INSTITUTO FEDERAL
Rondônia

MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

Campus Porto Velho Zona Norte
Coordenação do Curso Superior de Tecnologia em Redes de Computadores

RAMON SILAS SHOCKNESS ALFONSIN
JHON JETSON DE SOUZA GOMES

MODELO DE GERENCIAMENTO DE INFRAESTRUTURA VIRTUALIZADA DEFINIDA POR CÓDIGO

PORTO VELHO
2026

RAMON SILAS SHOCKNESS ALFONSIN
JHON JETSON DE SOUZA GOMES

MODELO DE GERENCIAMENTO DE INFRAESTRUTURA VIRTUALIZADA DEFINIDA POR CÓDIGO

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – (IFRO), Campus Porto Velho Zona Norte, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso Superior em Redes de Computadores, sob a orientação do professor Dr. Jhordano Malacarne Bravim.

PORTO VELHO
2026

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO.

Alfonsin, Ramon Silas Shockness.
Modelo de gerenciamento de infraestrutura virtualizada definida por código / Ramon Silas Shockness Alfonsin, Jhon Jetson de Souza Gomes. - Porto Velho, 2026.
25 f. : il.

Orientador(a): Prof. Dr. Jhordano Malacarne Bravim.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho, 2026.

1. Automação. 2. Infraestrutura como código. 3. Virtualização. 4. Segurança. 5. DevOps. I. Gomes, Jhon Jetson de Souza. II. Bravim, Jhordano Malacarne (orient.). III. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. IV. Título.

Bibliotecário(a) Responsável: Marlene Fouz da Silva, CRB-11/946

RAMON SILAS SHOCKNESS ALFONSIN
JHON JETSON DE SOUZA GOMES

MODELO DE GERENCIAMENTO DE INFRAESTRUTURA VIRTUALIZADA DEFINIDA POR CÓDIGO

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – (IFRO), *Campus* Porto Velho Zona Norte, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso Superior em Redes de Computadores, sob a orientação do professor Dr. Jhordano Malacarne Bravim

Aprovado em: 16/06/2026 pela banca examinadora.

gov.br Documento assinado digitalmente
SILMAR ANTONIO BUCHNER DE OLIVEIRA
Data: 30/06/2026 21:22:23-0300
Verifique em https://validar.iti.gov.br

Silmar Antonio Buchner de Oliveira
Membro da Banca

gov.br Documento assinado digitalmente
RENATO ALMEIDA DE OLIVEIRA
Data: 30/06/2026 20:29:27-0300
Verifique em https://validar.iti.gov.br

Renato Almeida de Oliveira
Membro da Banca

gov.br Documento assinado digitalmente
JHORDANO MALACARNE BRAVIM
Data: 30/06/2026 21:48:23-0300
Verifique em https://validar.iti.gov.br

Jhordano Malacarne Bravim
Membro da Banca
Orientador

MODELO DE GERENCIAMENTO DE INFRAESTRUTURA VIRTUALIZADA DEFINIDA POR CÓDIGO

RESUMO: A crescente demanda por ambientes computacionais dinâmicos e seguros em instituições de ensino tem impulsionado a adoção de práticas que garantam agilidade e padronização na gestão de infraestrutura. Nesse contexto, a Infraestrutura como Código (IaC) apresenta-se como uma abordagem capaz de reduzir erros operacionais e maximizar a eficiência, tratando a infraestrutura física como software. Este trabalho propõe desenvolver e validar um modelo de gerenciamento de infraestrutura virtualizada definida por código, aplicado ao laboratório de redes do Instituto Federal de Rondônia (IFRO), Campus Porto Velho Zona Norte. A pesquisa classifica-se como aplicada e experimental, estruturada sobre uma arquitetura de orquestração centralizada no Semaphore UI. A metodologia consistiu na integração de repositórios privados e na divisão de tarefas em pipelines independentes, utilizando o Terraform para o provisionamento automatizado no hipervisor Proxmox VE, o Ansible para a configuração autônoma de pacotes e o HashiCorp Vault para a injeção dinâmica e segura de credenciais. Os resultados práticos validaram a eficácia da esteira de automação, comprovando a segurança sistêmica por meio do princípio do menor privilégio em APIs. A execução da orquestração registrou um baixo lead time para o provisionamento e a configuração inicial de instâncias LXC. Essa integração garantiu a idempotência do ambiente e eliminou desvios de configuração (configuration drift), entregando nós operacionais padronizados e prontos para uso. Conclui-se que a substituição de processos manuais por este modelo automatizado, auditável e rastreável resolve os gargalos operacionais do laboratório, viabiliza o controle pedagógico seguro e promove a formação de profissionais rigorosamente alinhados à cultura DevOps e às exigências tecnológicas do mercado.

PALAVRAS-CHAVE: automação; infraestrutura como código; virtualização; segurança; DevOps.

ABSTRACT: The growing demand for dynamic and secure computing environments in educational institutions has driven the adoption of practices that ensure agility and standardization in infrastructure management. In this context, Infrastructure as Code (IaC) presents itself as an approach capable of reducing operational errors and maximizing efficiency by treating physical infrastructure as software. This study proposes to develop and validate a code-defined virtualized infrastructure management model, applied to the networking laboratory of the Federal Institute of Rondônia (IFRO), Porto Velho Zona Norte Campus. The research is classified as applied and experimental, structured upon an orchestration architecture centralized in Semaphore UI. The methodology consisted of integrating private repositories and dividing tasks into independent pipelines, using Terraform for automated provisioning on the Proxmox VE hypervisor, Ansible for autonomous package configuration, and HashiCorp Vault for the dynamic and secure injection of credentials. Practical results validated the effectiveness of the automation pipeline, demonstrating systemic security

through the principle of least privilege in APIs. The orchestration execution recorded a low lead time for the provisioning and initial configuration of LXC instances. This integration ensured environment idempotency and eliminated configuration drift, delivering standardized and ready-to-use operational nodes. It is concluded that replacing manual processes with this automated, auditable, and traceable model resolves the laboratory's operational bottlenecks, enables secure pedagogical control, and promotes the training of professionals strictly aligned with DevOps culture and technological market demands.

KEYWORDS: automation; infrastructure as code; virtualization; security; DevOps.

1 INTRODUÇÃO

A nova era da informação, pautada pela automação e pela inteligência artificial, exige uma gestão de infraestrutura de Tecnologia da Informação (TI) cada vez mais moderna e eficiente. Esse cenário decorre da crescente integração entre os diferentes setores da informática e os sistemas de comunicação que, aliados à computação em nuvem, redefinem os padrões operacionais tradicionais (SCHWAB, 2016).

Nesse contexto, segundo Morris (2021), a prática de Infraestrutura como Código (Infrastructure as Code - IaC) surge como a resposta fundamental a esse desafio, permitindo que a infraestrutura seja tratada como software, ou seja, definida, provisionada e gerenciada por meio de código. Essa metodologia possibilita a aplicação de princípios da engenharia de software, como automação, rastreabilidade e consistência, viabilizando mudanças rápidas, seguras e contínuas, ao mesmo tempo em que se alinha à cultura DevOps.

A urgência dessa transição tecnológica justifica-se pelas profundas transformações no mercado de trabalho. A automação tende a substituir tarefas rotineiras, sejam elas manuais ou cognitivas passíveis de codificação, elevando a demanda por habilidades de maior valor analítico e estratégico. O Guia de Ferramentas de Apoio Tecnológico do Ministério Público Militar (MPM, 2022) estima que mais de 81% do trabalho físico previsível, 69% do processamento de dados e 64% das atividades de coleta de informações poderiam ser facilmente automatizados com as tecnologias já disponíveis.

Diante dessa demanda por profissionais capacitados para operar e gerir tais inovações, o Instituto Federal de Rondônia (IFRO), Campus Porto Velho Zona Norte, desempenha um papel institucional estratégico na oferta de educação tecnológica na região. Dentre os cursos ofertados, destaca-se o Curso Superior de Tecnologia (CST) em Redes de Computadores, iniciado em 2017. O curso tem como objetivo formar profissionais de nível superior capazes de responder às necessidades regionais e aos desafios de uma sociedade em contínua transformação (IFRO, 2022). Conforme o Catálogo Nacional de Cursos Superiores de Tecnologia (BRASIL, 2016), o perfil esperado para esse tecnólogo abrange a capacidade de projetar, implantar, gerenciar e integrar redes; avaliar soluções de segurança; documentar projetos de diferentes portes; e propor medidas para a melhoria da qualidade dos serviços prestados.

Para sustentar essa formação de caráter eminentemente prático, o curso conta com um Laboratório de Redes de Computadores, disponibilizado sob o acompanhamento de professores e monitores. O espaço dispõe de hardwares que suportam a instalação de sistemas operacionais e aplicações robustas, além de equipamentos ativos e passivos de rede. Adicionalmente, estão disponíveis softwares para simulações e emulações, incluindo recursos de virtualização e contêinerização, que garantem ao discente a liberdade necessária para a criação de seus próprios sistemas e topologias (IFRO, 2022). Essa infraestrutura representa o ambiente físico sobre o qual recaem as decisões de gerenciamento investigadas no presente trabalho.

Embora situado em um contexto acadêmico, o laboratório do IFRO apresenta características físicas e demandas de processamento equivalentes às de um datacenter de pequeno porte. Por essa razão, este ambiente não deve ser gerido como um laboratório de informática tradicional, mas sim com o rigor operacional de uma infraestrutura corporativa. A matriz do curso exige que o espaço entregue valor às aulas práticas com agilidade e consistência. Contudo, a ausência de ferramentas adequadas de gestão lógica (automação) contradiz a robustez física instalada, criando um gargalo que impede a infraestrutura de cumprir sua função de forma plena. A resolução dessa incompatibilidade exige o abandono de práticas manuais em favor de um modelo operacional definido, integrando a tecnologia aos objetivos da instituição.

Corroborando a urgência dessa transição, Cruz (2020) observa que ambientes provisionados manualmente exigem aproximadamente o dobro das etapas em comparação à automação logica, além de serem altamente suscetíveis a erros humanos que introduzem retrabalho e geram indisponibilidade dos serviços.

Diante dessa problemática, o presente trabalho propõe um modelo de gerenciamento de infraestrutura virtualizada definida por código para o cluster do laboratório de redes do IFRO. O modelo integra a ferramenta Terraform para o provisionamento automatizado, o Ansible para a configuração padronizada e o HashiCorp Vault para a gestão segura de credenciais, utilizando o hipervisor Proxmox VE para a orquestração de contêineres Linux (LXC) — uma tecnologia de virtualização em nível de sistema operacional reconhecida por sua leveza e rápida inicialização. Dessa forma, a pesquisa objetiva investigar e demonstrar a viabilidade da automação como estratégia de modernização, avaliando seus impactos na padronização de

processos, na elevação da segurança sistêmica e na transferência de conhecimento prático alinhado às demandas atuais de inovação tecnológica do mercado.

2 DIAGNÓSTICO DA SITUAÇÃO PROBLEMA E/OU OPORTUNIDADE

O Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), Campus Porto Velho Zona Norte, constitui uma instituição pública de educação profissional, científica e tecnológica com atuação voltada à formação de recursos humanos qualificados para responder às demandas regionais de desenvolvimento. Entre os cursos ofertados pela unidade, destaca-se o Curso Superior de Tecnologia em Redes de Computadores, iniciado em 2017, cuja proposta formativa envolve competências relacionadas ao projeto, à implantação, ao gerenciamento, à integração e à documentação de infraestruturas de rede, bem como à análise de soluções de segurança e à melhoria da qualidade dos serviços tecnológicos.

Para sustentar essa formação prática, o curso conta com um Laboratório de Redes de Computadores, ambiente no qual se desenvolvem atividades de ensino, experimentação e apoio a projetos acadêmicos. O laboratório dispõe de equipamentos de rede, servidores, softwares de virtualização e recursos de conteinerização, o que lhe confere características operacionais próximas às de uma infraestrutura computacional de pequeno porte, ainda que situada em contexto educacional.

Do ponto de vista interno, o laboratório apresenta uma base física relevante para a execução de práticas avançadas, incluindo capacidade para hospedar contêineres e máquinas virtuais em cluster Proxmox VE. Entretanto, a análise do cenário revelou que a robustez da camada física não era acompanhada por um modelo lógico de gerenciamento igualmente maduro, pois a disponibilização de ambientes dependia de procedimentos manuais de criação, configuração e ajuste de acesso, o que reduzia a agilidade do atendimento às demandas acadêmicas e aumentava a suscetibilidade a falhas humanas.

No plano externo, esse diagnóstico se relaciona às exigências contemporâneas do mercado de tecnologia, no qual automação, padronização, segurança e rastreabilidade são atributos cada vez mais valorizados na administração de infraestruturas. Nesse sentido, a literatura mobilizada no trabalho demonstra que práticas baseadas em Infraestrutura como Código (IaC) e em princípios da cultura DevOps se mostram adequadas para enfrentar limitações típicas de ambientes

geridos manualmente, tais como retrabalho, inconsistências entre instâncias, dificuldade de replicação e exposição indevida de credenciais.

A situação do problema identificada, portanto, consiste na inadequação do modelo manual de gerenciamento da infraestrutura virtualizada do laboratório de redes do IFRO frente às necessidades de padronização, escalabilidade, segurança e rapidez exigidas pelas atividades didático-pedagógicas do curso. Embora o ambiente já possuísse recursos tecnológicos suficientes para suportar cenários mais avançados de uso, a ausência de automação e de um fluxo estruturado de provisionamento limitava o aproveitamento pleno dessa capacidade instalada.

Além do problema, o contexto investigado também evidencia uma oportunidade de melhoria e inovação. A implantação de um modelo de gerenciamento de infraestrutura virtualizada definida por código permitiria modernizar a gestão do laboratório, reduzir o tempo de entrega dos ambientes, elevar o controle sobre credenciais e configurações, e, simultaneamente, ampliar o valor pedagógico do espaço ao aproximar os estudantes de ferramentas e práticas efetivamente utilizadas em contextos profissionais de redes, infraestrutura e computação em nuvem.

3 ANÁLISE DA SITUAÇÃO PROBLEMA E PROPOSTAS DE INOVAÇÃO/INTERVENÇÃO/RECOMENDAÇÃO

A análise da situação-problema demonstrou que a principal limitação observada no laboratório de redes do IFRO não estava associada à insuficiência de hardware ou à ausência de um ambiente virtualizado, mas à carência de um modelo lógico de gerenciamento compatível com a complexidade da infraestrutura disponível. Embora o cluster Proxmox VE fornecesse a base necessária para a execução de máquinas virtuais e contêineres, a operacionalização cotidiana permanecia dependente de ações manuais, o que comprometia a padronização dos ambientes e o uso eficiente dos recursos institucionais.

Sob essa perspectiva, a manutenção do processo manual configurava uma primeira alternativa possível, porém inadequada. Esse modelo exigia múltiplas etapas operacionais, elevada intervenção humana e maior propensão a inconsistências, sobretudo na criação de instâncias, na instalação de pacotes e no controle de credenciais, o que se mostra incompatível com os princípios contemporâneos de reprodutibilidade e governança da infraestrutura.

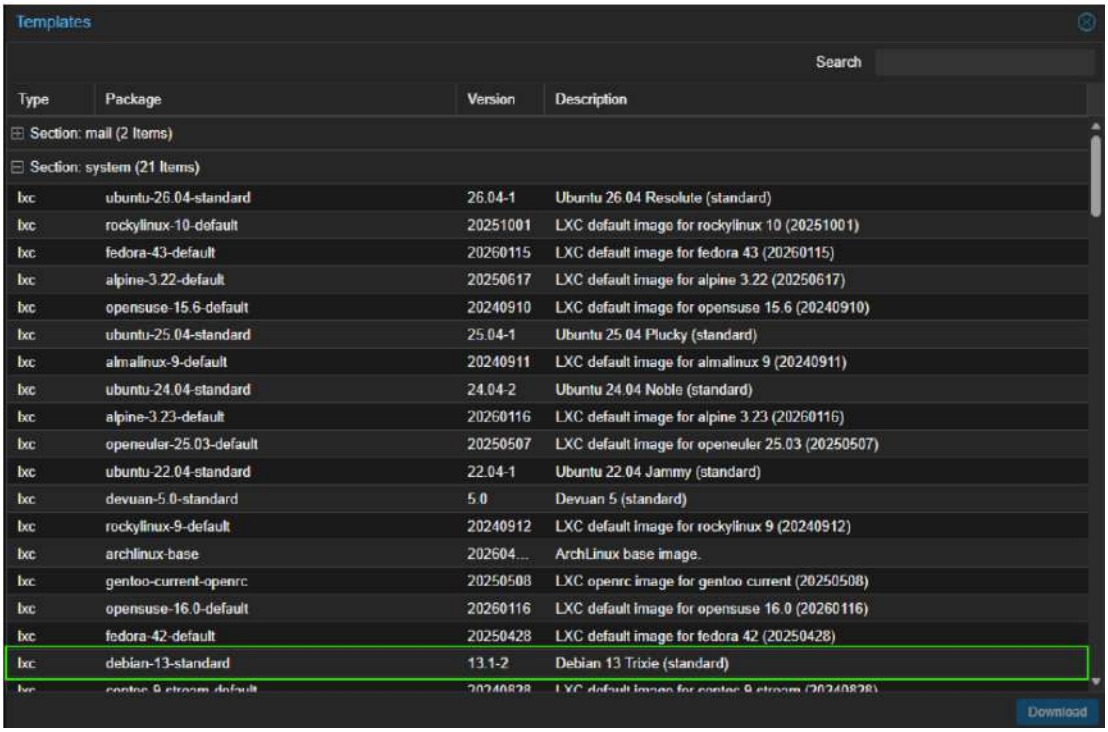
Uma segunda alternativa seria a adoção isolada de apenas uma ferramenta de automação, como Terraform ou Ansible, para solucionar parcialmente o problema. Apesar de representar um avanço em relação ao cenário manual, essa abordagem não atenderia de forma integral às necessidades do laboratório, pois o provisionamento automatizado, a configuração pós-criação e a proteção de segredos exigem funções distintas e complementares. Em outras palavras, a resolução efetiva da situação-problema depende de uma arquitetura integrada, e não de uma automação fragmentada.

Diante disso, a proposta de inovação adotada neste trabalho consistiu na implementação de um modelo integrado de Infraestrutura como Código aplicado ao laboratório de redes do IFRO. A solução foi estruturada com base no hipervisor Proxmox VE como camada de virtualização, no Terraform como mecanismo de provisionamento declarativo de contêineres LXC, no Ansible como ferramenta de configuração idempotente das instâncias, no HashiCorp Vault para a gestão centralizada de credenciais e no Semaphore UI como plataforma de orquestração das rotinas automatizadas.

Do ponto de vista teórico, a escolha dessa arquitetura encontra respaldo nos referenciais que sustentam a importância da padronização, da idempotência, da rastreabilidade e da separação entre definição de infraestrutura, configuração de serviços e gestão segura de segredos. A proposta também dialoga com a cultura DevOps ao reduzir a dependência de ajustes manuais, favorecer o versionamento das mudanças e permitir a repetibilidade dos ambientes provisionados no laboratório.

A construção da proposta ocorreu em etapas encadeadas. Inicialmente, procedeu-se à preparação do ambiente base, com a definição da arquitetura e a seleção da stack tecnológica mais compatível com as demandas do laboratório. Em seguida, foram implementados mecanismos de autenticação e confiança entre os serviços, incluindo a criação de um perfil restrito de API no Proxmox e a adoção de chaves SSH para comunicação segura com as instâncias provisionadas.

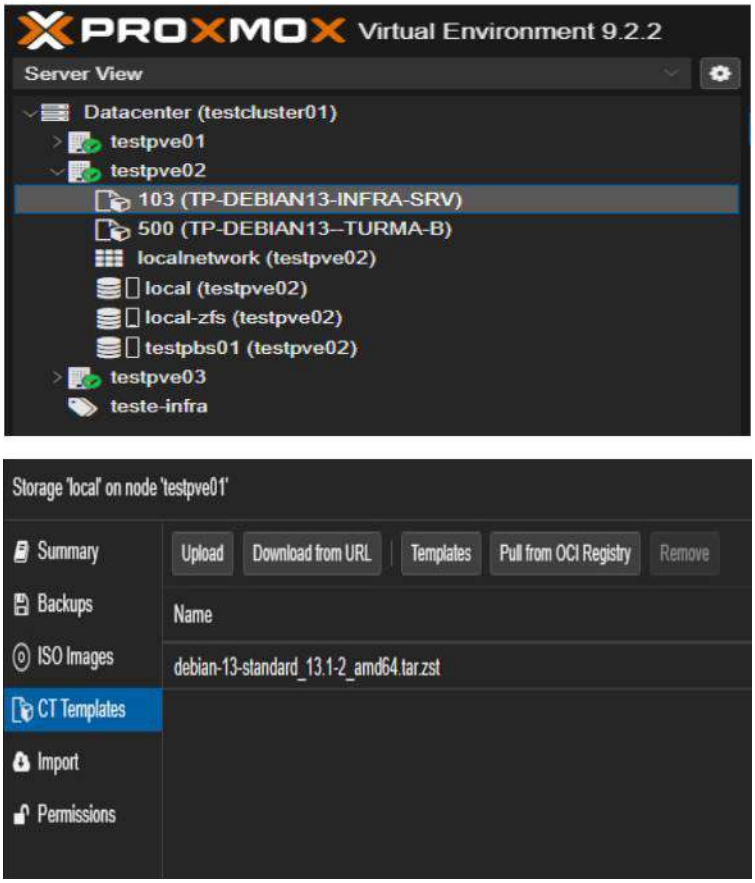
Figura 1 - Lista de template para baixar no Proxmox



Fonte: PRÓPRIA, 2026.

Na etapa seguinte, foi avaliada a estratégia de uso de templates personalizados para criação dos contêineres. Os testes mostraram que essa abordagem ampliava a complexidade do fluxo e reduzia a rastreabilidade das alterações, razão pela qual se optou pela adoção do template original disponibilizado pelo Proxmox, deixando a padronização do ambiente sob responsabilidade do Ansible.

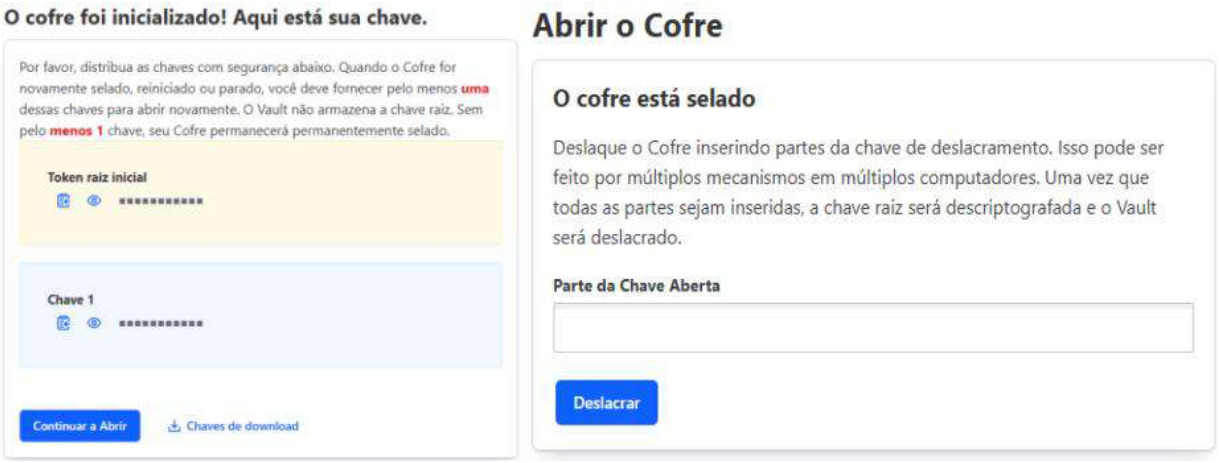
Figura 2 - Preparação do template para a criação dos conteiners



Fonte: PRÓPRIA, 2026.

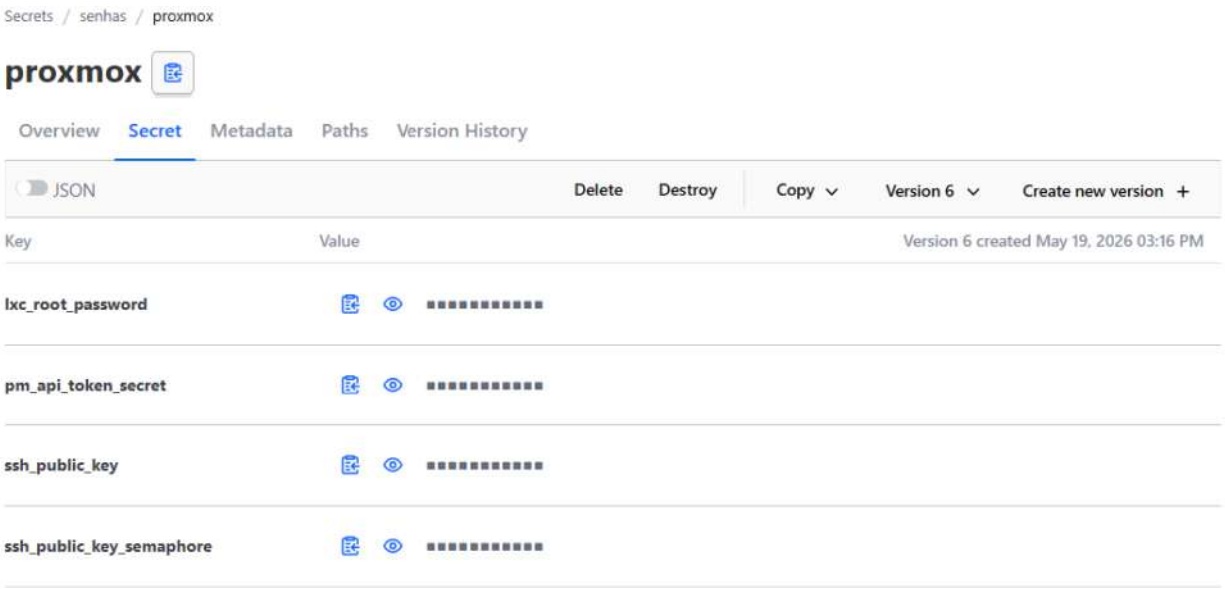
Como parte da camada de segurança da proposta, foi implantado o HashiCorp Vault em um contêiner LXC dedicado, com a finalidade de centralizar a guarda de segredos e impedir a exposição de senhas, chaves e tokens nos arquivos de automação. Essa decisão fortaleceu a governança de credenciais do laboratório e permitiu que o pipeline operasse com maior segurança e auditabilidade.

Figura 3 - (Unseal) manual via chaves mestras e autenticação por Root



Fonte: PRÓPRIA, 2026.

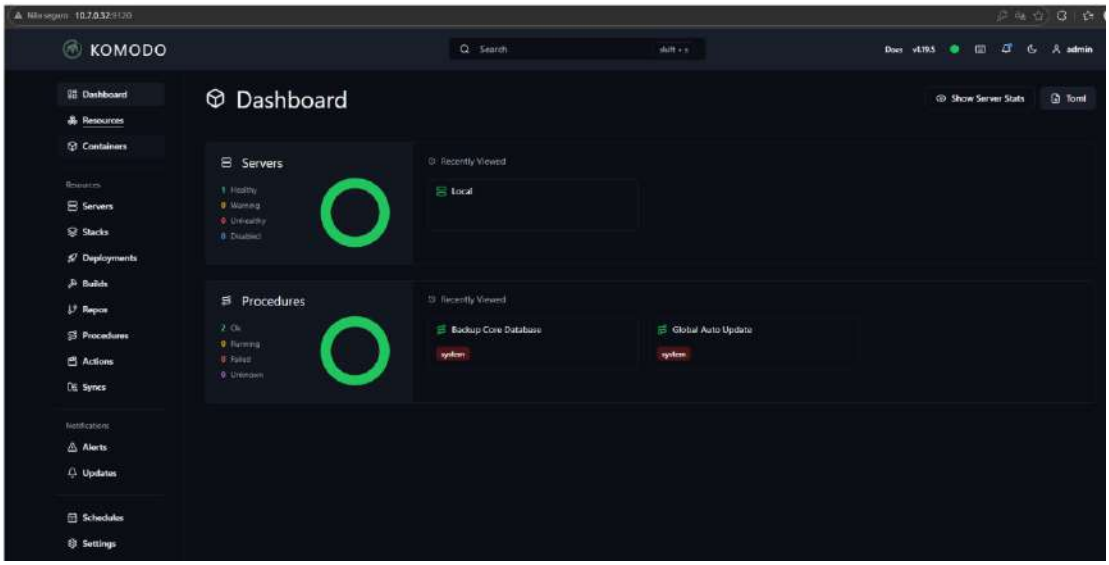
Figura 4 - Interface web Semaphore



Fonte: PRÓPRIA, 2026.

A implementação do ambiente de apoio à orquestração também incluiu a criação de um contêiner LXC voltado à execução de serviços auxiliares em Docker, com destaque para o uso do painel Komodo como instrumento de apoio visual à gestão dos contêineres. Essa etapa contribuiu para organizar a operação do ambiente e facilitar a observação prática das rotinas automatizadas.

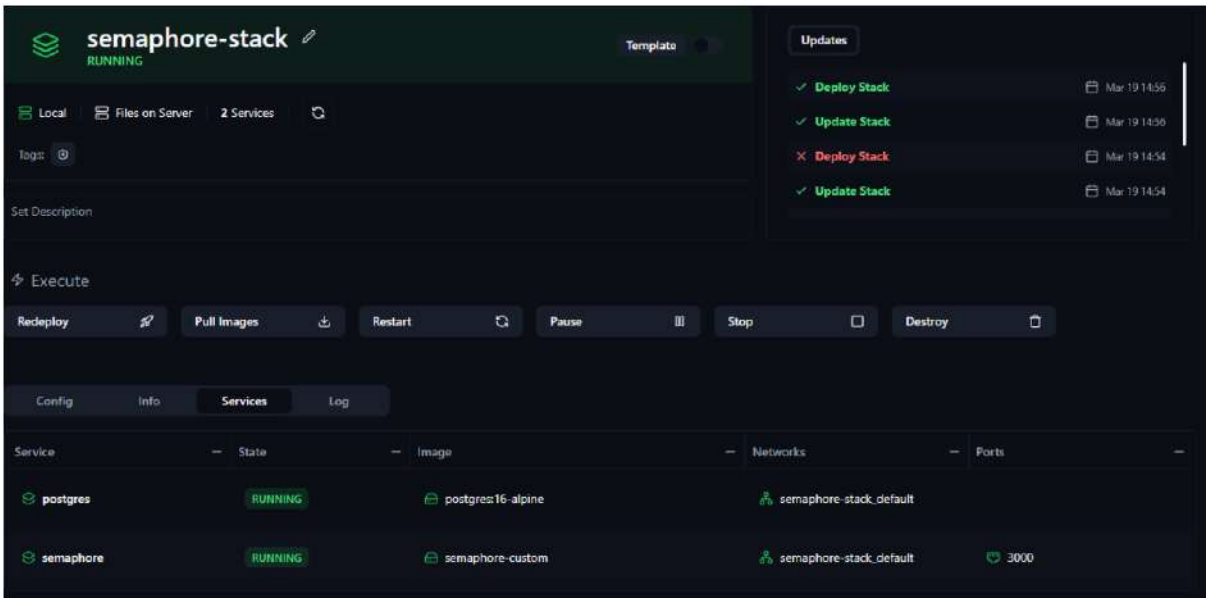
Figura 5 - Dashboard Komodo



Fonte: PRÓPRIA, 2026.

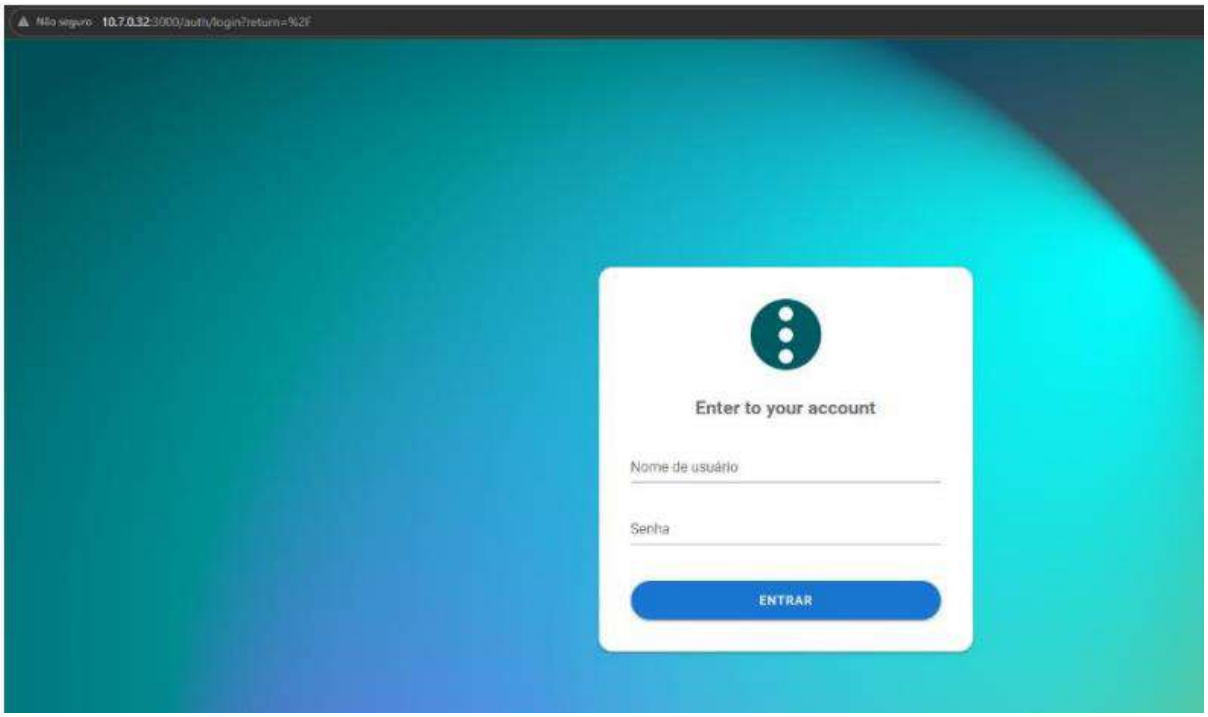
Na sequência, foi implantado o Semaphore UI como núcleo central de orquestração do modelo. Sua instalação foi realizada em uma stack dedicada, com uso de imagem Docker customizada e técnica de multi-stage build, a fim de garantir isolamento de dependências, leveza e melhor controle do ambiente de execução.

Figura 6 - Stack do Semaphore



Fonte: PRÓPRIA, 2026.

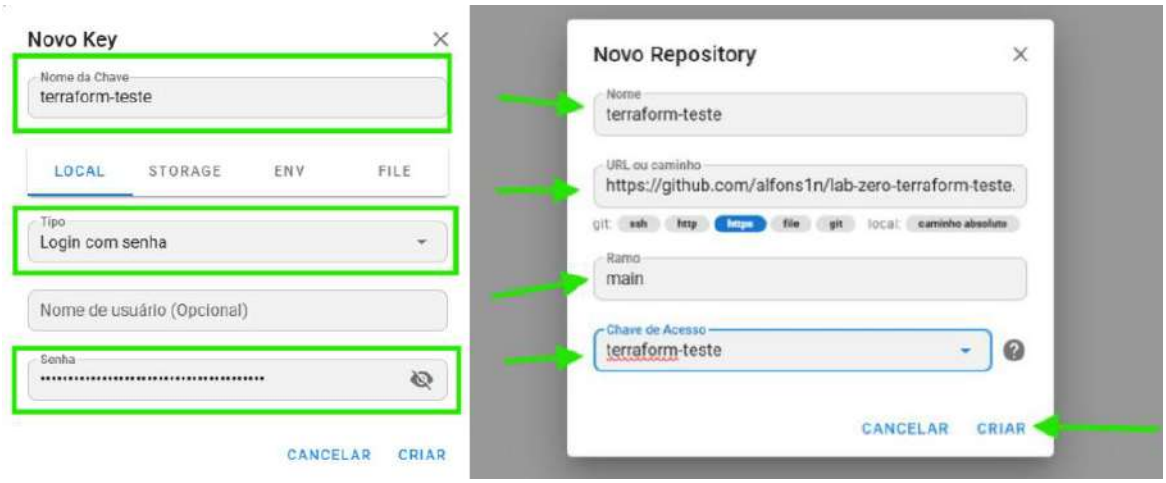
Figura 7 - Interface web Semaphore



Fonte: PRÓPRIA, 2026.

A integração entre Semaphore UI e os repositórios privados do GitHub foi implementada para assegurar versionamento, rastreabilidade e controle de mudanças nos códigos de infraestrutura. Para isso, o trabalho abandonou autenticação por senha e adotou Personal Access Token (PAT), armazenado de forma protegida no ambiente do orquestrador, permitindo o consumo seguro dos repositórios privados.

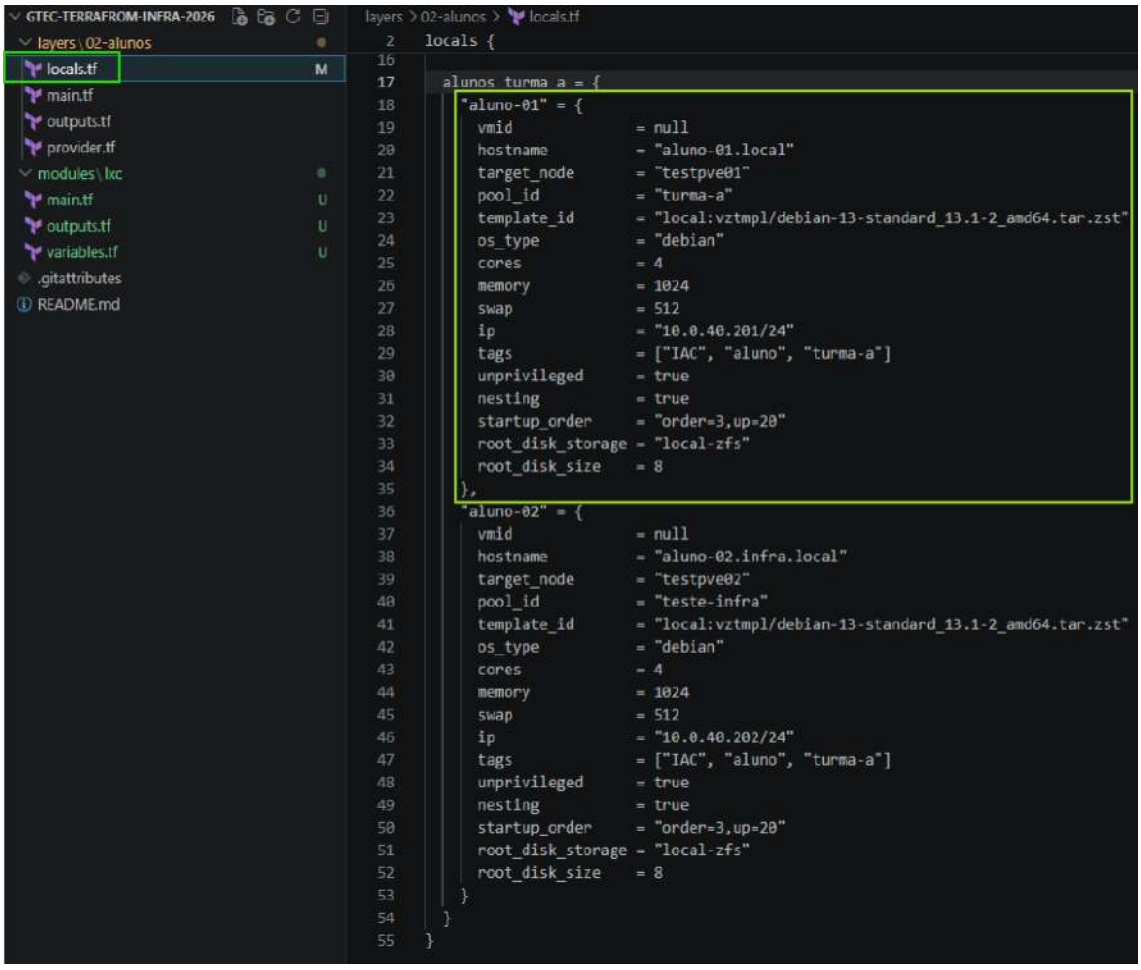
Figura 8 - Parametrização Semaphore



Fonte: PRÓPRIA, 2026.

No plano de provisionamento da infraestrutura, o Terraform foi organizado de forma modular para permitir escalabilidade, legibilidade e reaproveitamento do código. A transição do provider legado Telmate para o provider bpg/proxmox representou um refinamento técnico importante, pois tornou a modelagem dos recursos mais expressiva e compatível com versões mais atuais da API do Proxmox VE.

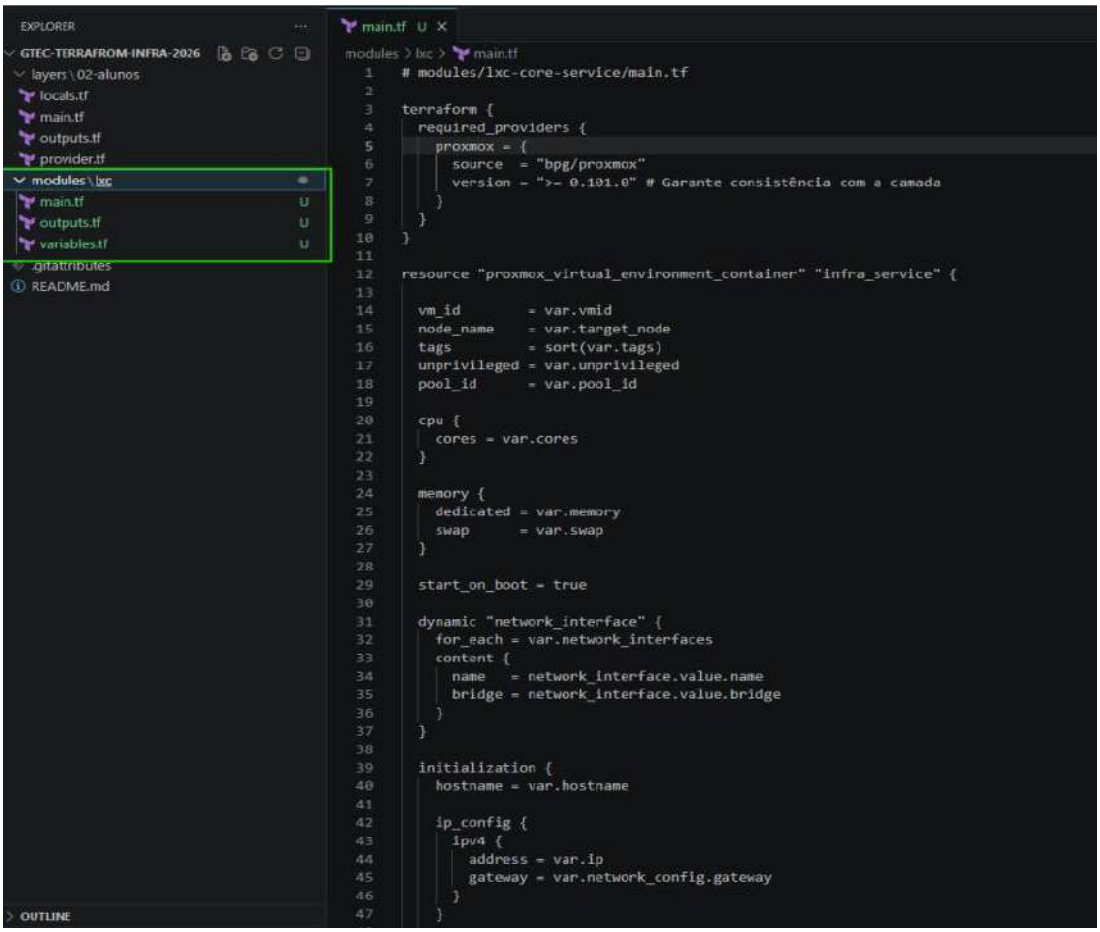
Figura 9 - Bloco de código bpg/proxmox



Fonte: PRÓPRIA, 2026.

A lógica de execução foi dividida em camadas, separando a composição do inventário e dos parâmetros da infraestrutura da lógica bruta de criação dos contêineres. Essa organização modular tornou o modelo mais reutilizável e facilitou a expansão futura do laboratório sem necessidade de duplicação manual de código.

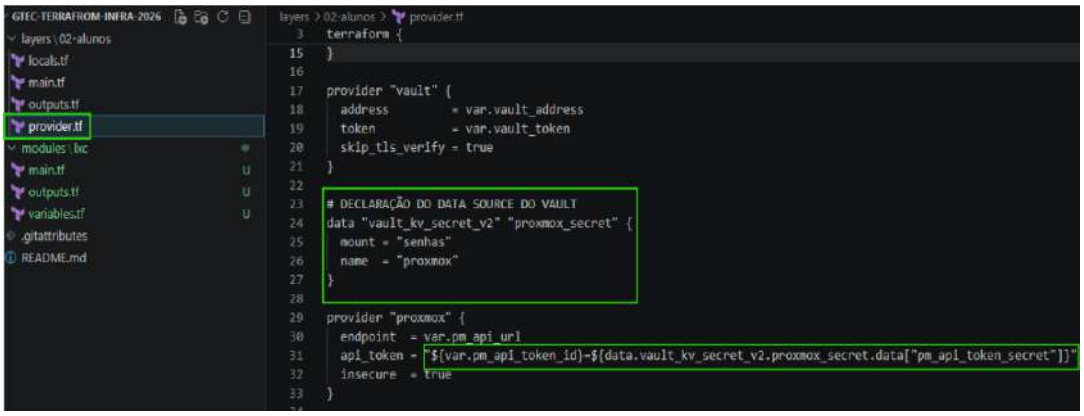
Figura 10 - Módulo de execução



Fonte: PRÓPRIA, 2026.

A segurança do provisionamento foi reforçada pela integração entre Terraform, Vault e Proxmox, de modo que os segredos necessários à autenticação fossem obtidos dinamicamente, sem exposição em texto claro no código-fonte. Essa solução reduziu riscos de vazamento e tornou o fluxo mais aderente às boas práticas de DevOps.

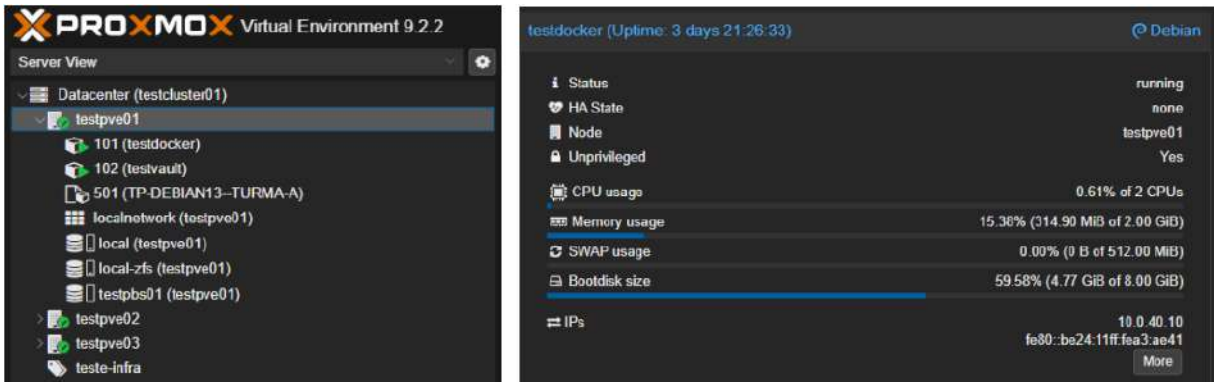
Figura 11 - Provider Proxmox



Fonte: PRÓPRIA, 2026.

Após a consolidação da arquitetura de provisionamento, a proposta foi validada por meio da execução do pipeline completo no Semaphore UI, integrando repositório privado, Vault e cluster Proxmox VE. Essa validação demonstrou a viabilidade funcional do modelo no contexto do laboratório e permitiu verificar a criação automatizada das instâncias com rastreabilidade operacional.

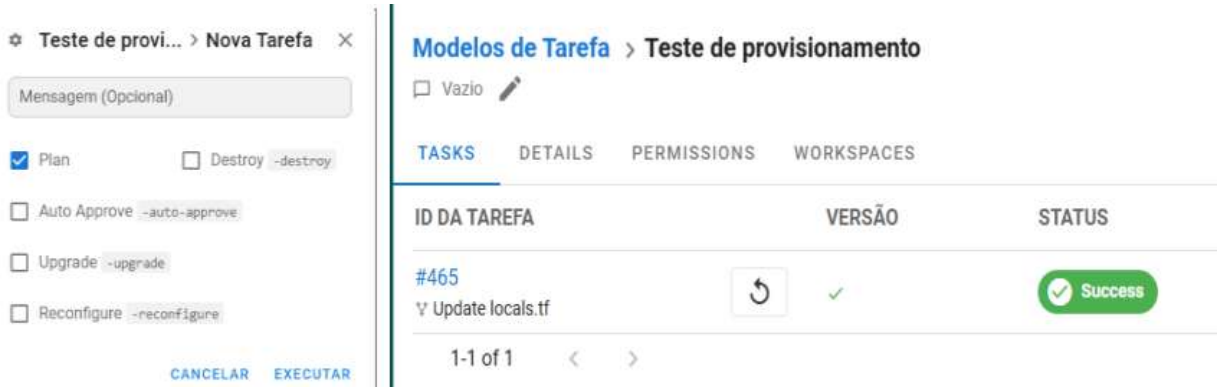
Figura 12 - Cluster de virtualização Proxmox VE



Fonte: PRÓPRIA, 2026.

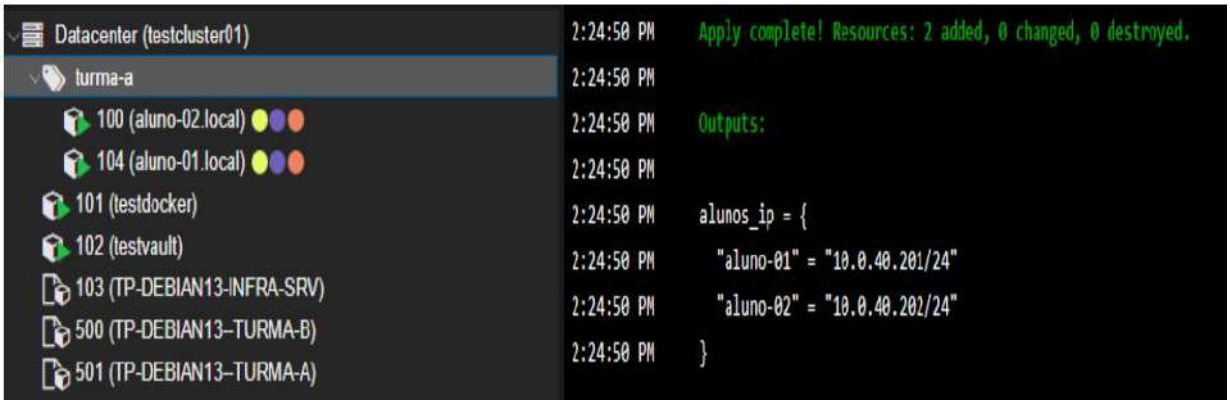
O Terraform Plan foi utilizado como etapa prévia de conferência das alterações a serem aplicadas, permitindo maior previsibilidade sobre a infraestrutura declarada. Na sequência, a execução do apply resultou na criação automatizada das instâncias e na geração de saídas com os endereços IP dos contêineres provisionados.

Figura 13 - Plano simulado (Terraform Plan)



Fonte: PRÓPRIA, 2026.

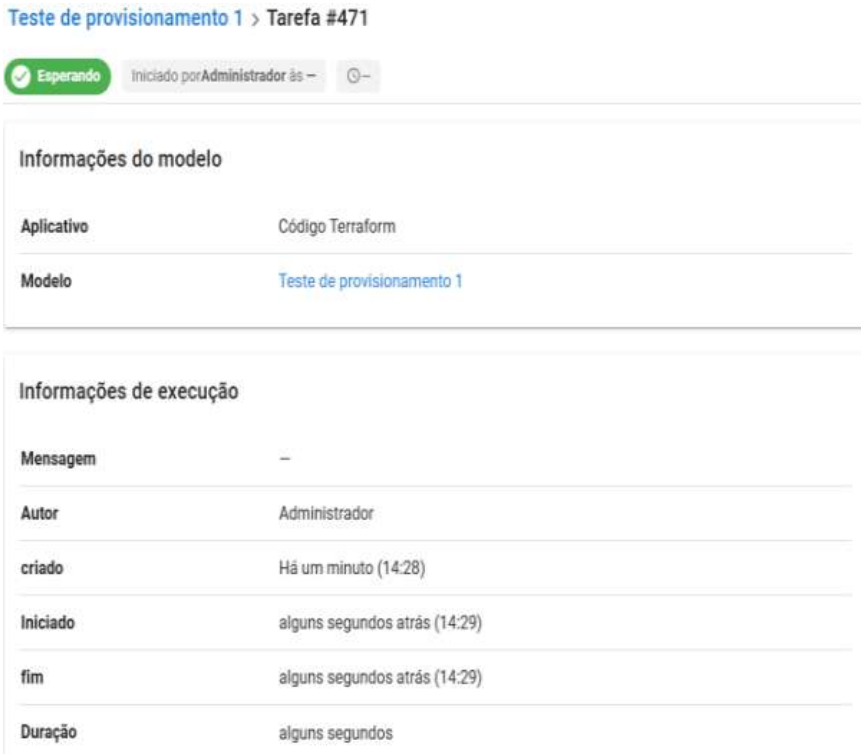
Figura 14 - Provisionamento automático das instâncias



Fonte: PRÓPRIA, 2026.

Quanto ao desempenho operacional, os testes registraram tempo reduzido para a criação inicial das instâncias, indicando ganho de agilidade em relação ao processo manual. Ainda assim, recomenda-se evitar formulações superlativas, substituindo expressões como “extrema eficiência” por afirmações mais objetivas e compatíveis com a evidência observada em laboratório.

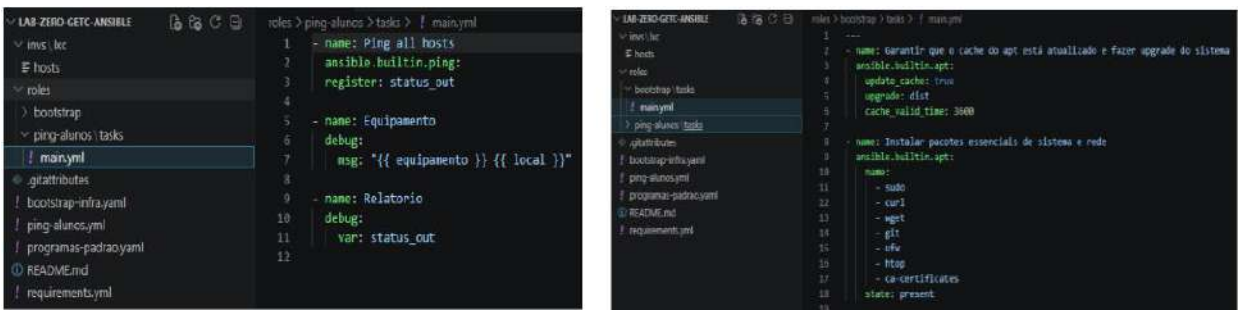
Figura 15 - Lead time teste



Fonte: PRÓPRIA, 2026.

Na camada de configuração dos ambientes, o Ansible foi utilizado para transformar os contêineres provisionados em instâncias padronizadas, aptas ao uso acadêmico. Sua arquitetura foi organizada em roles, playbooks e inventários, com destaque para a role de bootstrap, responsável por tarefas iniciais como atualização de repositórios, instalação de dependências e criação de identidade sistêmica do orquestrador.

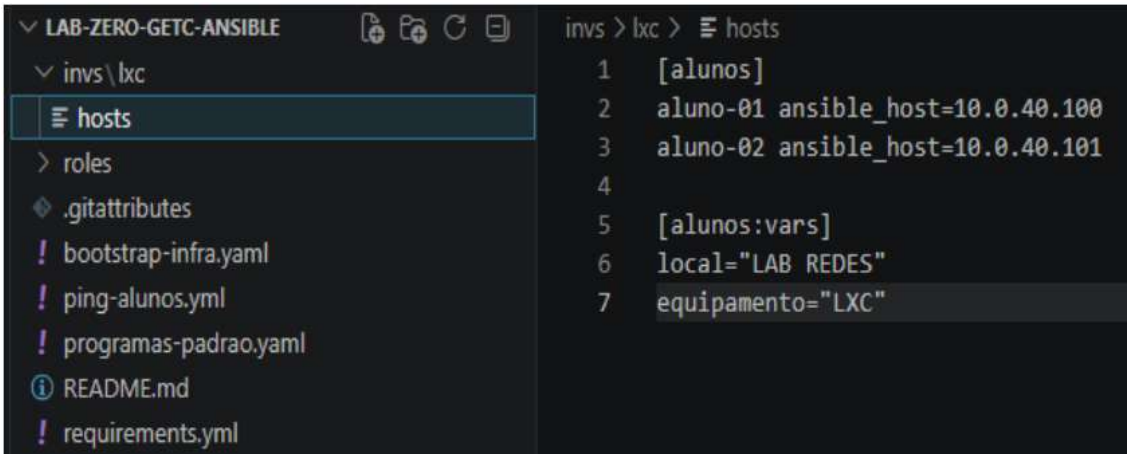
Figura 16 - Arquitetura do Ansible



Fonte: PRÓPRIA, 2026.

No que se refere à estratégia de inventário, adotou-se inicialmente o inventário estático, e essa decisão foi justificada por razões pedagógicas, de estabilidade e de validação humana prévia. Em termos práticos, o inventário estático consiste em um arquivo previamente definido com a lista de hosts e seus parâmetros de acesso, ao passo que o inventário dinâmico é gerado automaticamente por scripts, plugins ou APIs no momento da execução. Para o contexto do laboratório, a escolha pelo inventário estático mostrou-se mais adequada à necessidade de controle sobre o fluxo “provisionamento, validação e configuração”.

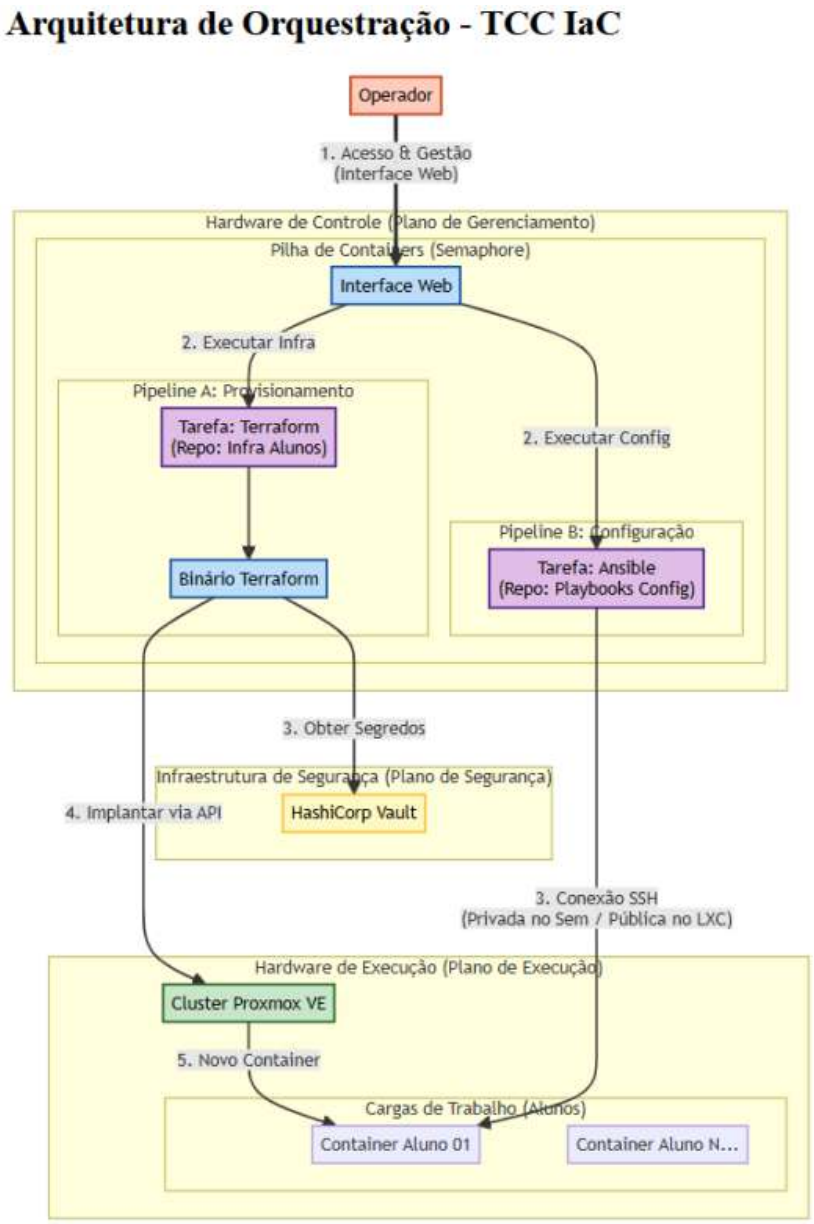
Figura 17 - Provisionamento automático das instâncias



Fonte: PRÓPRIA, 2026.

Como síntese analítica, a proposta demonstrou potencial para reduzir o tempo de provisionamento, padronizar ambientes, centralizar credenciais sensíveis e ampliar a reprodutibilidade do laboratório. Além disso, a documentação técnica produzida e o versionamento dos arquivos em repositório privado reforçam o caráter replicável da solução e sua utilidade para outros contextos educacionais ou institucionais com demandas semelhantes.

Figura 18 - Arquitetura do modelo



Fonte: PRÓPRIA, 2026.

4 CONCLUSÕES E CONTRIBUIÇÃO TECNOLÓGICA E/OU SOCIAL

A análise desenvolvida permitiu concluir que a implementação de um modelo de gerenciamento de infraestrutura virtualizada definida por código é tecnicamente viável e pertinente para o contexto do Laboratório de Redes de Computadores do IFRO, Campus Porto Velho Zona Norte. A proposta respondeu à situação do problema

identificada ao substituir práticas manuais por um fluxo automatizado, rastreável e mais padronizado de provisionamento e configuração da infraestrutura.

Em relação ao objetivo geral, verificou-se que a integração entre Terraform, Ansible, HashiCorp Vault, Semaphore UI e Proxmox VE constituiu uma solução coerente para automatizar o gerenciamento do laboratório e elevar o controle sobre os ambientes disponibilizados para uso acadêmico. Quanto aos objetivos específicos, observou-se avanço na automação do provisionamento de contêineres, na padronização das configurações internas, na centralização segura de credenciais e na consolidação de um modelo aplicável ao contexto institucional analisado.

A principal contribuição tecnológica do trabalho está na proposição e validação de uma arquitetura de automação que pode ser replicada, adaptada e evoluída em ambientes laboratoriais com características semelhantes. Já a contribuição social e educacional reside no fortalecimento da formação prática dos estudantes, que passam a ter contato com ferramentas, processos e padrões efetivamente utilizados em cenários profissionais de administração de infraestrutura.

Além de beneficiar a gestão interna do laboratório, a proposta também amplia o potencial institucional do IFRO ao alinhar ensino, experimentação e inovação tecnológica em um mesmo ambiente. Como desdobramento futuro, recomenda-se a continuidade dos testes em produção, a mensuração mais ampla de indicadores operacionais e a expansão do modelo para novas demandas de observabilidade, monitoramento e governança da infraestrutura.

5 AGRADECIMENTOS

O presente trabalho foi realizado e implementado com o apoio do Grupo de Pesquisa em Tecnologia, Comunicação e Governança — GTEC, do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO) — Campus Porto Velho Zona Norte.

REFERÊNCIAS

ALBUQUERQUE, P. H. M. et al. **Automação e o futuro do trabalho no Brasil**. Brasília: IPEA, 2019.

BPG. **Provedor Terraform Proxmox**. Registro Terraform, 2024. Disponível em: https://registry.terraform.io/providers/bpg/proxmox/latest/docs. Acesso em: 28 nov. 2025.

BRASIL. Ministério da Educação. **Catálogo Nacional de Cursos Superiores de Tecnologia**. Brasília: MEC, 2016. Disponível em: https://www.gov.br/mec/pt-br/media/seb-1/pdf/catalogo_cnct/CNCST__2016_a.pdf. Acesso em: 8 jul. 2026.

CRUZ, Renã Freitas da. **Infraestrutura por código: uma alternativa para gerenciamento de infraestrutura de redes de computadores**. Porto Alegre: Alcides Maya Faculdade e Escola Técnica, 2020. Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores).

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GRAGLIA, J. M.; LAZZARESCHI, N. **Indústria 4.0 e o futuro do trabalho**. Revista de Ciências Sociais, v. 1, 2018.

HASHICORP. **Retribuindo o favor, 5 vezes mais rápido: a empresa número 1 em pagamentos eletrônicos do Brasil usa a infraestrutura como código do Terraform da HashiCorp para lucrar com um tempo de lançamento no mercado 5 vezes mais rápido**. [S. l.]: HashiCorp. Disponível em: https://www.hashicorp.com/resources/cielo-infrastructure-as-code-terraform. Acesso em: 28 nov. 2025.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA (IFRO). **Projeto Pedagógico do Curso Superior de Tecnologia em Redes de Computadores – Campus Porto Velho Zona Norte**. Porto Velho: IFRO, 2022. Disponível em: https://cursos.ead.ifro.edu.br/pluginfile.php/1/theme_boost_union/additionalresources/0/arq_PPC_REDES_2022.pdf. Acesso em: 8 jul. 2026.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). **Mercado de trabalho e desigualdade no Brasil**. Brasília: IPEA, 2012.

KIM, Gene et al. **Manual de DevOps: como obter agilidade, confiabilidade e segurança em organizações tecnológicas**. Rio de Janeiro: Alta Books, 2018.

LIMA, Jonatas Ferreira de. **Terrascratch: aprendendo Terraform de maneira interativa**. Campina Grande: Universidade Federal de Campina Grande, 2024.

Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) — UFCG, CEEI, 2024.

MINISTÉRIO PÚBLICO MILITAR (MPM). **Guia de ferramentas de apoio tecnológico**. Brasília: MPM, 2022.

MORRIS, Kief. **Infraestrutura como Código: sistemas dinâmicos para a era da nuvem**. 2. ed. Sebastopol: O'Reilly Media, 2021.

MORRIS, Kief. **Infraestrutura como código: projetando e distribuindo sistemas dinâmicos para a era da computação em nuvem**. 3. ed. São Paulo: Novatec Editora, 2025.

NOGUEIRA, M.; SEABRA, M.; KÓS, J. **Dupla jornada no ensino superior**. Revista Educação e Sociedade, 2023.

ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL (OMPI). **Índice Global de Inovação 2024: desvendando o potencial do empreendedorismo social**. Genebra: OMPI, 2024.

PADILHA, Felipe. **Scripts: Usuário Terraform Proxmox**. GitHub, 2024. Disponível em: https://raw.githubusercontent.com/padilhafe/scripts/refs/heads/main/proxmox/terraform_user.sh. Acesso em: 28 nov. 2025.

PROXMOX SERVER SOLUTIONS GMBH. **Proxmox Virtual Environment documentation**. Vienna: Proxmox, 2024. Disponível em: https://pve.proxmox.com/pve-docs. Acesso em: 8 jul. 2026.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Édipro, 2016.
TELMATE. **Provedor Terraform Proxmox**. Registro Terraform. Disponível em: https://registry.terraform.io/providers/Telmate/proxmox/latest/docs. Acesso em: 28 nov. 2025.

VERAS, Manoel. **Datacenter: componente central da infraestrutura de TI**. Rio de Janeiro: Brasport, 2009.

VERAS, Manoel. **Gestão da tecnologia da informação: o modelo das cinco dimensões**. Rio de Janeiro: Ciência Moderna, 2010.

WEILL, Pedro; ROSS, Jeanne W. **Governança de TI: como as empresas mais lucrativas gerenciam os investimentos em tecnologia**. São Paulo: M. Books, 2010.

WEILL, Pedro; ROSS, Jeanne W.; ROBERTSON, David C. **Arquitetura de TI como estratégia empresarial**. Tradução de Roger Maioli dos Santos. São Paulo: M. Books, 2008.