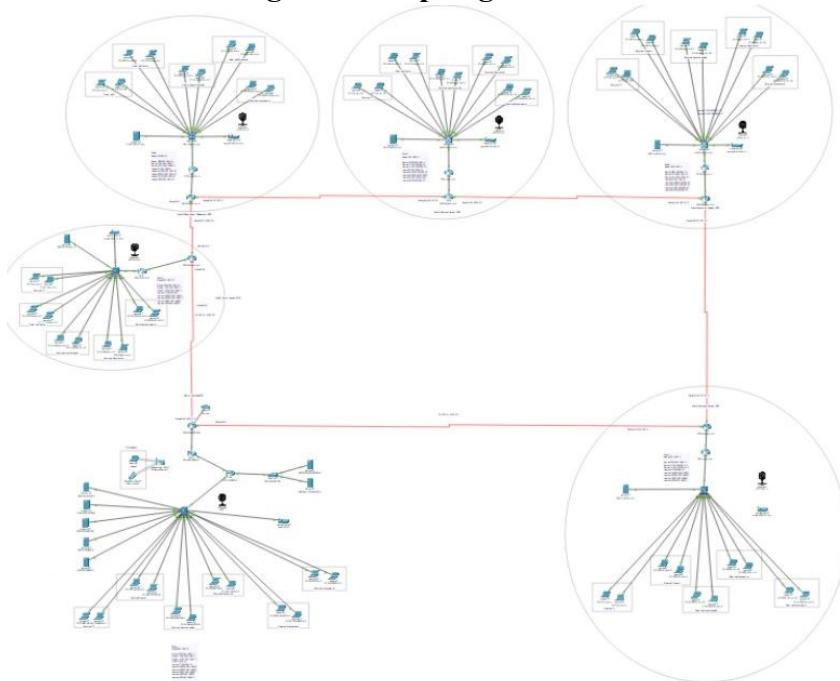
O projeto de rede proposto para a CoopCred visa garantir uma infraestrutura robusta, segura e escalável, capaz de atender às necessidades atuais e futuras da cooperativa. Isso inclui a implementação de tecnologias modernas para conexão entre a matriz e as filiais, políticas de segurança eficazes e mecanismos de redundância para minimizar interrupções.

1.9 Estrutura Lógica e Física da Rede

Topologia

A rede será projetada com foco em segmentação, segurança e alta disponibilidade. A comunicação entre as unidades será estabelecida por meio de uma WAN em Anel, na qual as filiais estão interconectadas entre si e com a matriz, formando um circuito fechado. Essa topologia proporciona redundância, garantindo que, em caso de falha em um dos links, o tráfego de dados seja redirecionado por um caminho alternativo, assegurando a continuidade e resiliência da rede.

Figura 1 – Topologia de Rede



Fonte: Packet tracer(2025)

Cada filial estará conectada às outras unidades e à matriz por meio de links dedicados, utilizando tecnologias como VPN/MPLS. Essas tecnologias garantirão a segurança da comunicação por meio de criptografia avançada e políticas rigorosas de controle de acesso, assegurando a integridade e confidencialidade dos dados (Stallings, 2016; Tanenbaum; Wetherall, 2013).

Na camada local, cada unidade contará com sua própria LAN hierárquica, segmentada em diferentes camadas para otimizar o gerenciamento e a segurança:

- **Camada de Acesso:** Nessa camada, encontram-se os dispositivos finais, como PCs e servidores, conectados a switches de acesso. Aqui, a prioridade é a conectividade com os dispositivos finais, garantindo acesso rápido e eficiente (Cisco Systems, Inc., 2018).
 - **Camada de Distribuição:** A comunicação entre as diversas áreas da rede (interna e DMZ) será gerenciada por switches de distribuição, que conectam a camada de acesso à camada de núcleo. Essa camada facilita a organização do tráfego e melhora a performance da rede (Forouzan, 2017).
 - **Camada de Núcleo:** Composta pelos roteadores da matriz e das filiais, responsáveis pela comunicação entre as localidades e com a rede externa. A topologia WAN em Anel assegura uma distribuição equilibrada do tráfego e melhora a resiliência da rede contra falhas (Tanenbaum; Wetherall, 2013).

A rede será projetada para alta disponibilidade, com redundância de links entre a matriz e as filiais, permitindo a continuidade das operações mesmo em caso de falha de conectividade. A adoção de VPN/MPLS proporciona uma solução robusta e segura para interligar as unidades de forma eficiente, mantendo a integridade dos dados e garantindo o desempenho da rede (Stallings, 2016).

1.10 Endereçamento IP e Sub-redes

A faixa de IP privada utilizada será **192.168.0.0/16** para a LAN, **10.10.0.0/16** para a WAN e **172.16.0.0/16** para a DMZ, subdividida em sub-redes /24 para garantir organização e escalabilidade conforme a Tabela 2.

Tabela 2 – Endereçamento IP das Unidades e Serviços

| Unidade | Cidade | Faixa de Rede | Máscara (CIDR) | Hosts Disponíveis |
|-------------------------|---------------------------|------------------|-----------------|-------------------|
| Matriz | Uberaba - MG | 192.168.0.0/24 | 255.255.255.0 | 254 |
| Filial 1 | Patos de Minas - MG | 192.168.1.0/24 | 255.255.255.0 | 254 |
| Filial 2 | Poços de Caldas - MG | 192.168.2.0/24 | 255.255.255.0 | 254 |
| Filial 3 | Montes Claros - MG | 192.168.3.0/24 | 255.255.255.0 | 254 |
| Filial 4 | Governador Valadares - MG | 192.168.4.0/24 | 255.255.255.0 | 254 |
| Filial 5 | Sete Lagoas - MG | 192.168.5.0/24 | 255.255.255.0 | 254 |
| Servidor Central | Uberaba - MG | 192.168.100.0/26 | 255.255.255.192 | 62 |
| VPN | Todas as Unidades | 10.10.200.0/27 | 255.255.255.224 | 30 |
| MPLS | Todas as Unidades | 10.10.200.32/27 | 255.255.255.224 | 30 |
| DMZ Web Pública | Uberaba - MG | 172.16.250.0/27 | 255.255.255.224 | 30 |
| DMZ E-mail | Uberaba - MG | 172.16.10.0/27 | 255.255.255.224 | 30 |

Fonte: Elaborado pelos autores (2025).

Tabela de Materiais

Matriz

Tabela 3 – Equipamentos - Matriz

| Equipamento | Quantidade |
|------------------|------------|
| Roteador 2911 | 3 |
| Switch 3560-24 | 1 |
| Switch 2960 24TT | 1 |
| Servidor PT | 6 |
| PC | 150 |
| Total | 161 |

Fonte: Elaborado pelos autores (2025).

Filiais**Tabela 4 – Equipamentos - Filiais**

| Equipamento | Quantidade por Filial | Total (5 Filiais) |
|--------------------|------------------------------|--------------------------|
| Roteador 2911 | 2 | 10 |
| Switch 3560-24 | 1 | 5 |
| Switch 2960 24TT | 1 | 5 |
| Servidor PT | 1 | 5 |
| PC | 40 | 200 |
| Total | - | 225 |

Fonte: Elaborado pelos autores (2025).

Tabela de Endereçamento IP - Matriz - Uberaba – MG**Tabela 5 - Endereçamento IP - Matriz - Uberaba – MG**

| Dispositivo | Nome | Faixa de Rede | Máscara (CIDR) | Gateway |
|-------------------------|---------------------|----------------------|-----------------------|----------------|
| Roteador WAN | RTR-WAN-MATRIZ | 10.10.0.0/24 | 255.255.255.0 | 10.10.0.1 |
| Firewall | RTR-FW-MATRIZ | 10.10.0.0/24 | 255.255.255.0 | 10.10.0.2 |
| Load Balancer | RTR-LB-MATRIZ | 10.10.0.0/24 | 255.255.255.0 | 10.10.0.3 |
| Switch Core | SW-CORE-MATRIZ | 192.168.0.0/24 | 255.255.255.0 | 192.168.0.1 |
| Servidor DHCP | SRV-DHCP-MATRIZ | 192.168.0.1/24 | 255.255.255.0 | 192.168.0.1 |
| Servidor DNS | SRV-DNS-MATRIZ | 192.168.0.0/24 | 255.255.255.0 | 192.168.0.1 |
| Servidor Web | SRV-WEB-MATRIZ | 192.168.0.0/24 | 255.255.255.0 | 192.168.0.1 |
| Servidor BD | SRV-BD-MATRIZ | 192.168.0.0/24 | 255.255.255.0 | 192.168.0.1 |
| Servidor FTP | SRV-FTP-MATRIZ | 192.168.0.0/24 | 255.255.255.0 | 192.168.0.1 |
| Switch DMZ | SW-DMZ-MATRIZ | 172.16.10.0/27 | 255.255.255.224 | N/A |
| Servidor Web | SRV-WEB-DMZ-MATRIZ | 172.16.10.2/27 | 255.255.255.224 | 172.16.10.1 |
| Servidor Email | SRV-MAIL-DMZ-MATRIZ | 172.16.10.3/27 | 255.255.255.224 | 172.16.10.1 |
| PC TI | PC-TI-MATRIZ-1 | 192.168.10.10/24 | 255.255.255.0 | 192.168.10.1 |
| PC TI | PC-TI-MATRIZ-2 | 192.168.10.11/24 | 255.255.255.0 | 192.168.10.1 |
| PC TI | PC-TI-MATRIZ-3 | 192.168.10.12/24 | 255.255.255.0 | 192.168.10.1 |
| PC Administração | PC-ADMIN-MATRIZ-1 | 192.168.20.10/24 | 255.255.255.0 | 192.168.20.1 |
| PC Administração | PC-ADMIN-MATRIZ-2 | 192.168.20.11/24 | 255.255.255.0 | 192.168.20.1 |
| PC Administração | PC-ADMIN-MATRIZ-3 | 192.168.20.12/24 | 255.255.255.0 | 192.168.20.1 |
| PC Atendimento | PC-ATEND-MATRIZ-1 | 192.168.30.10/24 | 255.255.255.0 | 192.168.30.1 |
| PC Atendimento | PC-ATEND-MATRIZ-2 | 192.168.30.11/24 | 255.255.255.0 | 192.168.30.1 |
| PC Atendimento | PC-ATEND-MATRIZ-3 | 192.168.30.12/24 | 255.255.255.0 | 192.168.30.1 |
| PC Crédito | PC-CRED-MATRIZ-1 | 192.168.40.10/24 | 255.255.255.0 | 192.168.40.1 |
| PC Crédito | PC-CRED-MATRIZ-2 | 192.168.40.11/24 | 255.255.255.0 | 192.168.40.1 |
| PC Crédito | PC-CRED-MATRIZ-3 | 192.168.40.12/24 | 255.255.255.0 | 192.168.40.1 |
| PC Segurança | PC-SEG-MATRIZ-1 | 192.168.50.10/24 | 255.255.255.0 | 192.168.50.1 |
| PC Segurança | PC-SEG-MATRIZ-2 | 192.168.50.11/24 | 255.255.255.0 | 192.168.50.1 |
| PC Segurança | PC-SEG-MATRIZ-3 | 192.168.50.12/24 | 255.255.255.0 | 192.168.50.1 |

| | | | | |
|---------------------|-----------------|------------------|---------------|--------------|
| PC Diretoria | PC-DIR-MATRIZ-1 | 192.168.60.10/24 | 255.255.255.0 | 192.168.60.1 |
| PC Diretoria | PC-DIR-MATRIZ-2 | 192.168.60.11/24 | 255.255.255.0 | 192.168.60.1 |
| PC Diretoria | PC-DIR-MATRIZ-3 | 192.168.60.12/24 | 255.255.255.0 | 192.168.60.1 |

Fonte: Elaborado pelos autores (2025).

Tabela de Endereçamento IP - Filial 1 - Patos de Minas - MG

Tabela 6 - Endereçamento IP - Filial 1 - Patos de Minas - MG

| Dispositivo | Nome | Faixa de Rede | Máscara (CIDR) | Gateway |
|-------------------------|----------------------|----------------------|-----------------------|----------------|
| Roteador WAN | RTR-WAN-FILIAL1 | 10.10.1.0/24 | 255.255.255.0 | 10.10.1.1 |
| Switch Core | SW-CORE-FILIAL1 | 192.168.1.0/24 | 255.255.255.0 | 192.168.1.1 |
| Servidor DHCP | SRV-DHCP-FILIAL1 | 192.168.1.1/24 | 255.255.255.0 | 192.168.2.1 |
| PC TI | PC-TI-FILIAL1-1 | 192.168.11.10/24 | 255.255.255.0 | 192.168.11.1 |
| PC TI | PC-TI-FILIAL1-2 | 192.168.11.11/24 | 255.255.255.0 | 192.168.11.1 |
| PC Administração | PC-ADMIN-FILIAL1--1 | 192.168.21.10/24 | 255.255.255.0 | 192.168.21.1 |
| PC Administração | PC-ADMIN-MFILIAL1--2 | 192.168.21.11/24 | 255.255.255.0 | 192.168.21.1 |
| PC Atendimento | PC-ATEND-FILIAL1-1 | 192.168.31.10/24 | 255.255.255.0 | 192.168.31.1 |
| PC Atendimento | PC-ATEND-FILIAL1-2 | 192.168.31.11/24 | 255.255.255.0 | 192.168.31.1 |
| PC Crédito | PC-CRED-FILIAL1-1 | 192.168.41.10/24 | 255.255.255.0 | 192.168.41.1 |
| PC Crédito | PC-CRED-FILIAL1-2 | 192.168.41.11/24 | 255.255.255.0 | 192.168.41.1 |
| PC Segurança | PC-SEG-FILIAL1-1 | 192.168.51.10/24 | 255.255.255.0 | 192.168.51.1 |
| PC Segurança | PC-SEG-FILIAL1-2 | 192.168.51.11/24 | 255.255.255.0 | 192.168.51.1 |

Fonte: Elaborado pelos autores (2025).

Tabela de Endereçamento IP - Filial 2 - Poços de Caldas – MG

Tabela 7 - Endereçamento IP - Filial 2 - Poços de Caldas - MG

| Dispositivo | Nome | Faixa de Rede | Máscara (CIDR) | Gateway |
|-------------------------|---------------------|----------------------|-----------------------|----------------|
| Roteador WAN | RTR-WAN-FILIAL2 | 10.10.2.0/24 | 255.255.255.0 | 10.10.2.1 |
| Switch Core | SW-CORE-FILIAL2 | 192.168.2.0/24 | 255.255.255.0 | 192.168.2.1 |
| Servidor DHCP | SRV-DHCP-FILIAL2 | 192.168.2.1/24 | 255.255.255.0 | 192.168.2.1 |
| PC TI | PC-TI-FILIAL2-1 | 192.168.12.10/24 | 255.255.255.0 | 192.168.12.1 |
| PC TI | PC-TI-FILIAL2-2 | 192.168.12.11/24 | 255.255.255.0 | 192.168.12.1 |
| PC Administração | PC-ADMIN-FILIAL2-1 | 192.168.22.10/24 | 255.255.255.0 | 192.168.22.1 |
| PC Administração | PC-ADMIN-MFILIAL2-2 | 192.168.22.11/24 | 255.255.255.0 | 192.168.22.1 |
| PC Atendimento | PC-ATEND-FILIAL2-1 | 192.168.32.10/24 | 255.255.255.0 | 192.168.32.1 |
| PC Atendimento | PC-ATEND-FILIAL2-2 | 192.168.32.11/24 | 255.255.255.0 | 192.168.32.1 |
| PC Crédito | PC-CRED-FILIAL2-1 | 192.168.42.10/24 | 255.255.255.0 | 192.168.42.1 |
| PC Crédito | PC-CRED-FILIAL2-2 | 192.168.42.11/24 | 255.255.255.0 | 192.168.42.1 |
| PC Segurança | PC-SEG-FILIAL2-1 | 192.168.52.10/24 | 255.255.255.0 | 192.168.52.1 |
| PC Segurança | PC-SEG-FILIAL2-2 | 192.168.52.11/24 | 255.255.255.0 | 192.168.52.1 |

Fonte: Elaborado pelos autores (2025).

Tabela de Endereçamento IP - Filial 3 - Montes Claros - MG

Tabela 8 - Endereçamento IP - Filial 3 - Montes Claros - MG

| Dispositivo | Nome | Faixa de Rede | Máscara (CIDR) | Gateway |
|------------------|---------------------|------------------|----------------|--------------|
| Roteador WAN | RTR-WAN-FILIAL3 | 10.10.3.0/24 | 255.255.255.0 | 10.10.3.1 |
| Switch Core | SW-CORE-FILIAL3 | 192.168.3.0/24 | 255.255.255.0 | 192.168.3.1 |
| Servidor DHCP | SRV-DHCP-FILIAL3 | 192.168.3.1/24 | 255.255.255.0 | 192.168.3.1 |
| PC TI | PC-TI-FILIAL3-1 | 192.168.13.10/24 | 255.255.255.0 | 192.168.13.1 |
| PC TI | PC-TI-FILIAL3-2 | 192.168.13.11/24 | 255.255.255.0 | 192.168.13.1 |
| PC Administração | PC-ADMIN-FILIAL3-1 | 192.168.23.10/24 | 255.255.255.0 | 192.168.23.1 |
| PC Administração | PC-ADMIN-MFILIAL3-2 | 192.168.23.11/24 | 255.255.255.0 | 192.168.23.1 |
| PC Atendimento | PC-ATEND-FILIAL3-1 | 192.168.33.10/24 | 255.255.255.0 | 192.168.33.1 |
| PC Atendimento | PC-ATEND-FILIAL3-2 | 192.168.33.11/24 | 255.255.255.0 | 192.168.33.1 |
| PC Crédito | PC-CRED-FILIAL3-1 | 192.168.43.10/24 | 255.255.255.0 | 192.168.43.1 |
| PC Crédito | PC-CRED-FILIAL3-2 | 192.168.43.11/24 | 255.255.255.0 | 192.168.43.1 |
| PC Segurança | PC-SEG-FILIAL3-1 | 192.168.53.10/24 | 255.255.255.0 | 192.168.53.1 |
| PC Segurança | PC-SEG-FILIAL3-2 | 192.168.53.11/24 | 255.255.255.0 | 192.168.53.1 |

Fonte: Elaborado pelos autores (2025).

Tabela de Endereçamento IP - Filial 4 Governador Valadares - MG

Tabela 9 - Endereçamento IP - Filial 4 - Governador Valadares - MG

| Dispositivo | Nome | Faixa de Rede | Máscara (CIDR) | Gateway |
|------------------|---------------------|------------------|----------------|--------------|
| Roteador WAN | RTR-WAN-FILIAL4 | 10.10.4.0/24 | 255.255.255.0 | 10.10.4.1 |
| Switch Core | SW-CORE-FILIAL4 | 192.168.4.0/24 | 255.255.255.0 | 192.168.4.1 |
| Servidor DHCP | SRV-DHCP-FILIAL4 | 192.168.4.1/24 | 255.255.255.0 | 192.168.4.1 |
| PC TI | PC-TI-FILIAL4-1 | 192.168.14.10/24 | 255.255.255.0 | 192.168.14.1 |
| PC TI | PC-TI-FILIAL4-2 | 192.168.14.11/24 | 255.255.255.0 | 192.168.14.1 |
| PC Administração | PC-ADMIN-FILIAL4-1 | 192.168.24.10/24 | 255.255.255.0 | 192.168.24.1 |
| PC Administração | PC-ADMIN-MFILIAL4-2 | 192.168.24.11/24 | 255.255.255.0 | 192.168.24.1 |
| PC Atendimento | PC-ATEND-FILIAL4-1 | 192.168.34.10/24 | 255.255.255.0 | 192.168.34.1 |
| PC Atendimento | PC-ATEND-FILIAL4-2 | 192.168.34.11/24 | 255.255.255.0 | 192.168.34.1 |
| PC Crédito | PC-CRED-FILIAL4-1 | 192.168.44.10/24 | 255.255.255.0 | 192.168.44.1 |
| PC Crédito | PC-CRED-FILIAL4-2 | 192.168.44.11/24 | 255.255.255.0 | 192.168.44.1 |
| PC Segurança | PC-SEG-FILIAL4-1 | 192.168.54.10/24 | 255.255.255.0 | 192.168.54.1 |
| PC Segurança | PC-SEG-FILIAL4-2 | 192.168.54.11/24 | 255.255.255.0 | 192.168.54.1 |

Fonte: Elaborado pelos autores (2025).

Tabela de Endereçamento IP - Filial 5 Sete Lagoas - MG

Tabela 10 - Endereçamento IP - Filial 5 - Sete Lagoas - MG

| Dispositivo | Nome | Faixa de Rede | Máscara (CIDR) | Gateway |
|-------------------------|---------------------|----------------------|-----------------------|----------------|
| Roteador WAN | RTR-WAN-FILIAL5 | 10.10.5.0/24 | 255.255.255.0 | 10.10.5.1 |
| Switch Core | SW-CORE-FILIAL5 | 192.168.5.0/24 | 255.255.255.0 | 192.168.5.1 |
| Servidor DHCP | SRV-DHCP-FILIAL5 | 192.168.5.1/24 | 255.255.255.0 | 192.168.5.1 |
| PC TI | PC-TI-FILIAL5-1 | 192.168.15.10/24 | 255.255.255.0 | 192.168.15.1 |
| PC TI | PC-TI-FILIAL5-2 | 192.168.15.11/24 | 255.255.255.0 | 192.168.15.1 |
| PC Administração | PC-ADMIN-FILIAL5-1 | 192.168.25.10/24 | 255.255.255.0 | 192.168.25.1 |
| PC Administração | PC-ADMIN-MFILIAL5-2 | 192.168.25.11/24 | 255.255.255.0 | 192.168.25.1 |
| PC Atendimento | PC-ATEND-FILIAL5-1 | 192.168.35.10/24 | 255.255.255.0 | 192.168.35.1 |
| PC Atendimento | PC-ATEND-FILIAL5-2 | 192.168.35.11/24 | 255.255.255.0 | 192.168.35.1 |
| PC Crédito | PC-CRED-FILIAL5-1 | 192.168.45.10/24 | 255.255.255.0 | 192.168.45.1 |
| PC Crédito | PC-CRED-FILIAL5-2 | 192.168.45.11/24 | 255.255.255.0 | 192.168.45.1 |
| PC Segurança | PC-SEG-FILIAL5-1 | 192.168.55.10/24 | 255.255.255.0 | 192.168.55.1 |
| PC Segurança | PC-SEG-FILIAL5-2 | 192.168.55.11/24 | 255.255.255.0 | 192.168.55.1 |

Fonte: Elaborado pelos autores (2025).

1.11 Serviços de Rede Implementados

- **Firewall:** Controle de acessos entre as unidades.
- **VPN/MPLS:** Comunicação segura entre as unidades.
- **DHCP:** Distribuição dinâmica de IPs.
- **Wi-Fi:** Implementação de redes sem fio segmentadas para uso interno e de convidados, com autenticação segura e políticas de controle de acesso.
- **DNS:** Resolução de nomes na rede.
- **NAT:** Tradução de endereços para acesso externo.
- **VoIP:** Chamadas de voz entre dispositivos na rede e atendimento aos clientes.
- **Banco de Dados:** Servidor de banco de dados para armazenamento de informações.
- **FTP:** Servidor para registro de arquivos.
- **NFS:** Compartilhamento de dados entre sistemas da rede e implementação de backup.

Segurança e Compliance

- **Serviço de Controle de Acesso:** Implementação de políticas de RBAC e MFA para controlar o acesso aos sistemas de dados críticos, como o banco de dados, servidores de e-mail e servidores web.
- **Segurança da Rede Wi-Fi:** Configuração de redes separadas para colaboradores e convidados, uso de VLANs para segmentação de tráfego, autenticação WPA3 e controle de acesso baseado em MAC ou portal cativo para usuários convidados.

- **Monitoramento do Sistema de Rede:** Coleta de dados de desempenho e detecção de anomalias para garantir a integridade e eficiência da infraestrutura.
- **Ferramentas de Auditoria e Segurança:** Implementação de ferramentas para monitoramento contínuo da segurança e compliance da rede.

Planos de Backup

- Backup Diário para dados críticos (banco de dados e arquivos) e Backup Semanal Completo.
- Backup Incremental diário, copiando apenas dados alterados.
- Armazenamento em nuvem e servidores dedicados para maior segurança.
- Criptografia dos backups e redundância para proteção contra falhas.

Plano de Recuperação de Desastres

- **Redundância de Hardware:** Equipamentos críticos como servidores de banco de dados, roteadores e switches terão backup em caso de falha.
- **Failover Automático:** Para garantir continuidade de serviços em caso de falhas de hardware.
- **Procedimentos de Restauração:** Bem documentados e testes regulares para garantir a eficiência da recuperação.
- **Plano de Comunicação:** Para notificação rápida e ações imediatas em caso de falha.

2 VIRTUALBOX E CLOUD COMPUTING

2.1 On premises

Demonstração: Configuração do servidor DHCP e DNS no VirtualBox - Etapa 2 - CoopCred
<https://www.youtube.com/watch?v=W7aocVNanKU>

Virtualização com VirtualBox – Windows Server

Nesta etapa, utilizamos o VirtualBox para simular um ambiente local de rede corporativa utilizando o sistema Windows Server. A Figura 2 apresenta as instâncias das máquinas virtuais criadas: um servidor responsável pelo DHCP e DNS, e duas máquinas representando os clientes da rede de TI e Administração.

Servidor DHCP

Figura 2 – VM VirtualBox Manager



Fonte: VM VirtualBox (Oracle, 2025)

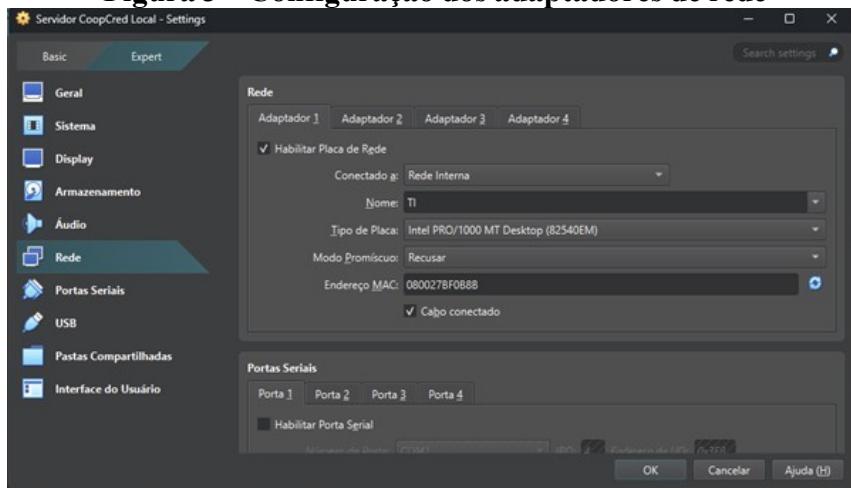
Distribuição de IP via DHCP

Foi configurado um escopo de DHCP no Windows Server para fornecer endereçamento IP automático às máquinas virtuais da rede interna. Essa configuração permite:

- Definir uma faixa de IPs (ver Tabela 2);
- Atribuir automaticamente a máscara de sub-rede;
- Definir o gateway padrão;
- Fornecer o servidor DNS de forma automática.

A Figura 3 exibe a tela em que foram configurados os adaptadores de rede utilizados na topologia.

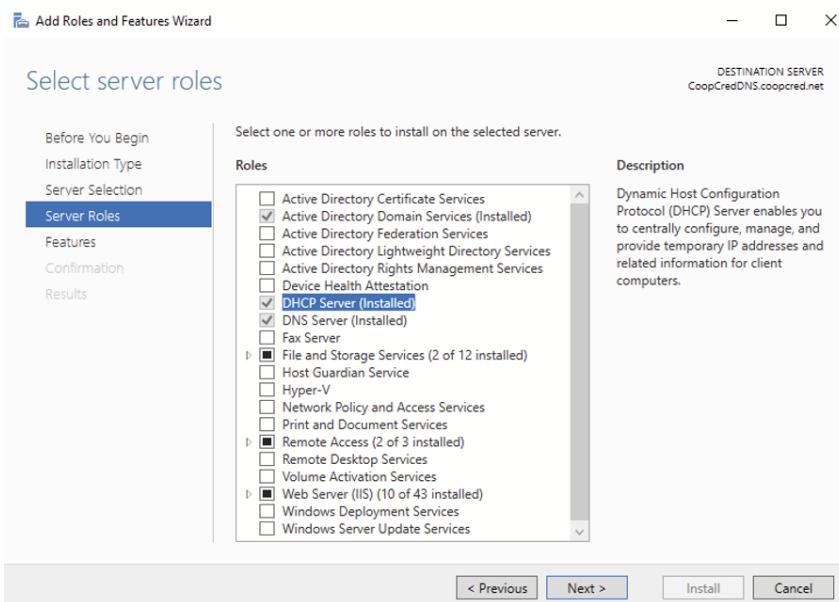
Figura 3 – Configuração dos adaptadores de rede



Fonte: VM VirtualBox (Oracle, 2025)

Em seguida, foi adicionada a função de servidor DHCP à instância do Windows Server, como ilustrado na Figura 4.

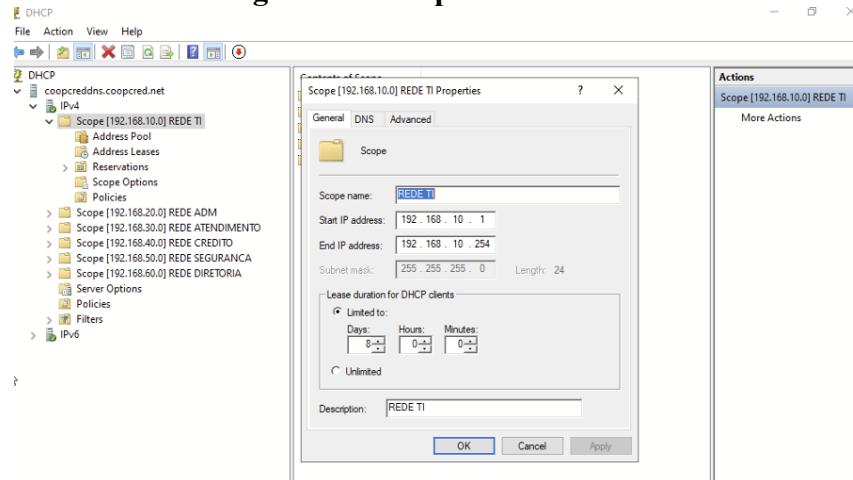
Figura 4 – Adição da role do DHCP



Fonte: VM VirtualBox (Oracle, 2025)

Após a instalação, foram criados os escopos de rede com a faixa de IPs que serão atribuídos automaticamente, conforme apresentado na Figura 5.

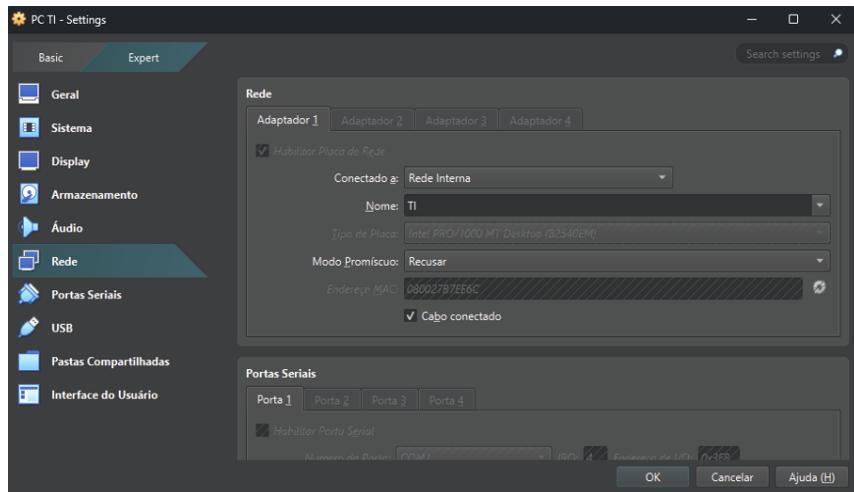
Figura 5 – Escopo de faixa de IP



Fonte: VM VirtualBox (Oracle, 2025)

Na máquina cliente, é realizada a seleção do adaptador de rede a ser utilizado, como mostrado na Figura 6.

Figura 6 – Seleção do adaptador de rede utilizado



Fonte: VM VirtualBox (Oracle, 2025)

Após a seleção do adaptador, dentro da instância é possível utilizar o comando *ping* para validar a atribuição de IP pelo servidor DHCP, conforme mostra a Figura 7.

Figura 7 – Atribuição do IP via servidor DHCP para máquina cliente

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vinci>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : coopcred.net
  Link-local IPv6 Address . . . . . : fe80::d46f:eb8b:45c:b991%15
  IPv4 Address. . . . . : 192.168.10.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.10.1

C:\Users\vinci>
```

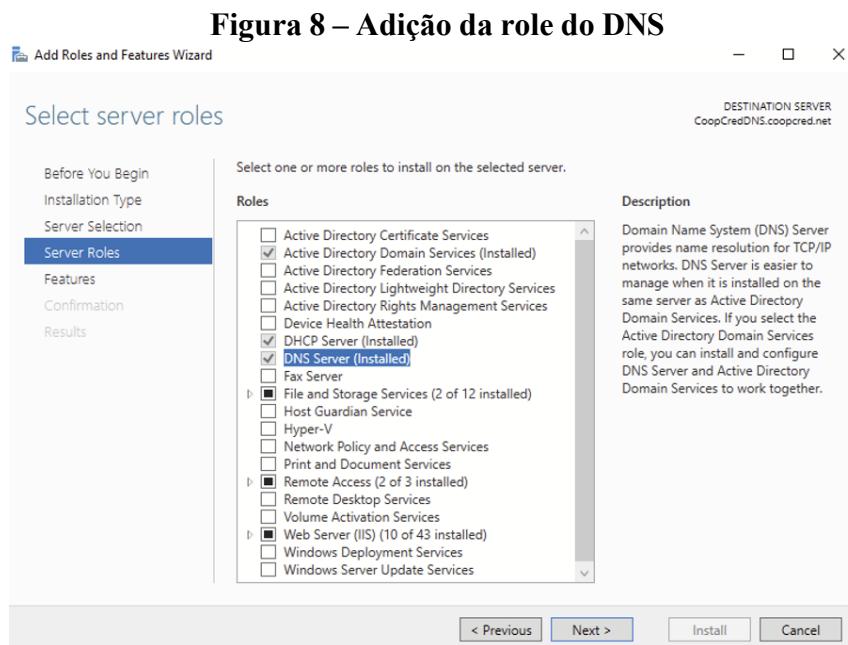
Fonte: VM VirtualBox (Oracle, 2025)

Servidor DNS

Configuração de DNS Integrado ao AD

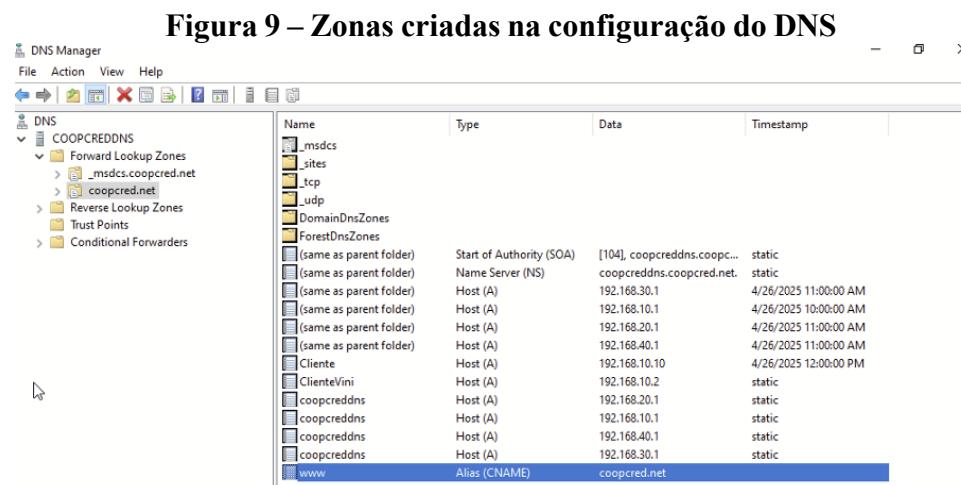
O servidor DNS foi instalado e configurado para trabalhar em conjunto com o Active Directory (AD), permitindo:

- Resolução de nomes dentro da rede interna;
- Configuração de forwarders para resolução de nomes externos;
- Integração com as Políticas de Grupo (GPO) para apontar automaticamente o DNS do servidor às estações.



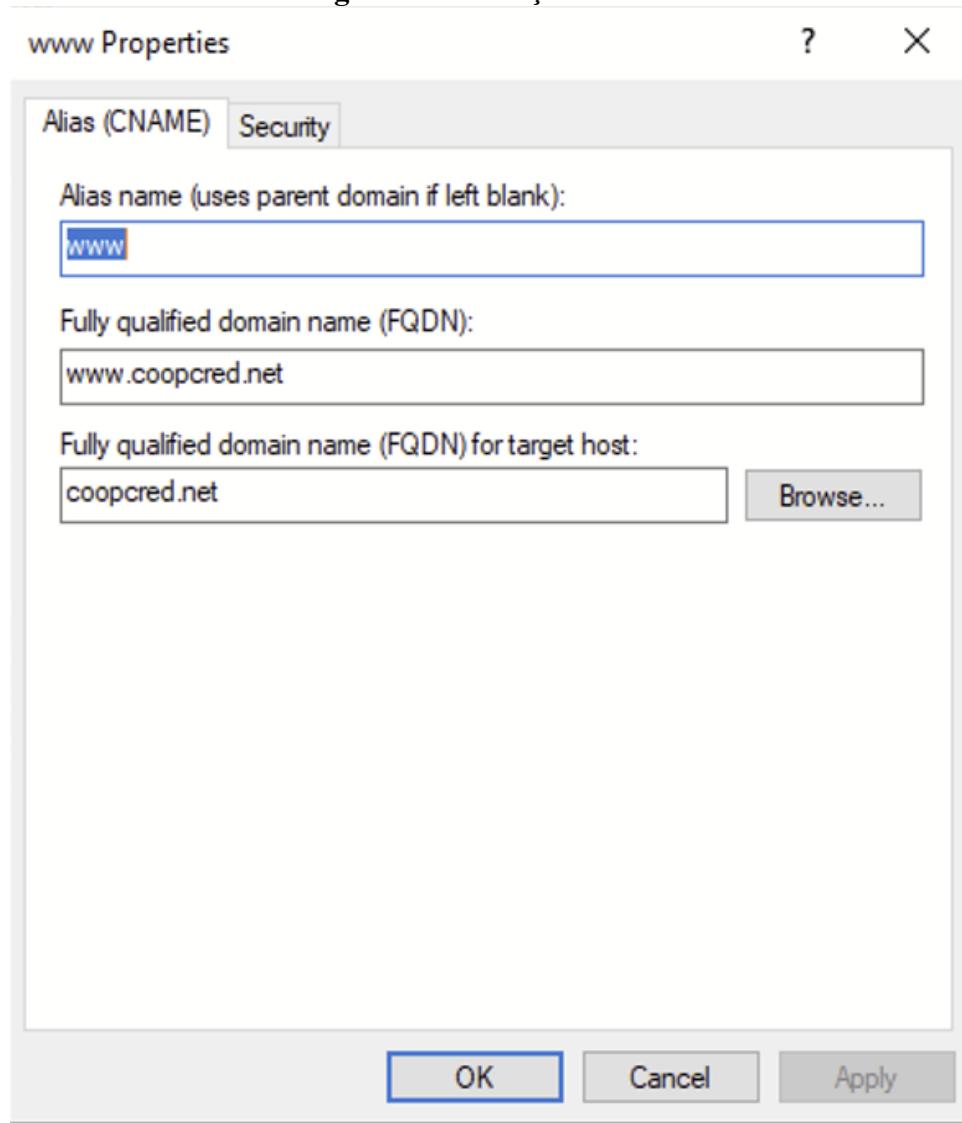
Fonte: VM VirtualBox (Oracle, 2025)

Nas Figuras 9 e 10 está sendo configurado o domínio coopcred.net e atribuindo o alias www.coopcred.net.



Fonte: VM VirtualBox (Oracle, 2025)

Figura 10 – Criação do Alias



Fonte: VM VirtualBox (Oracle, 2025)

Na figura 11 é exibido o resultado de um ping para o dns criado.

Figura 11 – Execução do ping para www.coopcred.net

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\coopcred>ping www.coopcred.net

Pinging coopcred.net [192.168.30.1] with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\coopcred>
```

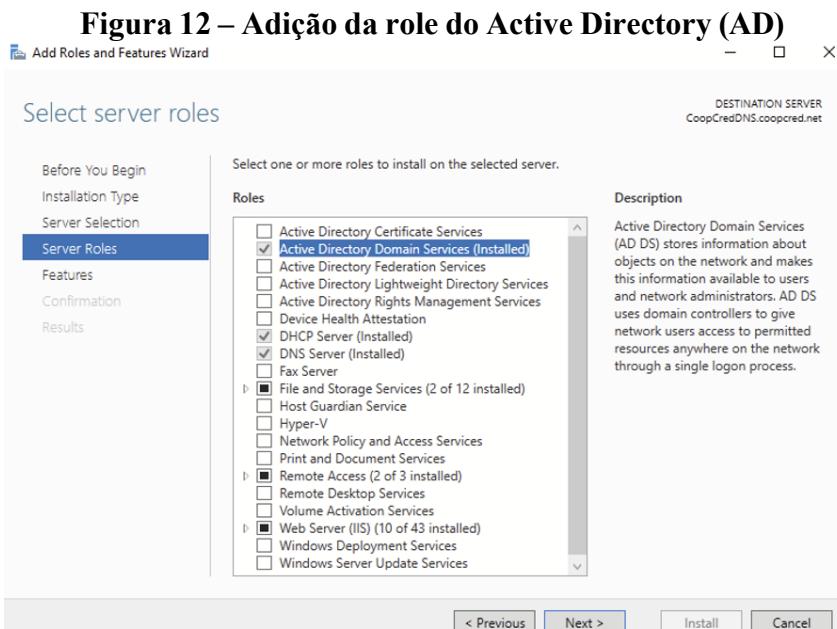
Fonte: VM VirtualBox (Oracle, 2025)

ACTIVE DIRECTORY

Configuração do Active Directory (AD) e Políticas de Grupo (GPO)

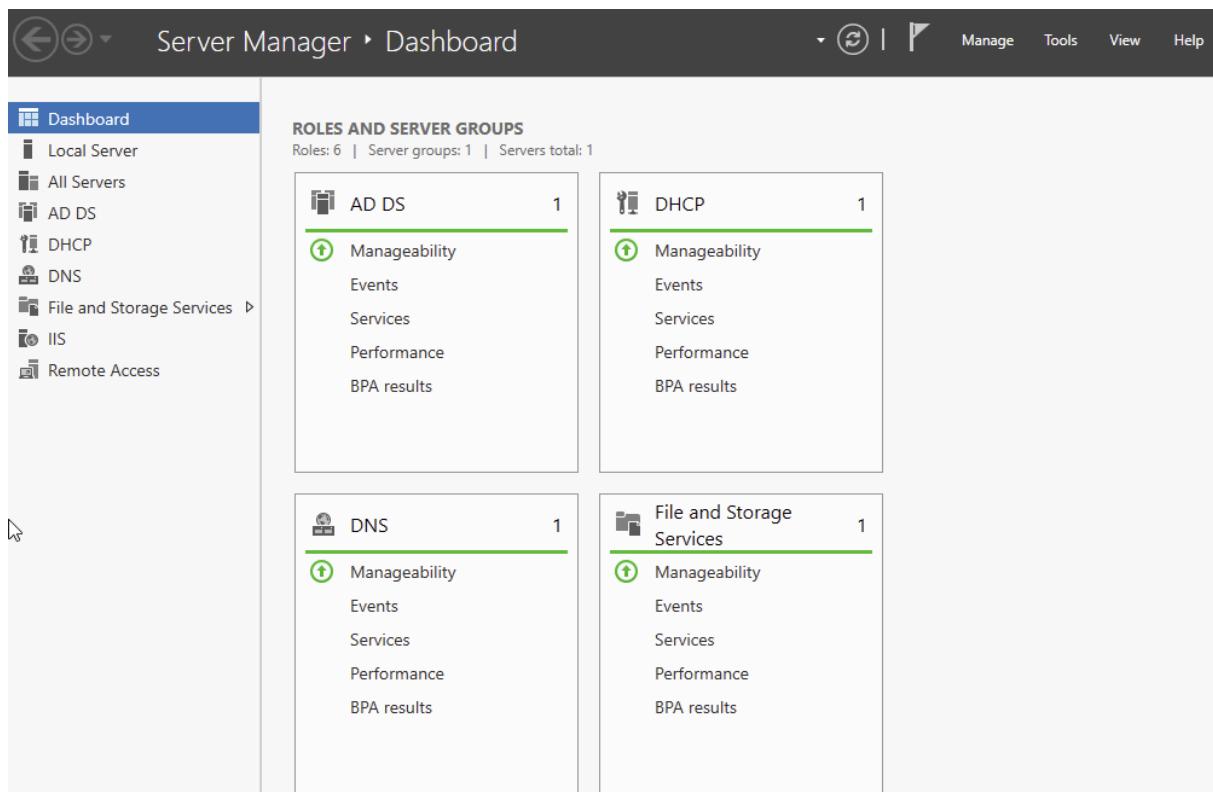
- Criação de domínio para gerenciamento centralizado da rede (coopcred.net);
- Inclusão de usuários e grupos organizacionais (TI, Administração, Atendimento, Crédito, Segurança, Diretoria);
- Aplicação de GPOs para controle de desktop, políticas de senha, acesso a dispositivos e restrições específicas por grupo.

Para a configuração do Active Directory é adicionada a role necessária para o serviço, assim como mostra a Figura 12.



Fonte: VM VirtualBox (Oracle, 2025)

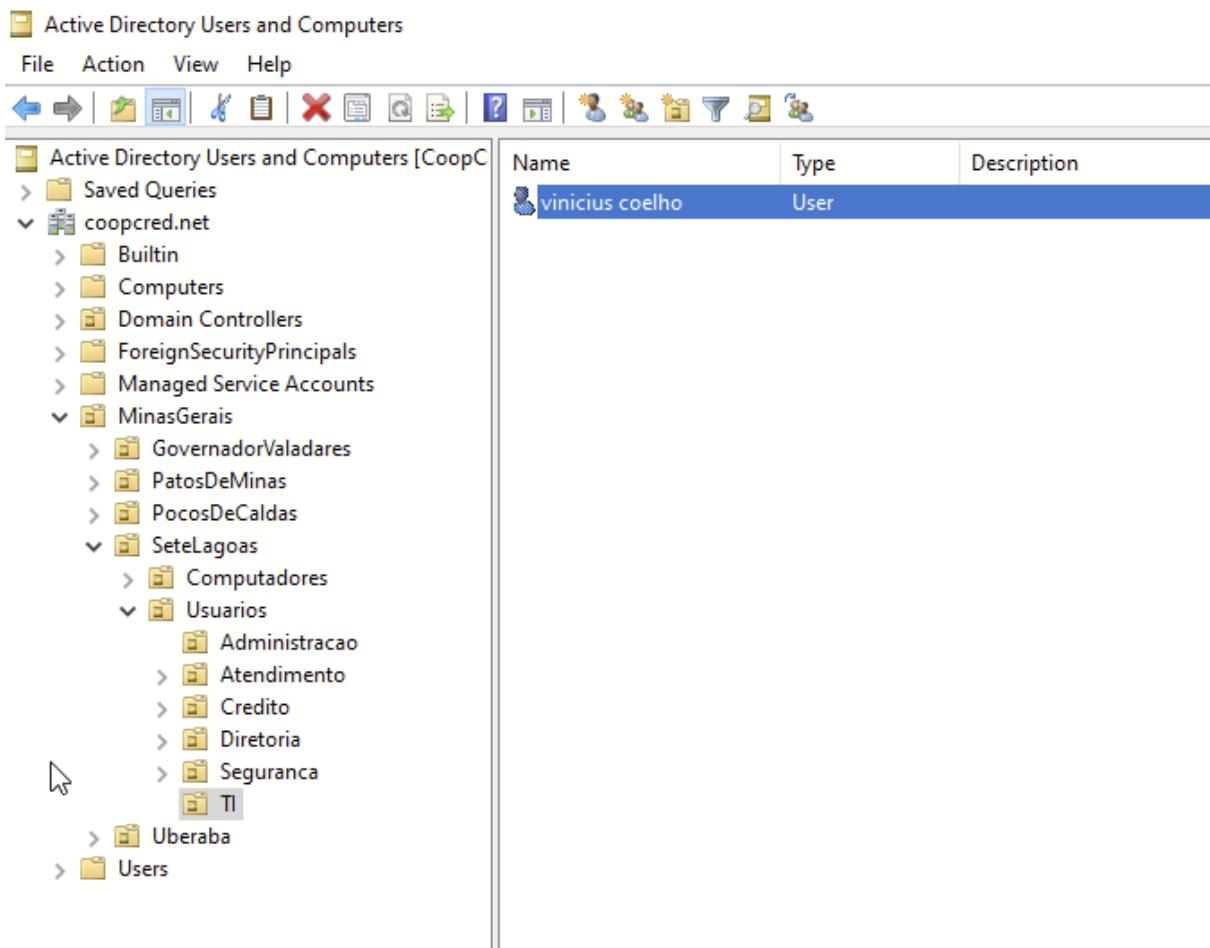
Figura 13 - Serviços instalados de AD, DNS, DHCP no Windows Server



Fonte: VM VirtualBox (Oracle, 2025)

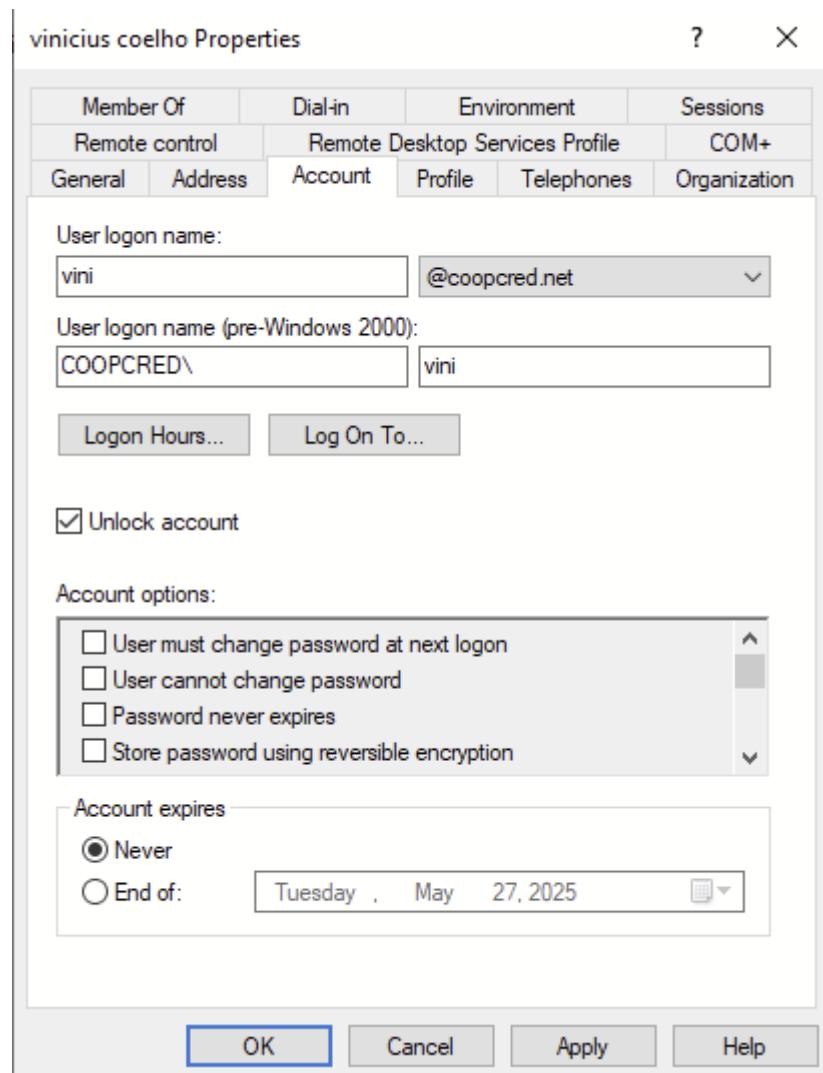
Na Figura 14 é apresentada a estrutura de unidades organizacionais e objetos no Active Directory para o domínio coopcred.net. E na Figura 15, verificamos a criação de um usuário. Em seguida, podemos identificar que há um computador logado com o nome de Cliente, conforme mostra a Figura 16.

Figura 14 - Containers com a estrutura da cooperativa de crédito CoopCred



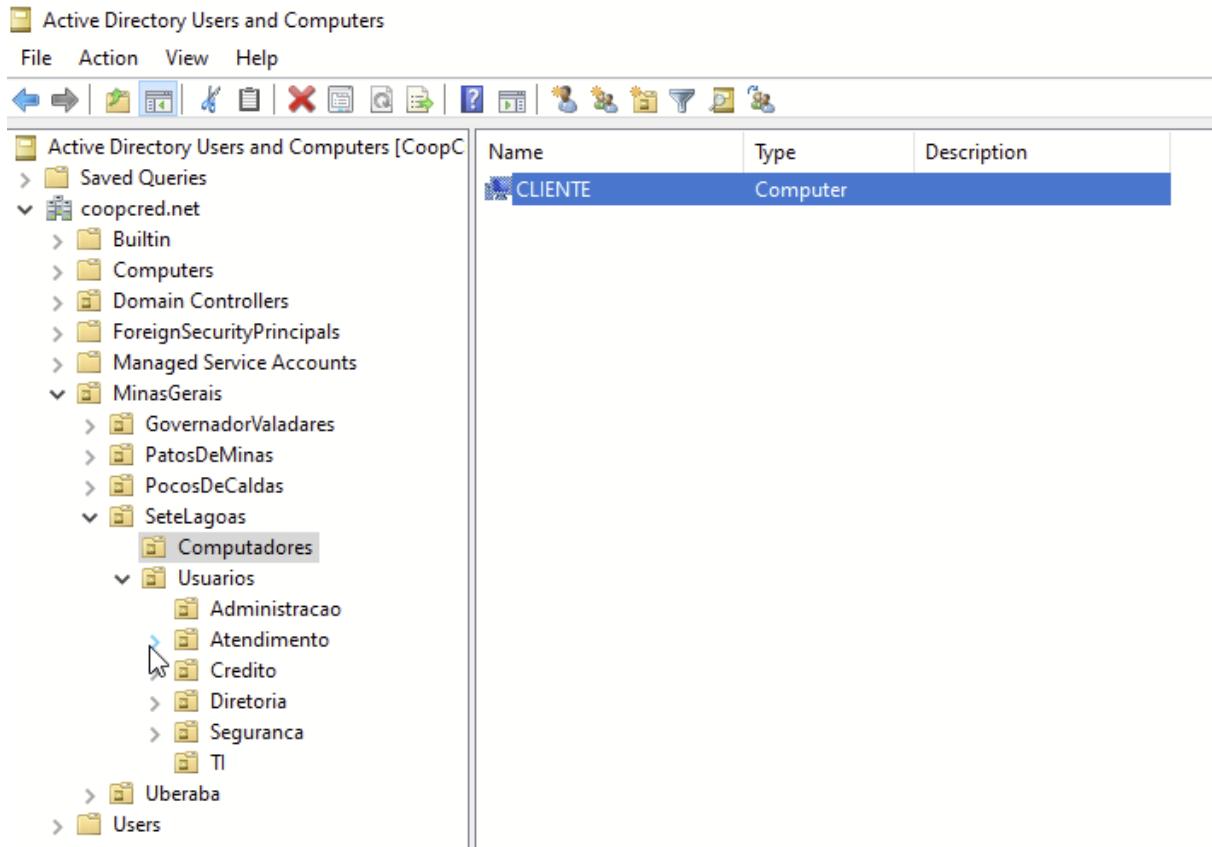
Fonte: VM VirtualBox (Oracle, 2025)

Figura 15 - Criação de conta de usuário e email



Fonte: VM VirtualBox (Oracle, 2025)

Figura 16 - Máquina cliente logada na máquina servidor



Fonte: VM VirtualBox (Oracle, 2025)

No servidor, é realizado o ping para a máquina de cliente para validação da comunicação entre as partes, isso é visto na Figura 17. E o contrário também é realizado, sendo feito um ping da máquina do cliente para o servidor, conforme mostra a Figura 18.

Figura 17 - Execução ping servidor para máquina cliente

```
cmd Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\coopcred>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=5ms TTL=128
Reply from 192.168.10.10: bytes=32 time=6ms TTL=128
Reply from 192.168.10.10: bytes=32 time=2ms TTL=128
Reply from 192.168.10.10: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\Users\coopcred>
```

Fonte: VM VirtualBox (Oracle, 2025)

Figura 18 - Execução ping da máquina cliente para servidor

```
C:\Users\vini>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=23ms TTL=128
Reply from 192.168.10.1: bytes=32 time=4ms TTL=128
Reply from 192.168.10.1: bytes=32 time=2ms TTL=128
Reply from 192.168.10.1: bytes=32 time=34ms TTL=128

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 34ms, Average = 15ms

C:\Users\vini>
```

Fonte: VM VirtualBox (Oracle, 2025)

Configurações de Group Policy Object (GPO):

Por fim, com base na estrutura organizacional da rede, foram criadas as políticas de grupo, um exemplo dessa é exibido nas Figura 19, Figura 20 e Figura 21.

Figura 19 - Configuração do GPO para políticas de usuário

The screenshot shows the 'Control Panel' policy settings under 'User Configuration'. The 'Prohibit access to Control Panel and PC settings' policy is selected, with its details displayed. The 'Setting' column lists various options like 'Add or Remove Programs', 'Display', etc., each with a 'State' and 'Comment' column. One setting, 'Prohibit access to Control Panel and PC settings', is highlighted as 'Enabled' with a comment 'Bloqueo do painel de controle'.

| Setting | State | Comment |
|--|----------------|--------------------------------------|
| Add or Remove Programs | Not configured | No |
| Display | Not configured | No |
| Personalization | Not configured | No |
| Printers | Not configured | No |
| Programs | Not configured | No |
| Regional and Language Options | Not configured | No |
| Hide specified Control Panel items | Not configured | No |
| Always open All Control Panel items when opening Control ... | Not configured | No |
| Prohibit access to Control Panel and PC settings | Enabled | Bloqueo do painel de controle |
| Show only specified Control Panel items | Not configured | No |
| Settings Page Visibility | Not configured | No |

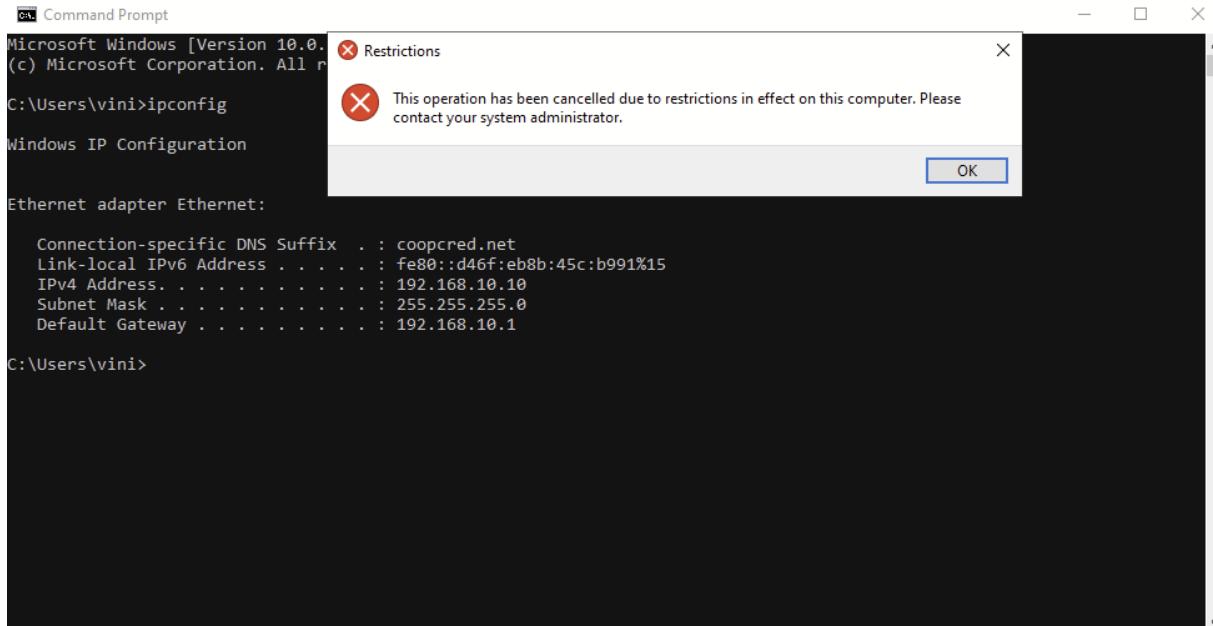
Fonte: VM VirtualBox (Oracle, 2025)

Figura 20- Tela de informações da política GPO para o usuário de TI

The screenshot shows the 'gpoli' GPO details page. It includes sections for 'Links' (with one link to 'TI'), 'Security Filtering' (applying to 'NT AUTHORITY\Authenticated Users'), and 'Delegation' (listing permissions for various security principals). The 'Computer Configuration' and 'User Configuration' tabs are also visible at the bottom.

Fonte: VM VirtualBox (Oracle, 2025)

Figura 21 - Mensagem bloqueio de painel de controle pelo GPO



Fonte: VM VirtualBox (Oracle, 2025)

2.2 On cloud - Ambientes em Nuvem (AWS)

∅ Demonstração: [Serviços AWS - Etapa 2 - CoopCred.mp4](#)

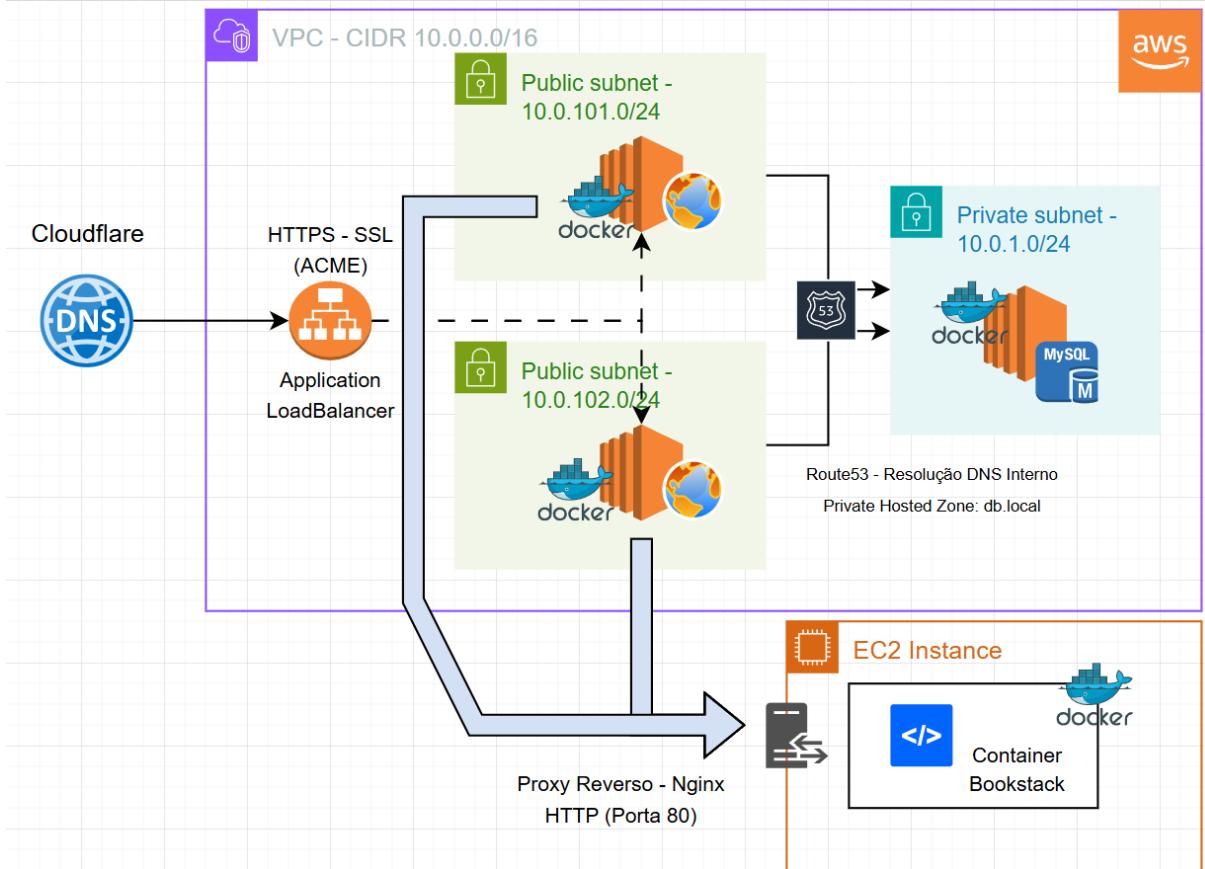
https://drive.google.com/file/d/17X_xe7xSr5GN_TKDaL4blsyJ0giir7tw/view?usp=sharing

Computação em Nuvem com AWS

O ambiente de nuvem foi construído utilizando serviços da Amazon Web Services (AWS), com foco em alta disponibilidade, segurança e escalabilidade.

Diagrama de Arquitetura da AWS

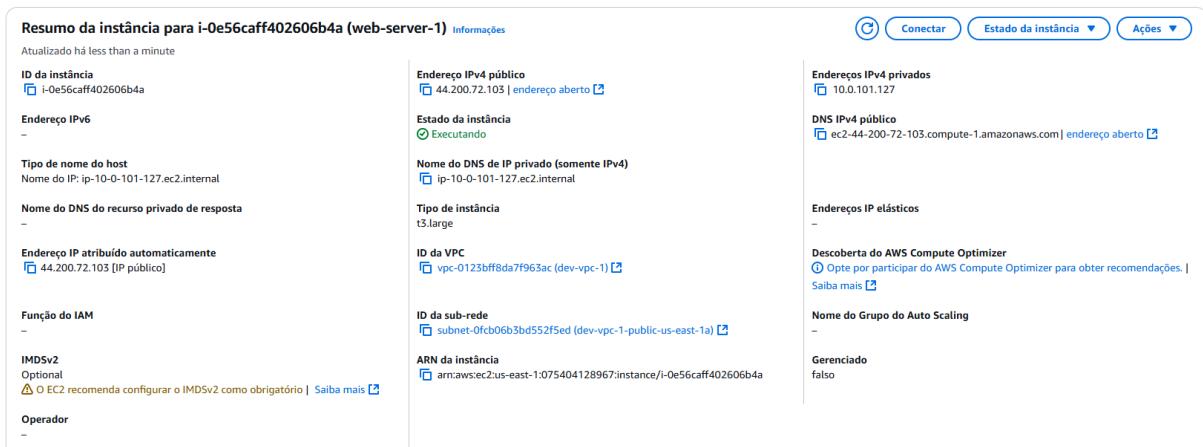
Figura 22 - Diagrama do Ambiente AWS



Fonte: Elaborado pelos autores (2025).

O diagrama acima ilustra a topologia da rede na AWS, mostrando como os recursos estão conectados e distribuídos entre as diferentes zonas de disponibilidade e sub-redes.

Figura 23 - EC2 do web-server-1



Fonte: AWS (2025).

Figura 24 - EC2 do web-server-1 - Detalhes

| Detalhes | Status e alarmes | Monitoramento | Segurança | Redes | Armazenamento | Tags |
|---|---|---|-----------|-------|---------------|------|
| ▼ Detalhes da instância <small>Informações</small> | | | | | | |
| ID da AMI ami-04b4f1a9cf54c11d0 | Monitoramento desativado | Detalhes da plataforma Linux/UNIX | | | | |
| Nome da AMI ubuntu/images/hvm-ssd/gp3/ubuntu-noble-24.04-amd64-server-20250115 | Imagen permitida - | Proteção contra encerramento Desabilitado | | | | |
| Interromper proteção Desabilitado | Data de lançamento Sat May 17 2025 10:22:21 GMT-0300 (Horário Padrão de Brasília) (36 minutos) | Local da AMI amazon/ubuntu/images/hvm-ssd/gp3/ubuntu-noble-24.04-amd64-server-20250115 | | | | |
| Recuperação automática de instância Padrão | Ciclo de vida normal | Interromper - Comportamento de hibernação Desabilitado | | | | |
| Índice de execução de AMIs 0 | Par de chaves atribuído na execução coopcred-new | Motivo de transição de estado - | | | | |
| Especificação de crédito standard | ID de kernel - | Mensagem de transição de estado - | | | | |
| Operação de uso RunInstances | ID do disco RAM - | Proprietário 075404128967 | | | | |
| Suporte a enclave Desabilitado | Modo de inicialização uefi-preferred | Modo de inicialização da instância atual uefi | | | | |
| Permitir tags nos metadados da instância Desabilitado | Usar RBN como nome de host do sistema operacional convidado Desabilitado | Responder IPv4 do nome de host DNS de RBN Desabilitado | | | | |
| ▼ Host e grupo de posicionamento <small>Informações</small> | | | | | | |
| ID do host - | Afinidade - | Grupo de posicionamento - | | | | |
| Nome do grupo de recursos do host - | Locação default | ID do grupo de posicionamento - | | | | |
| Tipo de virtualização hvm | Reserva r-03501a1dd1dd1e8c | Número de partição - | | | | |
| Número de vCPUs 2 | | | | | | |
| ▼ Reserva de capacidade <small>Informações</small> | | | | | | |
| ID da reserva de capacidade - | Configuração de reserva de capacidade open | | | | | |

Fonte: AWS (2025).

Figura 25 - EC2 do web-server-1 - Segurança

| Detalhes | Status e alarmes | Monitoramento | Segurança | Redes | Armazenamento | Tags |
|--|--|--|-----------|-----------|---|----------------------------|
| ▼ Detalhes de segurança | | | | | | |
| Função do IAM - | ID do proprietário 075404128967 | Data de lançamento Sat May 17 2025 10:22:21 GMT-0300 (Horário Padrão de Brasília) | | | | |
| Grupos de segurança sg-0b4cf5463bb3e1892 (web-sg) | | | | | | |
| ▼ Regras de entrada | | | | | | |
| Nome | ID da regra do grupo de ... | Intervalo de p... | Protocolo | Origem | Grupos de segurança | Descrição |
| - | 2 IDs | 22 | TCP | 0.0.0.0/0 | web-sg web-sg | SSH port |
| - | 2 IDs | 10050 | TCP | 0.0.0.0/0 | web-sg web-sg | - |
| - | 2 IDs | 80 | TCP | 0.0.0.0/0 | web-sg web-sg | HTTP |
| - | 2 IDs | 12000 - 12100 | TCP | 0.0.0.0/0 | web-sg web-sg | - |
| - | 2 IDs | 20 - 21 | TCP | 0.0.0.0/0 | web-sg web-sg | - |
| - | 2 IDs | Todos | Todos | 0.0.0.0/0 | web-sg web-sg | - |
| - | 2 IDs | 443 | TCP | 0.0.0.0/0 | web-sg web-sg | HTTPS |
| ▼ Regras de saída | | | | | | |
| Nome | ID da regra do grupo de ... | Intervalo de p... | Protocolo | Destino | Grupos de segurança | Descrição |
| - | 2 IDs | Todos | Todos | 0.0.0.0/0 | web-sg web-sg | Allow all outbound traffic |

Fonte: AWS (2025).

Figura 26 - EC2 do web-server-2

The screenshot displays the AWS CloudWatch Metrics interface for an EC2 instance named 'web-server-2'. The top navigation bar includes 'Conectar', 'Estado da instância', and 'Ações'. The main content area is titled 'Resumo da instância para i-0b6f6cd8e05f952f8 (web-server-2)'. It lists several sections with detailed information:

- Endereço IP:** i-0b6f6cd8e05f952f8
- Endereço IPv6:** –
- Tipo de nome do host:** Nome do IP: ip-10-0-101-22.ec2.internal
- Nome do DNS do recurso privado de resposta:** –
- Endereço IP atribuído automaticamente:** –
- Função do IAM:** –
- IMDSv2:** Optional. ⚠️ EC2 recomenda configurar o IMDSv2 como obrigatório | Saiba mais
- Operador:** –
- Endereço IPv4 público:** 44.200.125.230 | endereço aberto
- Estado da instância:** Executando
- Nome do DNS de IP privado (somente IPv4):** ip-10-0-101-22.ec2.internal
- Tipo de Instância:** t2.micro
- ID da VPC:** vpc-0123bfff8da7f963ac (dev-vpc-1)
- ID da sub-rede:** subnet-0fc06b3bd552f5ed (dev-vpc-1-public-us-east-1a)
- ARN da instância:** arn:aws:ec2:us-east-1:075404128967:instance/i-0b6f6cd8e05f952f8
- Endereços IP elásticos:** –
- Descoberta do AWS Compute Optimizer:** –
- Nome do Grupo do Auto Scaling:** –
- Gerenciado:** falso

Fonte: AWS (2025).

Figura 27 - EC2 do web-server-2 - Detalhes

The screenshot shows the 'Detalhes' tab of the AWS EC2 instance configuration page for 'web-server-2'. The page is divided into several sections:

- Detalhes da instância:**
 - ID da AMI:** ami-04b4f1a9cf54c11d0
 - Nome da AMI:** ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd64-server-20250115
 - Interromper proteção:** Desabilitado
 - Recuperação automática de instância:** Padrão
 - Índice de execução de AMIs:** 0
 - Especificação de crédito:** standard
 - Operação de uso:** RunInstances
 - Supporte a enclaves:** –
 - Permitir tags nos metadados da instância:** Desabilitado
- Monitoramento:** desativado
- Redes:**
 - Monitoramento:** permitido
 - Data de lançamento:** Sat May 17 2025 10:22:21 GMT-0300 (Horário Padrão de Brasília) (38 minutos)
 - Ciclo de vida:** normal
 - Par de chaves atribuído na execução:** coopcred-new
 - ID de kernel:** –
 - ID do disco RAM:** –
 - Modo de inicialização:** uefi-preferred
 - Usar RBN como nome de host do sistema operacional convidado:** Desabilitado
- Armazenamento:**
 - Detalhes da plataforma:** Linux/UNIX
 - Proteção contra encerramento:** Desabilitado
 - Local da AMI:** amazon/ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd64-server-20250115
 - Interromper - Comportamento de hibernação:** Desabilitado
 - Motivo de transição de estado:** –
 - Mensagem de transição de estado:** –
 - Proprietário:** 075404128967
 - Modo de inicialização da instância atual:** legacy-bios
 - Responder IPv4 do nome de host DNS de RBN:** Desabilitado
- Tags:** –
- Host e grupo de posicionamento:**
 - ID do host:** –
 - Nome do grupo de recursos do host:** –
 - Tipo de virtualização:** hvm
 - Número de vCPUs:** 1
- Reserva de capacidade:**
 - ID da reserva de capacidade:** –
 - Configuração de reserva de capacidade:** open

Fonte: AWS (2025).

Figura 28 - EC2 do web-server-2 - Segurança

The screenshot shows the AWS Management Console for an EC2 instance named 'web-server-2'. The 'Segurança' (Security) tab is selected. Under 'Regras de entrada' (Inbound Rules), there are seven rules listed:

| Nome | ID da regra do grupo de... | Intervalo de p... | Protocolo | Origem | Grupos de segurança | Descrição |
|------|----------------------------|-------------------|-----------|-----------|------------------------|-----------|
| - | sgr-0621c703de5dcd10c | 22 | TCP | 0.0.0.0/0 | web-sg | SSH port |
| - | sgr-09a711ac49dcf5166 | 10050 | TCP | 0.0.0.0/0 | web-sg | - |
| - | sgr-03d6761a10d21fb6 | 80 | TCP | 0.0.0.0/0 | web-sg | HTTP |
| - | sgr-0b0b87a88a754d25d | 12000 - 12100 | TCP | 0.0.0.0/0 | web-sg | - |
| - | sgr-0a90faac7cd46dcae | 20 - 21 | TCP | 0.0.0.0/0 | web-sg | - |
| - | sgr-067db3a667b6950ce | Todos | Todos | 0.0.0.0/0 | web-sg | - |
| - | sgr-0fb91ea46aadc186c | 443 | TCP | 0.0.0.0/0 | web-sg | HTTPS |

Fonte: AWS (2025).

Deploy de VPC (Virtual Private Cloud)

A configuração de rede foi realizada por meio da criação de uma Virtual Private Cloud (VPC) personalizada, que assegura a segmentação da infraestrutura e o isolamento de recursos. A VPC foi dividida em sub-redes públicas e privadas, permitindo a distribuição eficiente dos serviços, mantendo os dados sensíveis em sub-redes isoladas.

Tabela 11 - Informações do Ambiente AWS - VPC e Subnets

| Componente | Descrição | Faixa de IP |
|------------------|--|---------------------------------|
| VPC (CIDR) | CIDR da VPC para endereçamento de rede | 10.0.0.0/16 |
| Subnets Públicas | Sub-redes acessíveis pela internet, usadas para frontend e平衡adores de carga | 10.0.101.0/24, 10.0.102.0/24 |
| Subnets Privadas | Sub-redes isoladas da internet, utilizadas para banco de dados e serviços internos | 10.0.1.0/24, 10.0.2.0/24 |

Fonte: AWS (2025).

Configurações adicionais:

- Tabelas de rotas específicas para garantir o tráfego adequado entre as sub-redes;
- Gateway NAT configurado para permitir que instâncias nas sub-redes privadas acessem a internet de forma segura;
- Internet Gateway associado à VPC, possibilitando o acesso à internet das instâncias nas sub-redes

Deploy de EC2 (Instâncias Virtuais)

As instâncias EC2 foram configuradas para hospedar os serviços frontend e backend da plataforma CoopCred, com alta disponibilidade e balanceamento de carga.

Tabela 12 - Informações do Ambiente AWS - Instâncias EC2

| Tipo instância | Descrição | Endereço IP Externo | Endereço IP Interno |
|----------------------------|--------------------------------------|----------------------------|----------------------------|
| Pública - web-server-1 | Servidor para frontend | 18.234.205.86 | 10.0.101.134 |
| Pública - web-server-2 | Servidor para frontend | 52.23.241.144 | 10.0.101.4 |
| Privada - private-server-1 | Servidor para backend/banco de dados | - | 10.0.1.106 |

Fonte: AWS (2025).

A seguir, a tabela 13 detalha os acessos e permissões configurados para cada instância EC2, garantindo o controle adequado e seguro da infraestrutura.

Tabela 13 - Informações do Ambiente AWS - Acessos/Usuários das Instâncias EC2

| Usuário | Acesso | Descrição |
|----------------|---|-----------------------------------|
| ubuntu | SSH | Usuário padrão ao criar instância |
| coopcred | SSH | Usuário para FTP |
| root | Assumir por usuários com permissão root | Usuário Administrador |

Fonte: AWS (2025).

Para a configuração de acesso às máquinas, foram utilizadas chaves privadas SSH geradas pela AWS.

Figura 29- Detalhes ssh

```
pnunes@DESKTOP-1II7RVN:~/.ssh$ ssh -i id_rsa.pem ubuntu@44.204.138.207
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1028-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Sun May 18 14:36:05 UTC 2025

System load: 0.03          Processes:           140
Usage of /:   48.4% of 8.65GB  Users logged in:    0
Memory usage: 32%          IPv4 address for enX0: 10.0.101.22
Swap usage:   0%           ████

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun May 18 14:33:15 2025 from 177.191.160.83
ubuntu@public-02:~$ ████
```

Fonte: AWS (2025).

Configuração de Aplicação Web com Docker e Proxy Reverso (Nginx)

Em relação à aplicação web, foi utilizado o Docker para o deploy de containers nas instâncias EC2 públicas. A aplicação web foi configurada para ser acessível através de um proxy reverso Nginx, que redireciona as requisições para os containers apropriados. Essa configuração permite uma gestão eficiente do tráfego, além de garantir uma comunicação segura entre a aplicação frontend e o banco de dados, hospedado nas instâncias privadas.

Pipeline no git para deploy dos códigos (back-end e front-end)

Figura 30 - Pipeline git



Fonte: GIT (2025).

Figura 31 - códigos (back-end e front-end)

```

1 ► Run ssh ***@*** "cd *** && docker compose up -d --build"
4 time="2025-05-18T14:53:58Z" level=warning msg="***/docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion"
5 Compose can now delegate builds to bake for better performance.
6 To do so, set COMPOSE_BAKE=true.
7 ## building with "default" instance using docker driver
8
9 # [backend internal] load build definition from Dockerfile
10 #1 transferring dockerfile: 1548 0.0s done
11 #1 DONE 0.0s
12
13 #2 [backend internal] load metadata for docker.io/library/node:18-alpine
14 #2 DONE 0.4s
15
16 #3 [backend internal] load .dockerignore
17 #3 transferring context: 2B done
18 #3 DONE 0.0s
19
20 #4 [Backend 1/5] FROM docker.io/library/node:18-alpine@sha256:8d6421d663b4c28fd3ebc498332f249011d118945588d0a35cb9fc4b8ca09d9e
21 #4 DONE 0.0s
22
23 #5 [Backend internal] load build context
24 #5 transferring context: 41.179kB
25 #5 DONE 0.0s
26

```

Fonte: GIT (2025).

Site da Instância

Figura 32 - Home page



ÁREA DE ACESSO

Usuário

Senha

ENTRAR

Fonte: Elaborado pelos autores (2025).

Figura 33 - Dashboard - Cadastro de Conta Bancária

Cadastro de Conta Bancária

Nome

CPF

Telefone

Email

Endereço

Tipo

Número da Conta

Cadastrar Conta

Sair

Fonte: Elaborado pelos autores (2025).

Figura 34 - Dashboard - Lista de Contas Bancárias

The screenshot shows the CoopCred dashboard with a dark green sidebar on the left containing navigation links: 'Cadastro Conta', 'Lista Contas' (highlighted in green), 'Cadastro Usuário', and 'Sair'. The main content area has a title 'Lista de Contas Bancárias' and a search bar. Below is a table with the following data:

| Nome | CPF | Telefone | Email | Endereço | Tipo | Número |
|----------------|----------------|-----------------|-----------------|---------------------------------------|----------|--------|
| Paulo Ferreira | 151.022.489-05 | (31) 99999-9999 | paulo@gmail.com | Rua das Américas, 31 - Belo Horizonte | corrente | 191569 |

Fonte: Elaborado pelos autores (2025).

Figura 35 - Dashboard - Usuário

The screenshot shows the CoopCred dashboard with a dark green sidebar on the left containing navigation links: 'Cadastro Conta', 'Lista Contas', 'Cadastro Usuário' (highlighted in green), and 'Sair'. The main content area has a title 'Cadastro de Usuário' and a search bar with the value 'usuarioTeste'. Below is a table with the following data:

| ID | Usuário | Email | Setor | Ações |
|----|--------------|--------------------|-------|--|
| 2 | usuarioTeste | teste@coopcred.com | | <input type="button" value="Salvar"/> <input type="button" value="Excluir"/> |

Below the table is a section titled 'Adicionar Usuário' with fields for 'Nome', 'E-mail', 'Setor', 'Senha', and a 'Adicionar Usuário' button.

Nome: Nome do usuário
E-mail: email@example.com
Setor: Setor (opcional)
Senha: Senha

Fonte: Elaborado pelos autores (2025).

Alta Disponibilidade com Load Balancer

Para garantir alta disponibilidade e distribuir o tráfego de maneira eficiente entre as instâncias EC2 públicas, foi implementado um Application Load Balancer (ALB). O ALB realiza a verificação contínua da saúde das instâncias (Health Checks) para assegurar que o tráfego seja redirecionado apenas para instâncias operacionais, aumentando a resiliência da plataforma.

Tabela 14 - Informações do Ambiente AWS - Application Load Balancer

| Tipo instância | Endereço DNS Externo |
|---------------------------|---|
| Application Load Balancer | dev06-pnunes-alb-1283229940.us-east-1.elb.amazonaws.com |

Fonte: AWS (2025).

Resolução de DNS com Route 53

Foi configurada uma zona privada no Amazon Route 53, que gerencia os registros DNS internos da VPC. Isso facilita a resolução de nomes entre as instâncias, com uma estrutura amigável, como db.local para os serviços de banco de dados.

3 Gerência e Monitoração de Ambientes de Redes

No projeto foi implementado um sistema de monitoramento utilizando as ferramentas Zabbix e Grafana, com o objetivo de acompanhar em tempo real o estado de serviços de rede, consumo de recursos e disponibilidade de dispositivos. A solução foi dividida em dois ambientes distintos: um local (VirtualBox), e outro em nuvem (AWS).

3.1 Ferramentas Utilizadas

- **Zabbix:** Ferramenta de monitoramento de código aberto utilizada para coleta e análise de métricas de infraestrutura, incluindo disponibilidade de serviços, consumo de CPU, uso de memória, tráfego de rede e status de portas em switches.
- **Grafana:** Plataforma de visualização de dados integrada ao Zabbix para criação de painéis interativos e dashboards personalizados.

3.2 Ambiente Local – VirtualBox

No ambiente local, foi utilizado o appliance Zabbix, importado como máquina virtual no VirtualBox. Esse appliance traz uma instalação completa do Zabbix, incluindo servidor, banco de dados e frontend web.

Após a configuração de rede e IP fixo, o acesso à interface gráfica foi realizado via

navegador. Em seguida, foram adicionados hosts locais (outros VMs ou dispositivos físicos na rede) para coleta de métricas, incluindo:

- Verificação de disponibilidade de serviços (HTTP, SSH, etc.)
- Consumo de CPU e memória
- Status de portas de switches simulados
- Alertas com triggers configuradas para eventos críticos

3.3 Ambiente em Nuvem (AWS)

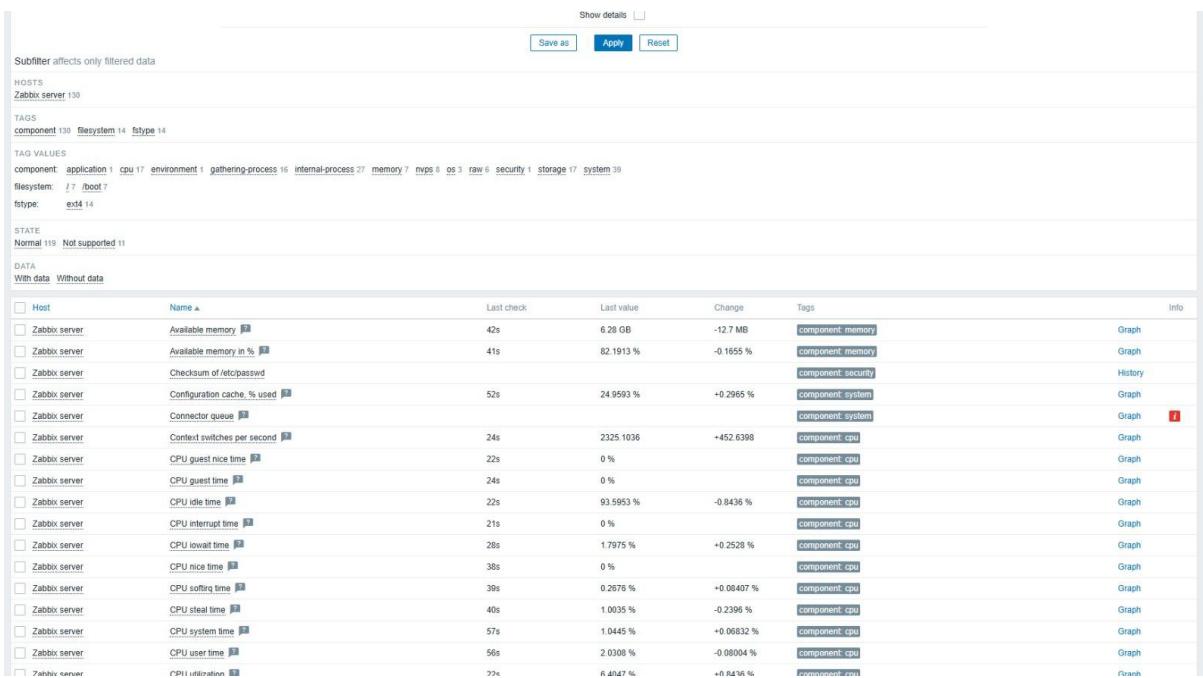
Na AWS, foi criada uma instância EC2 com sistema operacional Ubuntu Server, onde o Zabbix Server foi instalado manualmente, passo a passo. Essa abordagem permitiu maior controle sobre os componentes instalados e possibilitou o monitoramento de recursos da própria nuvem.

Figura 36 - Servidores cloud e local configurados no Zabbix

| Name | Interface | Availability | Tags | Status | Latest data | Problems | Graphs | Dashboards | Web |
|---------------|--------------------|--------------|---|---------|-----------------|----------|-----------|--------------|-----|
| zabbix-agent1 | 3.231.165.44:10050 | ZBX | class: os; class: software; target: linux | Enabled | Latest data 75 | Problems | Graphs 15 | Dashboards 4 | Web |
| Zabbix server | 127.0.0.1:10050 | ZBX | class: os; class: software; target: linux | Enabled | Latest data 130 | Problems | Graphs 12 | Dashboards 4 | Web |

Fonte: Zabbix (2025).

Figura 37 - Mapeamento de métricas pelo Zabbix



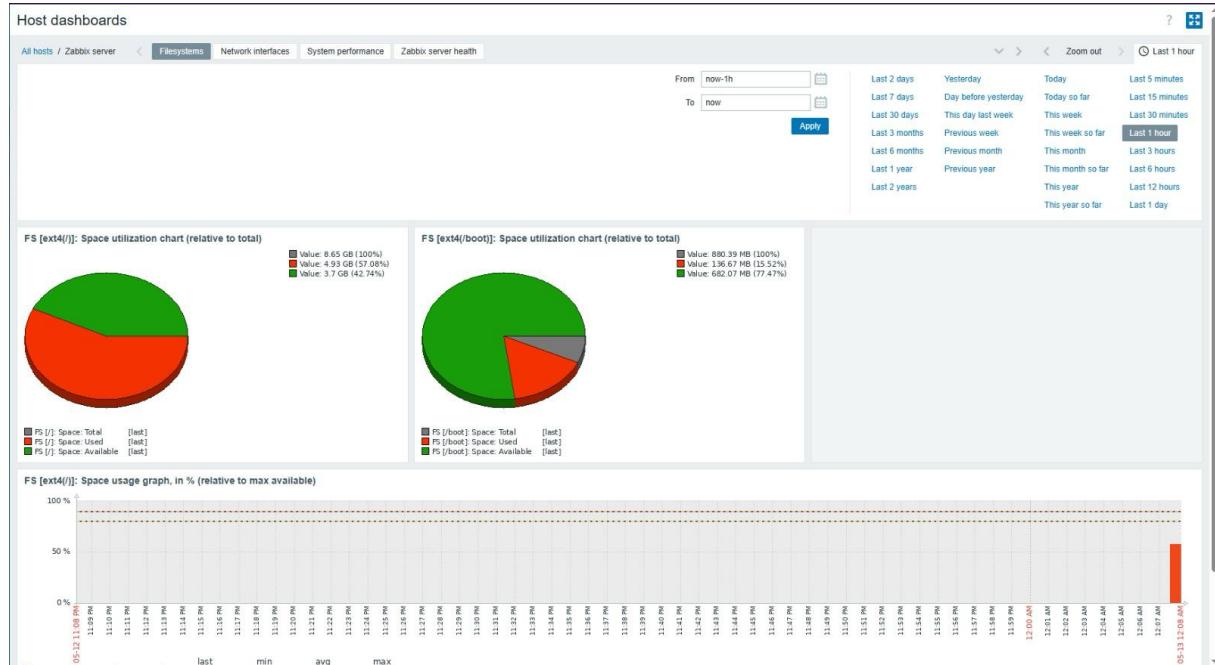
Fonte: Zabbix (2025).

Figura 38 - Informações de sistema do servidor cloud (Utilização de memória CPU e disco)



Fonte: Zabbix (2025).

Figura 39 - Informações de sistema do servidor cloud (Utilização de memória CPU e disco)



Fonte: Zabbix (2025).

Figura 40 - Mapa de monitoramento dos servidores

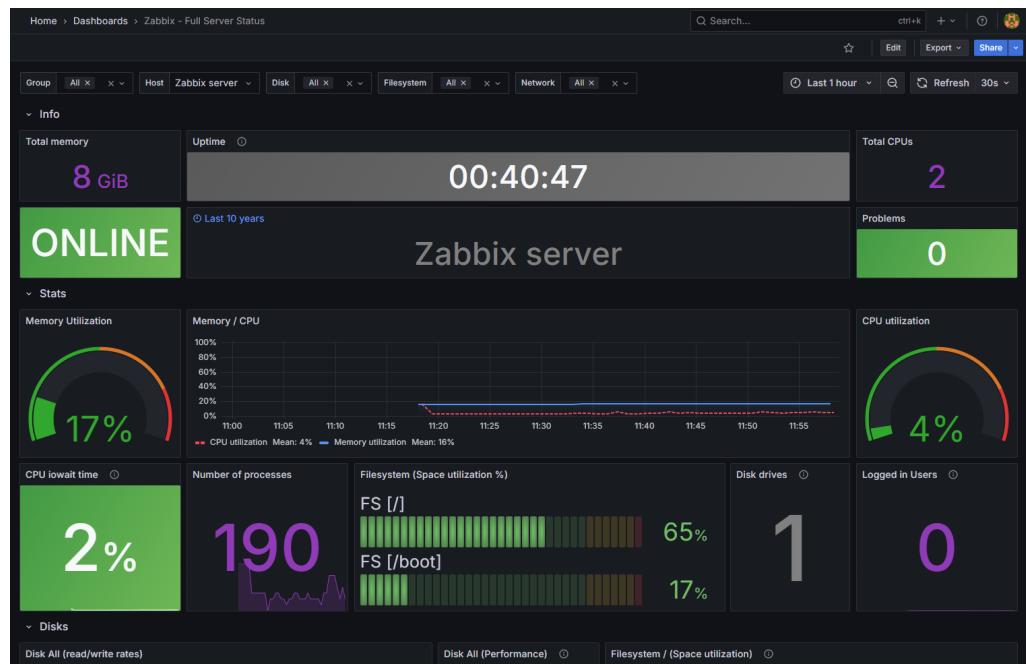


Fonte: Zabbix (2025).

3.4 Integração com Grafana

O Grafana foi instalado em ambos os ambientes e conectado ao banco de dados do Zabbix por meio de plugin específico. Foram criados dashboards personalizados, destacando:

Figura 41 - web-server-1 Monitoramento de processos gerais das máquinas (CPU, Consumo de memória, Consumo de disco, distribuição de processos)



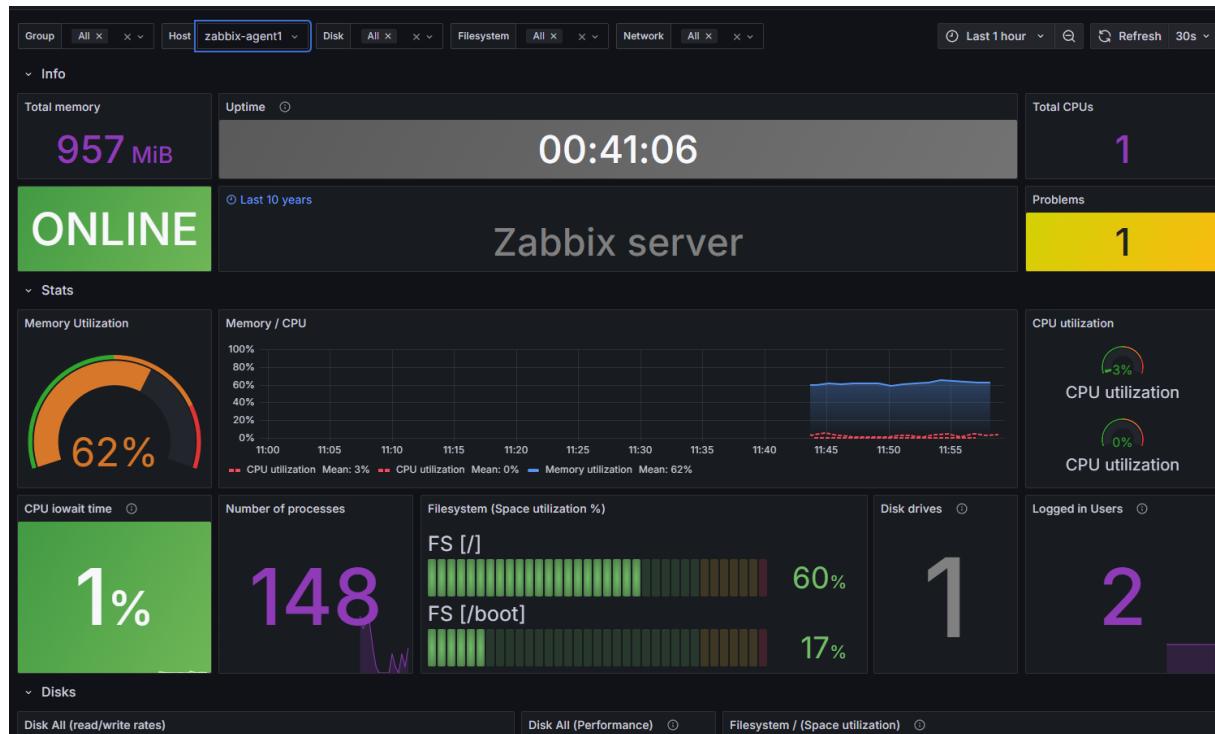
Fonte: Grafana (2025).

Figura 42 - web-server-1 Monitoramento da rede, Monitoramento de I/O da máquina, relatórios de erros.



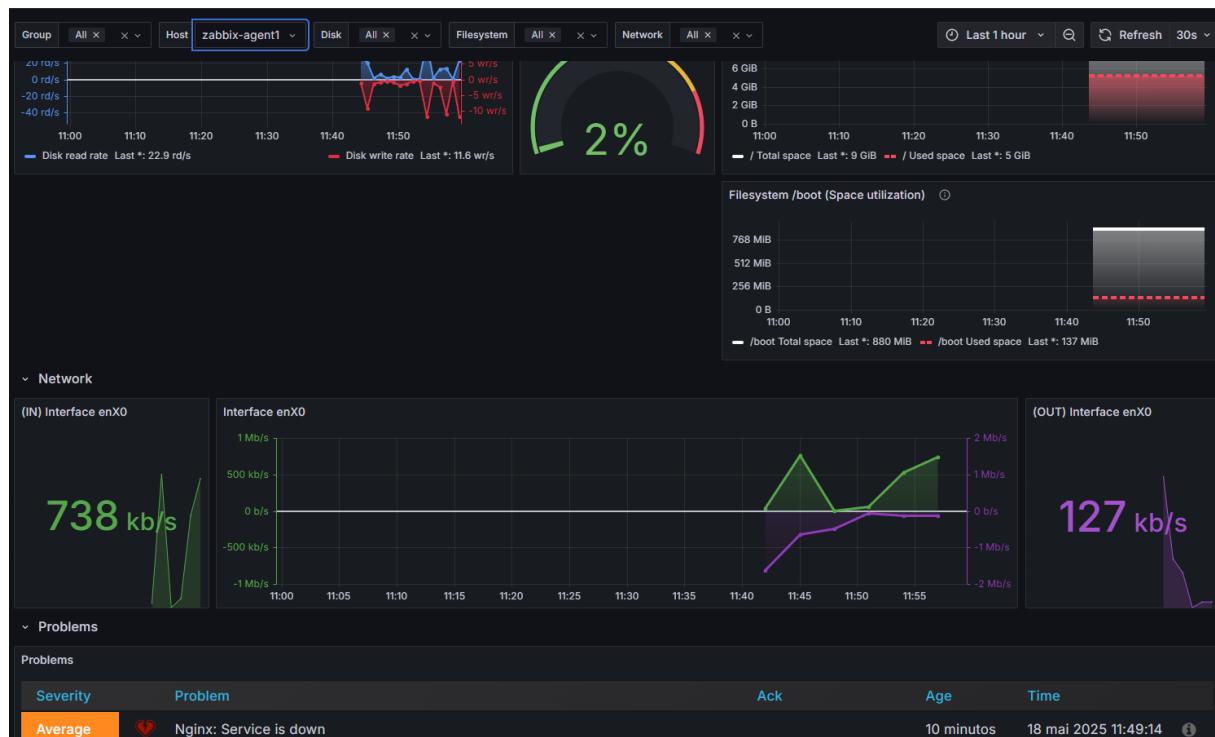
Fonte: Grafana (2025).

Figura 43 - web-server-2 Monitoramento de processos gerais das máquinas (CPU, Consumo de memória, Consumo de disco, distribuição de processos)



Fonte: Grafana (2025).

Figura 44 - web-server-2 Monitoramento da rede, Monitoramento de I/O da máquina, relatórios de erros

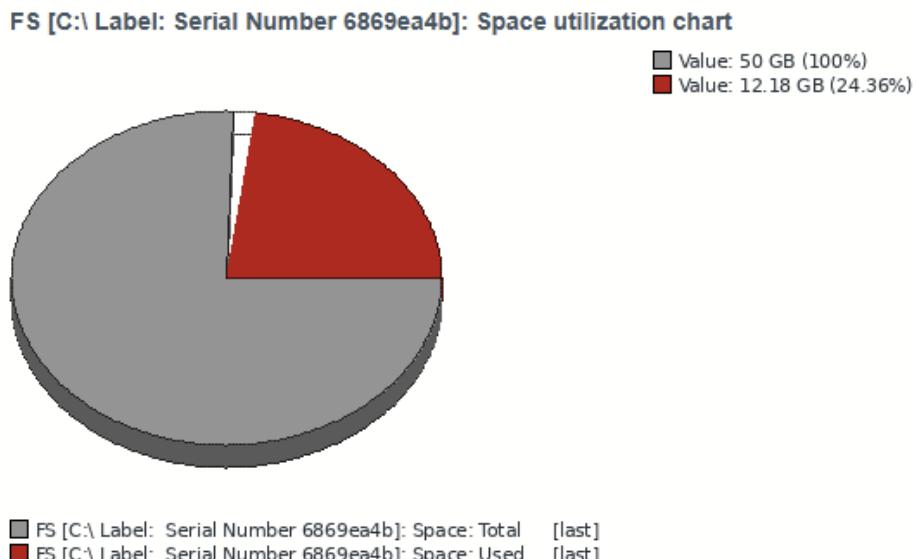


Fonte: Grafana (2025).

3.5 Ambiente local (VirtualBox)

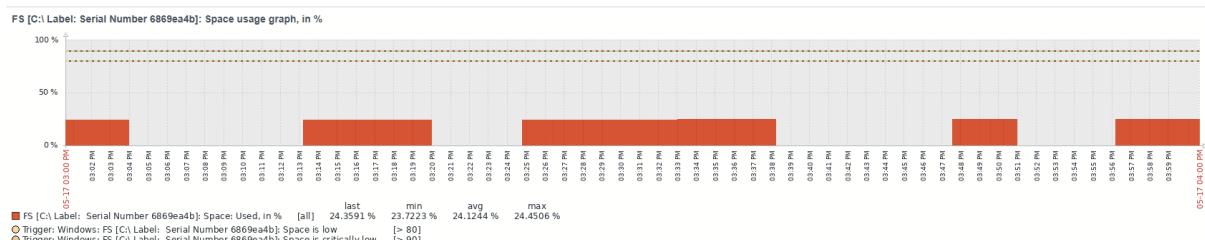
O Zabbix foi integrado ao servidor Windows, em execução em uma máquina virtual no VirtualBox, para monitoramento de desempenho e disponibilidade do sistema.

Figura 45 - Informações de sistema do servidor local (Utilização de memória disco rígido)



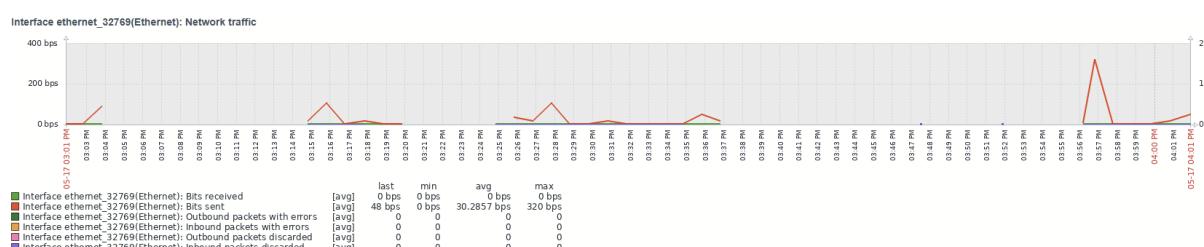
Fonte: Zabbix (2025).

Figura 46 - Informações de sistema do servidor local (Tráfego de internet)

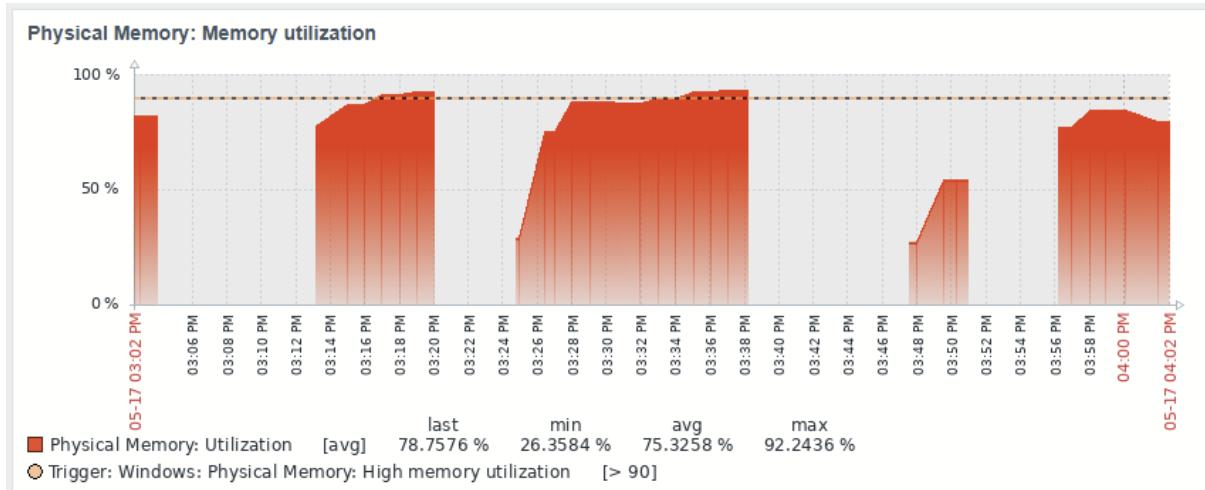


Fonte: Zabbix (2025)

Figura 47 - Informações de sistema do servidor local(Utilização de memória disco rígido em % por período)



Fonte: Zabbix (2025).

Figura 48 - Informações de sistema do servidor local (Utilização de memória RAM)

Fonte: Zabbix (2025).

4 Mecanismos de Segurança

4.1 PSI (Política de Segurança da Informação)

A Política de Segurança da Informação (PSI) da Coopcred estabelece os princípios, diretrizes e controles necessários para proteger os ativos informacionais da cooperativa. Alinhada às melhores práticas do mercado, como a norma ISO/IEC 27001, esta política visa assegurar que os dados e sistemas da Coopcred sejam utilizados de forma segura, íntegra e responsável.

Este documento formaliza regras para classificação da informação, controle de acessos, gestão de vulnerabilidades, resposta a incidentes e o uso adequado de recursos computacionais no ambiente da cooperativa. Sua aplicação busca reduzir riscos cibernéticos, atender às exigências legais e regulatórias (como a LGPD) e preservar a confidencialidade, integridade e disponibilidade das informações que sustentam as operações e a confiança dos cooperados.

O documento completo está disponível [neste link](#).

4.2 Cartilha de boas práticas

Figura 49 - Cartilha de orientação de segurança



A cartilha é um documento informativo com uma capa verde escura. No topo, há o logotipo da CoopCred, que inclui uma ilustração de um leão dourado correndo e o nome "COOPCRED" em branco. Abaixo do logotipo, uma faixa contém o lema "LIDERANDO O AGRO, FORTALECENDO O SEU FUTURO". O conteúdo principal é dividido em seções com ícones e listas de orientações.

Boas-Vindas e Orientações sobre Segurança

Segurança da informação começa com você.

Parabéns por fazer parte da nossa equipe!

Aqui na CoopCred, a segurança da informação é uma prioridade. Proteger os dados dos nossos associados e colaboradores faz parte do nosso compromisso com a confiança e a responsabilidade.

Para isso, é essencial que cada membro da equipe esteja alinhado com nossas boas práticas de segurança. Este folder foi criado para orientar você sobre os principais cuidados e atitudes que ajudam a manter um ambiente digital e físico mais seguro para todos.

Criação de Senhas

- Utilize senhas com no mínimo 8 caracteres, misturando letras maiúsculas e minúsculas, números e caracteres especiais.
- Evite utilizar dados pessoais como data de nascimento ou nomes.
- Cada serviço ou sistema deve ter uma senha única. Evite reutilizar senhas em várias plataformas.

Proteção de Senhas

- Nunca compartilhe sua senha com ninguém, nem mesmo com colegas ou supervisores. Se alguém solicitar sua senha, entre em contato com o setor de TI.
- Armazene suas senhas em um gerenciador confiável, se necessário.
- Evite anotá-las em locais de fácil acesso, como pot-its ou cadernos.

Dispositivos e Senhas

- Mantenha seus dispositivos (PCs, celular, etc.) sempre bloqueados quando não estiverem em uso.
- Atualize regularmente seus dispositivos para garantir que estão protegidos contra ameaças.

Cuidados com e-mail

- Desconfie de e-mails de remetentes desconhecidos ou links suspeitos.
- Nunca clique em links ou abra anexos sem verificar a procedência.
- Caso receba algo suspeito, entre em contato com o suporte de TI.

Manuseio de Informações Confidenciais

- Não compartilhe informações sensíveis da empresa sem autorização.
- Use apenas dispositivos e redes seguras para acessar sistemas corporativos.
- Relate imediatamente qualquer incidente de segurança ao departamento de TI.

Acesso ao Sistema

- Utilize apenas os sistemas e recursos para os quais você foi autorizado.
- Caso precise de acesso adicional, solicite formalmente à sua liderança ou ao departamento de TI.
- Todos os softwares devem ser aprovados pela área de segurança antes da instalação.
- Deslogue da sua conta ao finalizar o trabalho, especialmente em dispositivos compartilhados.

Tenha a cartilha sempre com você.

44

Fonte: Elaborado pelos autores (2025).

Figura 50 - Cartilha de responsabilidade do colaborador



Fonte: Elaborado pelos autores (2025).

4.3 Análise de Vulnerabilidades Relevantes

1. A01:2021 - Broken Access Control

Existe o risco de usuários acessarem recursos além de suas permissões devido a controles de acesso mal implementados. Na infraestrutura da CoopCred, é fundamental reforçar validações de autorização nos endpoints da API e garantir isolamento adequado entre containers, especialmente para serviços com diferentes níveis de privilégio.

2. A02:2021 - Cryptographic Failures

Falhas na implementação de criptografia podem levar à exposição de dados sensíveis, como credenciais e informações bancárias. É essencial garantir o uso de protocolos seguros (HTTPS/TLS), armazenamento seguro de senhas (ex: bcrypt/scrypt) e gerenciamento apropriado de chaves e segredos, evitando exposição em variáveis de ambiente ou arquivos versionados.

3. **A05:2021 - Security Misconfiguration**

Má configurações comuns em ambientes Docker podem abrir brechas, como:

- Containers executando como root sem necessidade;
- Exposição de portas desnecessárias;
- Falta de hardening em imagens base;
- Arquivos sensíveis (ex: .env, chaves SSH) presentes nos containers.
Recomenda-se automatizar validações de segurança na construção e no deploy dos containers.

4. **A06:2021 - Vulnerable and Outdated Components**

Imagens Docker e dependências desatualizadas representam risco elevado, especialmente com bibliotecas que possuem CVEs conhecidos. É importante utilizar imagens oficiais e atualizadas, bem como configurar scanners automáticos para detectar e mitigar vulnerabilidades conhecidas.

5. **A08:2021 - Software and Data Integrity Failures**

A ausência de mecanismos para validar a integridade de builds, imagens e dependências pode comprometer a cadeia de suprimentos de software. Na pipeline CI/CD da CoopCred, recomenda-se o uso de:

- Assinatura de imagens e validação via cosign ou Notary;
- Hash/checksum de arquivos críticos;
- Controle de integridade de pacotes e plugins usados nos pipelines.

6. **A09:2021 - Security Logging and Monitoring Failures**

Sem logs adequados, ataques e falhas operacionais podem passar despercebidos.

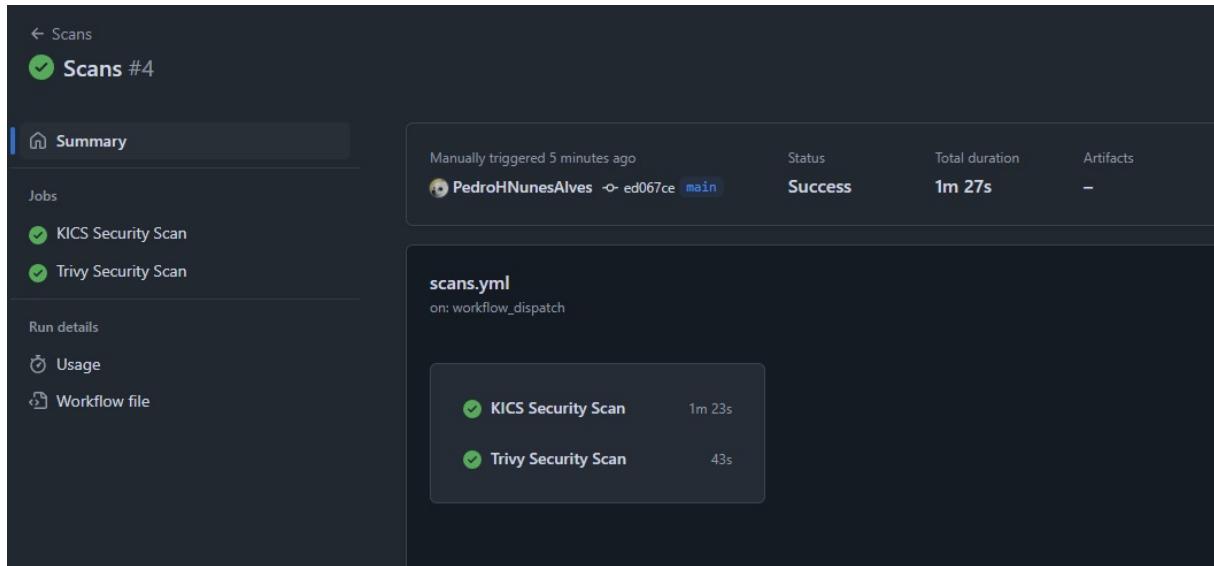
É essencial implementar:

- Log centralizado e seguro;
- Monitoramento ativo de containers e serviços (ex: Grafana);
- Auditoria de acessos e alterações em ambiente de produção.

4.4 Pipeline de Segurança

A implementação de um pipeline de segurança automatizada com foco em infraestrutura como código e análise de pacotes, visando garantir a conformidade e identificar vulnerabilidades de forma contínua.

Figura 51 - Scans KICS e Trivy



Fonte: Elaborado pelos autores (2025).

Varredura de IaC com KICS

Utilizando a ferramenta KICS (Keeping Infrastructure as Code Secure) para realizar varreduras em arquivos de infraestrutura como código.

Figura 52 - Findings Terraform

```

518 Passwords And Secrets - Generic Token, Severity: HIGH, Results: 2
519 Description: Query to find passwords and secrets in infrastructure code.
520 Platform: Common
521 Learn more about this vulnerability: https://docs.kics.io/latest/queries/common-queries/common/baee230e-1021-4801-9c3f-79ee1d7b2cbc
522 [1]: infraestrutura/terraform/config/dev.tfvars:4
523
524     003: acme_email_address = "xxxxxxxxxxxxxxxxxxxxxx"
525
526     004: cloudflare_api_token = <SECRET-MASKED-ON-PURPOSE>
527
528     005:
529
530
531 [2]: infraestrutura/terraform/config/prd.tfvars:4
532
533     003: acme_email_address = "xxxxxxxxxxxxxxxxxxxxxx"
534
535     004: cloudflare_api_token = <SECRET-MASKED-ON-PURPOSE>
536
537     005:
538
539 Passwords And Secrets - Generic Private Key, Severity: HIGH, Results: 1
540 Description: Query to find passwords and secrets in infrastructure code.
541 Platform: Common
542 Learn more about this vulnerability: https://docs.kics.io/latest/queries/common-queries/common/2f665079-c381-4b31-89de-88268c1fa58
543 [1]: infraestrutura/terraform/acme.tf:29
544
545     028:
546     029: private_key      = <SECRET-MASKED-ON-PURPOSE>
547     030: certificate_body = acme_certificate.certificate[each.key].certificate_pem
548
549
550 HTTP Port Open To Internet, Severity: HIGH, Results: 1
551 Description: The HTTP port is open to the internet in a Security Group
552 Platform: Terraform
553 Learn more about this vulnerability: https://docs.kics.io/latest/queries/terraform-queries/aws/ffac8a12-322e-42c1-b9b9-81ff85c39ef7
554 [1]: infraestrutura/terraform/alb-sec.tf:1
555
556     001: resource "aws_security_group" "alb_sg" {
557         002:   for_each = var.load_balancers
558         003:
559
560

```

Fonte: Elaborado pelos autores (2025).

Figura 53 - Findings Ansible

```

35 Scanning with Keeping Infrastructure as Code Secure v1.7.18
36
37
38
39
40
41 Risky File Permissions, Severity: INFO, Results: 1
42 Description: Some modules could end up creating new files on disk with permissions that might be too open or unpredictable
43 Platform: Ansible
44 Learn more about this vulnerability: https://docs.kics.io/latest/queries/ansible-queries/common/88841d5c-d22d-4b7e-a6a0-89ca50e44b9f
45
46 [1]: infraestrutura/ansible/roles/etapa-02/handlers/50-deployment.yml:1
47
48     030: - name: Copy Kuma template files
49     031:   ansible.builtin.copy:
50     032:     src: "{{ role_path }}/{{ templates/deployment/Kuma }}"
51
52
53 Logging of Sensitive Data, Severity: LOW, Results: 1
54 Description: To keep sensitive values out of logs, tasks that expose them need to be marked defining 'no_log' and setting to True
55 Platform: Ansible
56 Learn more about this vulnerability: https://docs.kics.io/latest/queries/ansible-queries/common/c6473dae-8477-4119-88b7-b909b435ce7b
57
58 [1]: infraestrutura/ansible/ansible.cfg:1
59
60     001: [defaults]
61     002: roles_path = ./roles
62     003: host_key_checking = False
63
64
65
66 Results Summary:
67 HIGH: 0
68 MEDIUM: 0
69 LOW: 1
70 INFO: 1
71 TOTAL: 2
72

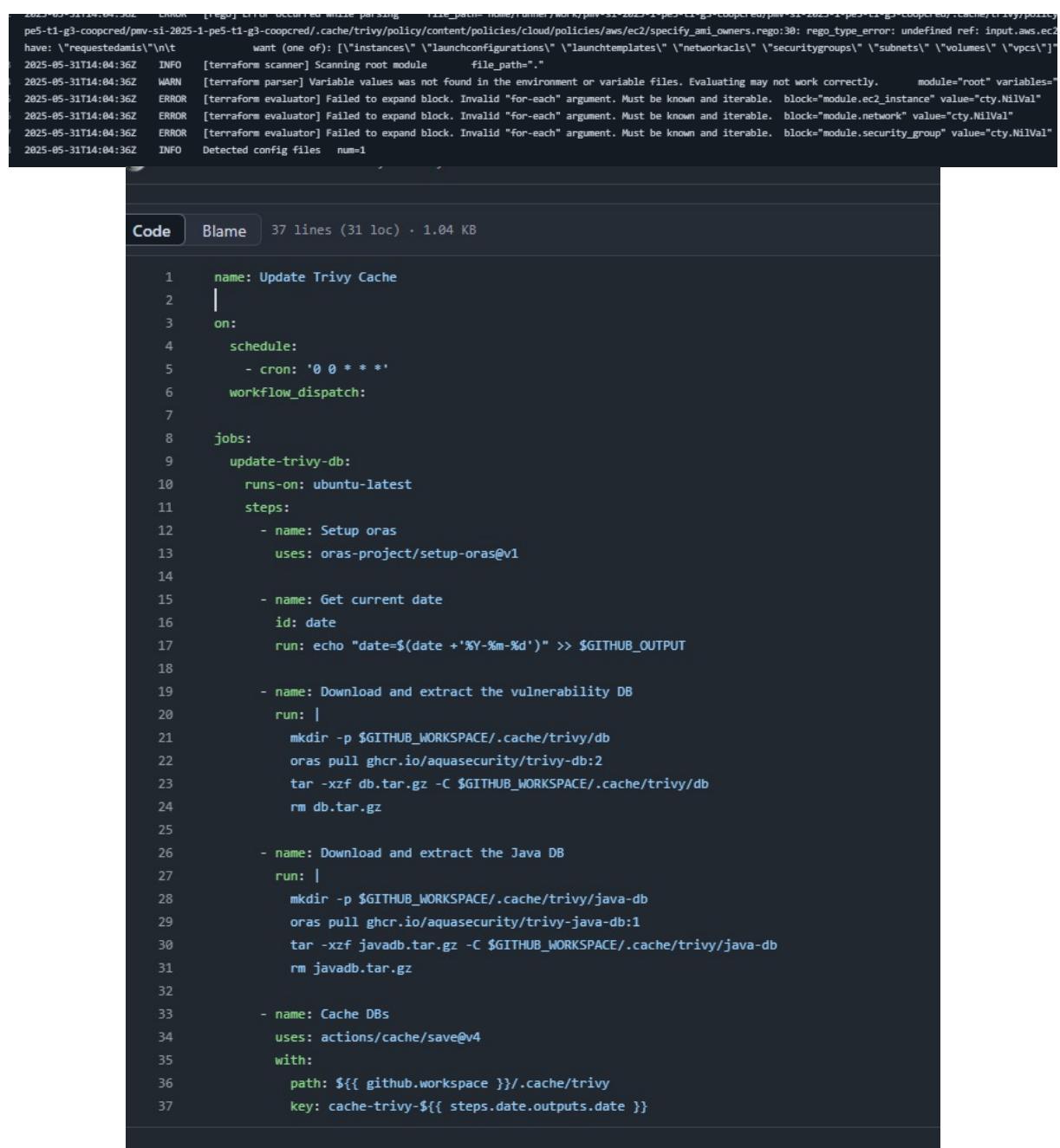
```

Fonte: Elaborado pelos autores (2025).

Análise de Vulnerabilidades com Trivy

Para análise de segurança em pacotes, containers e dependências, a pipeline executa um scan completo com o Trivy em todo o repositório. Esse processo é automatizado e executado diariamente à meia-noite, utilizando um cache atualizado das vulnerabilidades conhecido pelo Trivy, o que acelera as análises subsequentes e mantém os dados sempre recentes.

Figura 54 - Execução do Trivy Scan com análise de pacotes



The figure consists of two vertically stacked screenshots. The top screenshot shows a terminal window with Trivy scan logs. The logs indicate a policy error occurred while parsing a Terraform configuration file, specifically regarding the 'aws_ec2_specify_ami_owners' block. The log entries show various levels of severity (INFO, WARN, ERROR) from May 31, 2025, at 04:36Z. The bottom screenshot shows a GitHub Actions workflow file named 'update-trivy-db.yml'. The workflow defines a job named 'update-trivy-db' that runs on an Ubuntu-latest runner. It includes steps for setting up Oracle Linux (oras), getting the current date, downloading and extracting the Trivy vulnerability database, downloading and extracting the Java DB, and finally caching the databases using GitHub Actions' cache feature.

```

2025-05-31T14:04:36Z [ERROR] Error occurred while parsing file_path: /home/runner/.local/share/pmv-si-2025-1-pe5-t1-g3-coopcred/.cache/trivy/policy/content/policies/cloud/policies/aws/ec2/specify_ami_owners.rego:30: rego_type_error: undefined ref: input.aws.ec2 have: \"requestedamis\"\\n\\t      want (one of): [\"instances\" \"launchconfigurations\" \"launchtemplates\" \"networkaclss\" \"securitygroups\" \"subnets\" \"volumes\" \"vpcs\"]"
2025-05-31T14:04:36Z [INFO] [terraform scanner] Scanning root module file_paths..
2025-05-31T14:04:36Z [WARN] [terraform parser] Variable values was not found in the environment or variable files. Evaluating may not work correctly. module="root" variables=""
2025-05-31T14:04:36Z [ERROR] [terraform evaluator] Failed to expand block. Invalid "for-each" argument. Must be known and iterable. block="module.ec2_instance" value="cty.NilVal"
2025-05-31T14:04:36Z [ERROR] [terraform evaluator] Failed to expand block. Invalid "for-each" argument. Must be known and iterable. block="module.network" value="cty.NilVal"
2025-05-31T14:04:36Z [ERROR] [terraform evaluator] Failed to expand block. Invalid "for-each" argument. Must be known and iterable. block="module.security_group" value="cty.NilVal"
2025-05-31T14:04:36Z [INFO] Detected config files num=1

Code Blame 37 lines (31 loc) · 1.04 KB

1   name: Update Trivy Cache
2   |
3   on:
4     schedule:
5       - cron: '0 0 * * *'
6     workflow_dispatch:
7
8   jobs:
9     update-trivy-db:
10    runs-on: ubuntu-latest
11    steps:
12      - name: Setup oras
13        uses: oras-project/setup-oras@v1
14
15      - name: Get current date
16        id: date
17        run: echo "date=$(date +'%Y-%m-%d')" >> $GITHUB_OUTPUT
18
19      - name: Download and extract the vulnerability DB
20        run: |
21          mkdir -p $GITHUB_WORKSPACE/.cache/trivy/db
22          oras pull ghcr.io/aquasecurity/trivy-db:2
23          tar -xzf db.tar.gz -C $GITHUB_WORKSPACE/.cache/trivy/db
24          rm db.tar.gz
25
26      - name: Download and extract the Java DB
27        run: |
28          mkdir -p $GITHUB_WORKSPACE/.cache/trivy/java-db
29          oras pull ghcr.io/aquasecurity/trivy-java-db:1
30          tar -xzf javadb.tar.gz -C $GITHUB_WORKSPACE/.cache/trivy/java-db
31          rm javadb.tar.gz
32
33      - name: Cache DBs
34        uses: actions/cache/save@v4
35        with:
36          path: ${{ github.workspace }}/.cache/trivy
37          key: cache-trivy-${{ steps.date.outputs.date }}

```

Fonte: Elaborado pelos autores (2025).

Figura 55 - Cache de vulnerabilidades identificado pelo Trivy.

```
update-trivy-db
succeeded 16 hours ago in 26s

> ✓ Set up job
> ✓ Setup oras
> ✓ Get current date
> ✓ Download and extract the vulnerability DB
✓ ✓ Download and extract the Java DB
  1 ► Run mkdir -p $GITHUB_WORKSPACE/.cache/trivy/java-db
  7 Downloading ddf7331b23ea javadb.tar.gz
  8 Downloaded ddf7331b23ea javadb.tar.gz
  9 Pulled [registry] gcr.io/aquasecurity/trivy-java-db:1
 10 Digest: sha256:98664235e6bac8dfebfa10aaef23377311cb8468164e07b3807989f88a8ee69

✓ ✓ Cache DBs
  1 ► Run actions/cache/save@v4
  6 /usr/bin/tar --posix -cf cache.tzst --exclude cache.tzst -P -C /home/runner/work/pmv-si-2025-1-pe5-t1-g3-coopcred/pmv-si-2025-1-pe5-t1-g3-coopcred --files-f
  7 Sent 0 of 783516679 (0.0%), 0.0 MBs/sec
  8 Sent 335544328 of 783516679 (42.8%), 159.9 MBs/sec
  9 Sent 649298951 of 783516679 (82.9%), 206.3 MBs/sec
 10 Sent 783516679 of 783516679 (100.0%), 216.2 MBs/sec
 11 Cache saved with key: cache-trivy-2025-06-01

> ✓ Complete job
```

Fonte: Elaborado pelos autores (2025).

4.5 Aplicação Backend

Figura 56 – Registro do funcionário no banco de dados

```
coopcred=# SELECT * FROM users;
ERROR: relation "users" does not exist
LINE 1: SELECT * FROM users;
          ^
coopcred=# CREATE TABLE users (
    id      SERIAL PRIMARY KEY,
    username VARCHAR(50) NOT NULL,
    email   VARCHAR(100) NOT NULL,
    password VARCHAR(255) NOT NULL
);
coopcred=# \d
              Table "public.users"
  Column   | Type    | Modifiers | Not null | Description
 -----------
  id       | integer |           | not null | 
  username | character varying | not null | 
  email    | character varying | not null | 
  password | character varying | not null | 

coopcred=# INSERT INTO users (username, email, password) VALUES ('Rodrigo', 'Rodrigo@coopcred.com', '$2b$10$hTjeBT49Gj2.b0CmQf9/puASA67NE95aKEOpFckkEcACeaqYQFN4u');
(1 row)

coopcred=#
```

Fonte: Elaborado pelos autores (2025).

Código da aplicação

```
const express = require("express");
const cors = require("cors");
const { Pool } = require("pg");
const bcrypt = require("bcrypt");
const app = express();
const port = 3000;

app.use(cors());
app.use(express.json());

const pool = new Pool({
  host: process.env.DB_HOST,
  port: parseInt(process.env.DB_PORT),
  user: process.env.DB_USER,
  password: process.env.DB_PASSWORD,
  database: process.env.DB_NAME,
});

// Registro
app.post("/register", async (req, res) => {
  const { username, email, password } = req.body;

  if (!username || !email || !password) {
    return res.status(400).json({ error: "Preencha todos os campos" });
  }

  try {
    // Verifica se usuário já existe
    const exists = await pool.query(
      "SELECT * FROM usuarios WHERE username = $1",
      [username]
    );
    if (exists.rowCount > 0) {
      return res.status(400).json({ error: "Usuário já existe" });
    }

    // Hash da senha
    const hashedPassword = await bcrypt.hash(password, 10);

    // Insere usuário no banco
    await pool.query(
      "INSERT INTO usuarios (username, email, password) VALUES ($1, $2, $3)",
      [username, email, hashedPassword]
    );

    res.status(201).json({ message: "Usuário registrado com sucesso" });
  } catch (error) {
    console.error(error);
    res.status(500).json({ error: "Erro no servidor" });
  }
});
```

```
app.post("/login", async (req, res) => {
    const { username, password } = req.body;

    try {
        const result = await pool.query(
            "SELECT * FROM usuarios WHERE username = $1",
            [username]
        );
        const user = result.rows[0];

        if (!user) {
            return res.status(401).json({ error: "Usuário ou senha inválidos" });
        }

        // Compara senha
        const match = await bcrypt.compare(password, user.password);
        if (!match) {
            return res.status(401).json({ error: "Usuário ou senha inválidos" });
        }

        // Login OK - aqui você pode criar um token JWT, sessão, etc
        res.json({ message: "Login bem-sucedido" });
    } catch (err) {
        console.error(err);
        res.status(500).json({ error: "Erro no servidor" });
    }
});

// Listar usuários
app.get("/users", async (req, res) => {
    try {
        const result = await pool.query(
            "SELECT id, username, email FROM usuarios ORDER BY id"
        );
        res.json(result.rows);
    } catch (err) {
        res.status(500).json({ error: "Erro ao buscar usuários" });
    }
});

// Criar usuário
app.post("/users", async (req, res) => {
    const { username, email } = req.body;
    try {
        await pool.query(
            "INSERT INTO usuarios (username, email, password) VALUES ($1, $2, $3)",
            [username, email, ""]
        ); // Atenção: para senha pode deixar vazio ou ajustar para hash default
        res.status(201).json({ message: "Usuário criado" });
    } catch (err) {
        res.status(500).json({ error: "Erro ao criar usuário" });
    }
});
```

```
// Atualizar usuário
app.put("/users/:id", async (req, res) => {
  const id = req.params.id;
  const { username, email } = req.body;
  try {
    await pool.query("UPDATE usuarios SET username=$1, email=$2 WHERE id=$3", [
      username,
      email,
      id,
    ]);
    res.json({ message: "Usuário atualizado" });
  } catch (err) {
    res.status(500).json({ error: "Erro ao atualizar usuário" });
  }
});

// Deletar usuário
app.delete("/users/:id", async (req, res) => {
  const id = req.params.id;
  try {
    await pool.query("DELETE FROM usuarios WHERE id=$1", [id]);
    res.json({ message: "Usuário deletado" });
  } catch (err) {
    res.status(500).json({ error: "Erro ao deletar usuário" });
  }
});

app.get("/contas", async (req, res) => {
  try {
    const result = await pool.query("SELECT * FROM contaBancaria ORDER BY id");
    res.json(result.rows);
  } catch (err) {
    console.error(err);
    res.status(500).json({ error: "Erro ao buscar contas bancárias" });
  }
});

// Buscar conta bancária por ID
app.get("/contas/:id", async (req, res) => {
  const { id } = req.params;
  try {
    const result = await pool.query(
      "SELECT * FROM contaBancaria WHERE id = $1",
      [id]
    );
    if (result.rows.length === 0) {
      return res.status(404).json({ error: "Conta bancária não encontrada" });
    }
    res.json(result.rows[0]);
  } catch (err) {
    console.error(err);
    res.status(500).json({ error: "Erro ao buscar conta bancária" });
  }
});
```

```
app.post("/contas", async (req, res) => {
  const { cpf, numeroConta, tipoConta, agencia } = req.body;
  try {
    const result = await pool.query(
      "INSERT INTO contaBancaria (cpf, numeroConta, tipoConta, agencia) VALUES ($1, $2, $3, $4)",
      [cpf, numeroConta, tipoConta, agencia]
    );
    res.status(201).json(result.rows[0]);
  } catch (err) {
    console.error(err);
    res.status(500).json({ error: "Erro ao criar conta bancária" });
  }
});

// Atualizar conta bancária
app.put("/contas/:id", async (req, res) => {
  const { id } = req.params;
  const { cpf, numeroConta, tipoConta, agencia } = req.body;
  try {
    const result = await pool.query(
      "UPDATE contaBancaria SET cpf = $1, numeroConta = $2, tipoConta = $3, agencia = $4 WHERE id = $4",
      [cpf, numeroConta, tipoConta, agencia, id]
    );
    if (result.rows.length === 0) {
      return res.status(404).json({ error: "Conta bancária não encontrada" });
    }
    res.json(result.rows[0]);
  } catch (err) {
    console.error(err);
    res.status(500).json({ error: "Erro ao atualizar conta bancária" });
  }
});

// Deletar conta bancária
app.delete("/contas/:id", async (req, res) => {
  const { id } = req.params;
  try {
    const result = await pool.query(
      "DELETE FROM contaBancaria WHERE id = $1 RETURNING *",
      [id]
    );
    if (result.rows.length === 0) {
      return res.status(404).json({ error: "Conta bancária não encontrada" });
    }
    res.json({ message: "Conta bancária deletada com sucesso" });
  } catch (err) {
    console.error(err);
    res.status(500).json({ error: "Erro ao deletar conta bancária" });
  }
});
```

```
app.get("/transacoes", async (req, res) => {
    try {
        const result = await pool.query(
            "SELECT * FROM transacoes ORDER BY data DESC"
        );
        res.json(result.rows);
    } catch (err) {
        console.error(err);
        res.status(500).json({ error: "Erro ao buscar transações" });
    }
});

// Buscar transação por ID
app.get("/transacoes/:id", async (req, res) => {
    const { id } = req.params;
    try {
        const result = await pool.query("SELECT * FROM transacoes WHERE id = $1", [
            id,
        ]);
        if (result.rows.length === 0) {
            return res.status(404).json({ error: "Transação não encontrada" });
        }
        res.json(result.rows[0]);
    } catch (err) {
        console.error(err);
        res.status(500).json({ error: "Erro ao buscar transação" });
    }
});

// Criar transação
app.post("/transacoes", async (req, res) => {
    const { tipoTransacao, valor, contaOrigemId, contaDestinoId } = req.body;
    const client = await pool.connect();
    try {
        await client.query("BEGIN");
        // Verificar saldo suficiente na conta de origem
        if (contaOrigemId) {
            const contaOrigem = await client.query(
                "SELECT saldo FROM contaBancaria WHERE id = $1 FOR UPDATE",
                [contaOrigemId]
            );
            if (contaOrigem.rows.length === 0) {
                throw new Error("Conta de origem não encontrada");
            }
            if (contaOrigem.rows[0].saldo < valor) {
                throw new Error("Saldo insuficiente");
            }
            // Debitar da conta de origem
            await client.query(
                "UPDATE contaBancaria SET saldo = saldo - $1 WHERE id = $2",
                [valor, contaOrigemId]
            );
        }
        // Creditar na conta de destino
        if (contaDestinoId) {
            const contaDestino = await client.query(
                "SELECT id FROM contaBancaria WHERE id = $1 FOR UPDATE",
                [contaDestinoId]
            );
            if (contaDestino.rows.length === 0) {
                throw new Error("Conta de destino não encontrada");
            }
            const novoSaldo = contaDestino.rows[0].saldo + valor;
            await client.query(
                "UPDATE contaBancaria SET saldo = $1 WHERE id = $2",
                [novoSaldo, contaDestinoId]
            );
        }
    } catch (err) {
        client.query("ROLLBACK");
        console.error(err);
        res.status(500).json({ error: "Erro ao criar transação" });
    } finally {
        client.end();
    }
});
```

```
CREATE TABLE usuarios (
    id SERIAL PRIMARY KEY,
    username VARCHAR(50) UNIQUE NOT NULL,
    email VARCHAR(100) UNIQUE NOT NULL,
    password VARCHAR(255) NOT NULL
);

CREATE TABLE contaBancaria (
    id SERIAL PRIMARY KEY,
    cpf VARCHAR(11) NOT NULL,
    numeroConta VARCHAR(20) UNIQUE NOT NULL,
    saldo DECIMAL(10, 2) NOT NULL DEFAULT 0.00,
    tipoConta VARCHAR(20) NOT NULL DEFAULT 'Corrente',
    agencia VARCHAR(20) NOT NULL,
    );
;

CREATE TABLE transacoes (
    id SERIAL PRIMARY KEY,
    tipoTransacao VARCHAR(20) NOT NULL,
    valor DECIMAL(10, 2) NOT NULL,
    data TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
)
```

Conclusão

Desenvolver o projeto de infraestrutura de rede foi uma experiência muito rica.

Ao longo do trabalho, conseguimos aplicar na prática diversos conceitos aprendidos nas aulas de microfundamentos e também nas reuniões com o nosso orientador, desde o planejamento da rede física até a criação de uma aplicação completa, com foco na segurança, organização e funcionalidade.

Na parte de infraestrutura, pensar em uma rede bem estruturada, escolher os equipamentos certos e garantir que tudo estivesse funcionando de forma estável foi um grande desafio e também um aprendizado valioso.

Mais do que entregar um sistema funcional, o projeto nos permitiu entender a importância de unir a área de redes com o desenvolvimento de software. Essa integração foi essencial para criar uma solução completa, que de fato atende às necessidades da CoopCred. Ao final, o sentimento é de dever cumprido e, principalmente, de evolução profissional que levaremos para toda a nossa carreira.

REFERÊNCIAS

- ABNT. **NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.** [S.l.: s.n.], 2013. Norma brasileira baseada na ISO/IEC 27001 sobre gestão da segurança da informação.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).** 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 11 jun. 2025.
- CAVALCANTI, J. **Infraestrutura de Redes: Guia Prático de Projeto e Implementação.** São Paulo: Novatec Editora, 2021. Guia prático voltado para o planejamento e a implementação de redes.
- Cisco Systems, Inc. **Enterprise Networking, Security, and Automation Companion Guide.** Indianapolis: Cisco Press, 2018. Referência para arquitetura em camadas e segmentação de redes LAN.
- FOROUZAN, B. A. **Data Communications and Networking.** 5. ed. New York: McGraw-Hill Education, 2017. Edição usada para estudo de redes e comunicação de dados.
- STALLINGS, W. **Segurança em redes: princípios e prática.** 1. ed. São Paulo: Pearson, 2014. Referência em segurança da informação aplicada a redes.
- STALLINGS, W. **Data and Computer Communications.** 10. ed. Boston: Pearson, 2016. Capítulos sobre VPN, MPLS e topologias de rede.
- TANENBAUM, A. S.; WETHERALL, D. J. **Redes de Computadores.** 5. ed. São Paulo: Pearson, 2011. Obra fundamental sobre redes de computadores.
- TANENBAUM, A. S.; WETHERALL, D. J. **Computer Networks.** 5. ed. Boston: Pearson, 2013. Seção sobre topologias em anel e camadas de rede.