DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Segurança de Autenticação, Dados e Comunicação em Sistemas HPC (High Performance Computing)

Jaime de Melo Gama da Silva

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Segurança de Autenticação, Dados e Comunicação em Sistemas HPC (High Performance Computing)

Jaime de Melo Gama da Silva

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Clóvis Neumann, FT/UnB
Orientador

Prof. Dr. Georges Daniel Amvame Nze, FT/UnB
Examinador Interno

Prof. Dr. Caio Moura Daoud, FT/UnB
Examinador Externo

PUBLICAÇÃO: PPEE.MP.107 BRASÍLIA-DF, JANEIRO- 2026

FICHA CATALOGRÁFICA

DE MELO GAMA DA SILVA, JAIME
Segurança de Autenticação, Dados e Comunicação em Sistemas HPC (High Performance Computing) [Distrito Federal] 2026.
xvi, 72 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2026).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1. High Performance Computing (HPC) 2. SSH Authentication
3. Digital Certificates 4. Credential Management
I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

SILVA, J.M.G. (2026). *Segurança de Autenticação, Dados e Comunicação em Sistemas HPC (High Performance Computing)* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 72 p.

CESSÃO DE DIREITOS

PUBLICAÇÃO: PPEE.MP.107 BRASÍLIA-DF, JANEIRO- 2026

Jaime de Melo Gama da Silva
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Com a mais profunda gratidão e amor incondicional, dedico esta Dissertação à minha família, o alicerce fundamental que sustenta toda a minha jornada. Em um destaque especial, ao meu amado filho Heitor e à minha incomparável esposa Yasmin, que são a minha âncora nos momentos de tempestade e a maior inspiração para transcender os limites do conhecimento. É no amor de vocês que encontro a força e o propósito. Aos colegas e amigos, o meu sincero reconhecimento pelo apoio inestimável, pela compreensão da ausência e pelo incentivo constante que me acompanharam em cada etapa deste desafiador percurso acadêmico.

AGRADECIMENTOS

A conclusão desta etapa não representa um esforço individual, mas a materialização de um ideal de progresso contínuo, nutrido e incentivado por uma inestimável rede de apoio. Em primeiro lugar, expresso minha mais profunda gratidão aos meus pais, que desde a infância incutiram o valor do estudo e acolheram a incessante curiosidade, transformando o espírito do "garoto dos muitos porquês" em uma busca contínua por conhecimento. O apoio incondicional e incentivo constante constituíram o alicerce fundamental desta jornada.

A oportunidade de cursar o Mestrado Profissional em Segurança Cibernética em Computação de Alto Desempenho (HPC) na Universidade de Brasília (UnB) foi crucial para a concretização deste trabalho. Meu reconhecimento estende-se à Comissão Coordenadora e à prestativa Secretaria do Programa de Pós-Graduação em Engenharia Elétrica (PPEE/UnB), pelo suporte administrativo e logístico.

Aos docentes, que com generosidade e rigor guiaram e moldaram a visão técnica e científica desta dissertação, expresso minha sincera gratidão. Ao Professor Doutor Clóvis Neumann pelas suas orientações, ao Professor Doutor Robson Albuquerque, por iluminar o caminho e desvendar o porquê fundamental e a relevância estratégica da cibersegurança. Ao Professor Doutor Carlos André, por suas orientações precisas que pavimentaram o caminho para publicações acadêmicas. Ao Professor Doutor Daniel Café, por ser um mentor excepcional, sempre disponível e com uma participação ativa e inspiradora no desenvolvimento deste trabalho. Ao Professor Doutor Rômulo Santos, pelo apoio constante e dedicação em auxiliar o autor nos estudos, sempre com profundidade e clareza. Ao Professor Doutor Georges, cujo vasto conhecimento técnico e excelência didática foram inestimáveis, reforçando o rigor científico da pesquisa.

Aos colegas e amigos do PPEE/UnB, o agradecimento é dedicado pelo estímulo intelectual, pelo ambiente colaborativo e pelo suporte mútuo que tornou a experiência do Mestrado mais produtiva. Finalmente, e de forma mais pessoal, agradeço imensamente a minha esposa. Sua compreensão inabalável, paciência e o suporte emocional durante as incontáveis horas dedicadas a este trabalho, em detrimento do convívio diário, representaram o verdadeiro motor para a conclusão desta dissertação.

RESUMO

A segurança em sistemas de Computação de Alto Desempenho (HPC) tem se tornado um tema central diante do avanço das infraestruturas distribuídas e do aumento do compartilhamento de dados científicos sensíveis. Este trabalho propõe e avalia um modelo de autenticação segura baseado em certificados digitais emitidos por uma autoridade certificadora interna (SSH-CA), aliado à autenticação multifator (2FA), aplicado a um cluster multiusuário de HPC. O estudo parte de um diagnóstico de vulnerabilidades em um ambiente que utilizava chaves estáticas e avança para a implementação de uma arquitetura federada, inspirada em diretrizes de segurança da NIST e em práticas adotadas em infraestruturas científicas internacionais. A metodologia combina mapeamento bibliográfico sistematizado e experimentação prática, integrando princípios de identidade federada, proveniência científica e criptografia pós-quântica.

Os resultados indicam que a substituição de credenciais persistentes por certificados efêmeros melhora significativamente a rastreabilidade e reduz riscos associados à exposição de chaves, mantendo impacto mínimo sobre o desempenho operacional. A integração com autenticação de segundo fator reforça o controle de acesso e a revogabilidade de certificados, enquanto o monitoramento contínuo de logs e fluxos SSH permitem auditoria e detecção de anomalias em tempo real. A análise comparativa demonstra que abordagens de identidade federada e autenticação adaptativa podem ser incorporadas de forma incremental a clusters já em operação, sem comprometer latência, throughput ou escalabilidade.

Conclui-se que a aplicação de padrões de segurança compatíveis com as recomendações da NIST, em especial os referentes a controle de acesso, gestão de credenciais e governança de identidade, é viável e benéfica para ambientes HPC modernos. O trabalho contribui para o amadurecimento da discussão sobre segurança em supercomputação, propondo um referencial técnico que une desempenho, rastreabilidade e confiança digital em ecossistemas científicos distribuídos.

Palavras-chave: Computação de Alto Desempenho; Autenticação Federada; Certificados Digitais; NIST; 2FA; Segurança em HPC; Governança de Identidade; Proveniência Científica.

ABSTRACT

Security in High-Performance Computing (HPC) systems has become a central concern due to the rapid expansion of distributed infrastructures and the growing exchange of sensitive scientific data. This work proposes and evaluates a secure authentication model based on digital certificates issued by an internal certification authority (SSH-CA), combined with two-factor authentication (2FA), applied to a multi-user HPC cluster. The study begins with a diagnosis of vulnerabilities in an environment that previously relied on static SSH keys and advances toward the implementation of a federated architecture inspired by NIST security guidelines and practices adopted in international scientific infrastructures. The methodology combines

a systematic literature mapping and experimental validation, integrating principles of federated identity, scientific data provenance, and post-quantum cryptography.

The results indicate that replacing persistent credentials with ephemeral certificates significantly improves traceability and reduces risks associated with key exposure, while maintaining minimal impact on system performance. The integration of two-factor authentication strengthens access control and certificates revocability, whereas continuous monitoring of SSH logs and flows enables real-time auditing and anomaly detection. Comparative analysis demonstrates that federated identity and adaptive authentication approaches can be incrementally incorporated into existing clusters without compromising latency, throughput, or scalability.

It is concluded that applying security standards consistent with NIST recommendations, particularly those related to access control, credential management, and identity governance, is both feasible and beneficial for modern HPC environments. This work contributes to the advancement of secure supercomputing by proposing a technical framework that unites performance, traceability, and digital trust across distributed scientific ecosystems.

Keywords: High-Performance Computing; Federated Authentication; Digital Certificates; NIST; Two-Factor Authentication; HPC Security; Identity Governance; Scientific Provenance.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

A Computação de Alto Desempenho (HPC — *High-Performance Computing*) consolidou-se como um dos eixos estruturantes da inovação científica e tecnológica contemporânea. Ao viabilizar o processamento de dados em escala massiva e a execução de cálculos complexos em tempo reduzido, o HPC tornou-se elemento essencial para a formulação, simulação e validação de hipóteses em áreas críticas do conhecimento humano. Sua presença é hoje indispensável em domínios que vão desde a previsão meteorológica e o desenvolvimento de novos fármacos até a análise genômica, a modelagem molecular, o aprendizado profundo e a simulação de fenômenos físicos de alta complexidade. Esses ambientes computacionais não apenas aumentam a precisão e a reprodutibilidade dos experimentos, como também promovem uma transformação estrutural na forma de produzir ciência, permitindo que a exploração científica se torne mais preditiva, escalável e colaborativa.

Murugan et al. (Murugan et al. 2021) destacam que a evolução do paralelismo, aliada ao aumento exponencial da densidade de núcleos de processamento e à expansão das arquiteturas heterogêneas, consolidou o HPC como principal vetor de avanço em ciência e engenharia moderna. Nesse contexto, as infraestruturas computacionais devem ser capazes de executar bilhões ou até trilhões de operações por segundo, sustentando fluxos contínuos de dados e simulações de alta fidelidade. Cano Aguilera et al. (Aguilera et al. 2024) complementam essa visão ao enfatizar que tais sistemas, ao mesmo tempo em que são projetados para desempenho máximo e latência mínima, tornam-se progressivamente suscetíveis a ameaças de segurança e vulnerabilidades operacionais. Essa dualidade entre eficiência e exposição impõe a necessidade de novos mecanismos de proteção criptográfica, autenticação federada e controle de acesso contextual, capazes de preservar integridade e confidencialidade sem comprometer a performance.

Os ambientes de HPC operam sobre infraestruturas altamente especializadas, compostas por milhares de núcleos de processamento, unidades de GPU e interconexões de altíssima velocidade, todas projetadas para maximizar o *throughput* e minimizar o tempo de resposta. Tais sistemas lidam com volumes massivos de dados científicos e computacionais, distribuídos em múltiplos nós, e exigem gerenciamento sofisticado de recursos e comunicação entre processos. Bort et al. (Bort et al. 2022) exemplificam esse cenário ao demonstrar o uso de clusters de GPU e redes otimizadas para o treinamento de modelos de *deep learning*, reduzindo drasticamente o tempo de convergência de modelos complexos e evidenciando que a eficiência computacional é determinante para viabilizar experimentos em escala industrial ou científica.

À medida que a Computação de Alto Desempenho se torna mais poderosa, interconectada e essencial para a pesquisa contemporânea, cresce proporcionalmente a complexidade de garantir os princípios clássicos de segurança da informação: confidencialidade, integridade, disponibilidade e rastreabilidade. Pleiter (Pleiter 2020) projeta que os sistemas da próxima década serão ainda mais heterogêneos e orientados a fluxos massivos de dados interinstitucionais, demandando abordagens arquitetônicas integradas que conciliem desempenho, interoperabilidade e segurança. Isso implica uma revisão dos paradigmas de confiabilidade, autenticação e controle em infraestruturas científicas de grande porte.

A expansão de áreas emergentes como modelagem matemática avançada, biologia computacional e topologia computacional reforça que as novas fronteiras da pesquisa dependem de infraestruturas computacionais resilientes e de mecanismos de proteção adaptáveis (Shyamal 2025). A tendência é a integração progressiva de arquiteturas híbridas que combinam CPUs, GPUs e aceleradores especializados, formando ecossistemas cada vez mais complexos e distribuídos. Tais transformações ampliam o potencial científico, mas também multiplicam os vetores de risco, especialmente quando recursos e dados sensíveis são compartilhados entre múltiplos usuários ou instituições.

Historicamente, o foco no desempenho absoluto orientou o desenvolvimento da HPC. (Schulthess 2019) observa que a busca incessante por eficiência e previsibilidade temporal levou à criação de bibliotecas de comunicação otimizadas, protocolos de baixa latência e arquiteturas paralelas capazes de reduzir sobrecargas computacionais. Contudo, essa ênfase no desempenho frequentemente ocorreu em detrimento de mecanismos de segurança mais robustos. Assim, formaram-se sistemas extremamente eficientes, porém vulneráveis, especialmente em ambientes multiusuário e colaborativos, onde a ausência de políticas integradas de autenticação e rastreabilidade abre espaço para ataques, falhas de isolamento e acessos indevidos.

Liu et al. (Liu et al. 2021) destacam que a convergência entre HPC e inteligência artificial, particularmente em aplicações de descoberta de fármacos e modelagem molecular, amplia a superfície de ataque e introduz novos desafios relacionados à integridade de modelos e à proteção de dados sensíveis. A crescente dependência de fluxos automatizados de aprendizado de máquina, frequentemente interligados a sistemas de HPC, evidencia que a segurança deve evoluir em sincronia com o desempenho computacional, evitando que a proteção se torne um gargalo ou uma barreira à escalabilidade.

A consolidação do modelo de *High-Performance Computing as a Service* (HPCaaS), impulsionado pela integração entre supercomputadores e nuvens privadas ou públicas, representa uma nova etapa na evolução da HPC e, simultaneamente, uma ampliação das vulnerabilidades associadas à virtualização e à interconectividade. Nesse contexto, a segurança deixa de ser tratada como um componente periférico e passa a ser uma dimensão arquitetural essencial. Koleini e Pahlevanzadeh (Koleini e Pahlevanzadeh 2024) apontam que ambientes federados de HPC demandam autenticação multifatorial, mecanismos de confiança verificável e políticas de rastreabilidade contínua, de modo a assegurar a integridade e a interoperabilidade entre domínios distribuídos. Essa abordagem estabelece uma base de confiança interinstitucional, indispensável para a pesquisa colaborativa global.

Outro fator que redefine o paradigma da segurança em HPC é o advento da computação quântica. Cano Aguilera et al. (Aguilera et al. 2024) alertam que algoritmos criptográficos clássicos podem se tornar vulneráveis frente à capacidade de processamento de computadores quânticos. A transição para esquemas pós-quânticos, embora necessária, representa um desafio considerável devido ao impacto potencial na performance. O estudo dos autores apresenta evidências experimentais de que algoritmos pós-quânticos selecionados pelo NIST podem ser aplicados em unidades de processamento de dados (DPUs) mantendo taxas próximas a 100 Gbit/s, o que demonstra a viabilidade de uma criptografia resistente a ataques quânticos em infraestruturas de grande escala sem degradação perceptível do desempenho.

A literatura recente também apresenta esforços significativos na tentativa de equilibrar segurança e desempenho. Díaz et al. (Díaz 2020) mostram que a segurança deve ser incorporada desde as camadas mais baixas da pilha tecnológica, abrangendo bibliotecas de comunicação e políticas de identidade. O modelo

de *eTokens* proposto pelos autores substitui credenciais fixas por tokens efêmeros e adaptativos, reduzindo a exposição de chaves e fortalecendo o controle de sessão. Alam et al. (Alam et al. 2024) complementam essa linha de pesquisa com uma arquitetura federada baseada em princípios de *Zero Trust*, demonstrando que é possível conciliar desempenho e proteção sem aumentar significativamente a latência das aplicações.

No mesmo sentido, Saxena e Singh (Saxena e Singh 2021) introduzem o modelo *Online Secure Communication* (OSC-MC), que adota detecção preditiva de anomalias e isolamento dinâmico de tráfego, ajustando políticas de comunicação em tempo real. Essa proposta comprova que fluxos massivos de dados podem ser protegidos sem comprometer a eficiência, reforçando que segurança e desempenho são dimensões compatíveis. Em paralelo, Pouchard et al. (Pouchard, Islam e Nicolae 2022) enfatizam o papel da proveniência científica como um novo pilar da segurança computacional. O modelo PROV-IO+ registra automaticamente execuções, parâmetros e resultados, garantindo auditoria, rastreabilidade e reprodutibilidade, elementos fundamentais para a confiabilidade e a integridade científica.

A preparação do ecossistema HPC para a era pós-quântica é outro tema recorrente. Pouchard et al. (Pouchard, Islam e Nicolae 2022) argumentam que a adoção de esquemas de criptografia híbrida, que combinem algoritmos clássicos e pós-quânticos, deve ocorrer de forma gradual, garantindo compatibilidade e continuidade operacional. Essa estratégia, integrada a mecanismos de autenticação federada, constitui uma via promissora para proteger comunicações e identidades sem comprometer a interoperabilidade entre centros de supercomputação e redes científicas.

Além dos aspectos técnicos, cresce a importância da privacidade e da conformidade regulatória em ambientes de HPC. Gioiosa et al. (Gioiosa et al. 2025) apresentam um estudo de caso emblemático: uma infraestrutura compatível com o Regulamento Geral de Proteção de Dados (GDPR), aplicada ao processamento genômico de larga escala no consórcio Network for Italian Genomes. A arquitetura proposta integra máquinas virtuais isoladas, criptografia de armazenamento (LUKS), autenticação multifatorial e certificados digitais, alinhando-se a padrões ISO 9001 e 27001. Segundo os autores, essa abordagem demonstra que desempenho e conformidade podem coexistir, viabilizando a análise segura de dados biomédicos e reforçando o conceito de ciência aberta auditável.

Em síntese, os estudos revisados convergem para uma mesma conclusão: a segurança em HPC deixou de ser um elemento periférico para se tornar uma componente estrutural da arquitetura computacional. A integração entre autenticação federada, comunicação adaptativa, proveniência científica e conformidade regulatória delineia um novo paradigma no qual desempenho e proteção não são dimensões concorrentes, mas complementares, sustentando, em conjunto, a confiabilidade, a escalabilidade e a sustentabilidade dos ecossistemas de Computação de Alto Desempenho.

1.2 MOTIVAÇÃO

Esta dissertação se insere no esforço contemporâneo de conciliar segurança, confiabilidade e desempenho em ambientes de Computação de Alto Desempenho (HPC), compreendidos aqui não apenas como infraestruturas de processamento avançado, mas como ecossistemas sociotécnicos complexos que sustentam a pesquisa científica moderna. Em tais ambientes, a proteção das identidades, das comunicações e

dos dados processados deve ser concebida de forma integrada à própria arquitetura computacional — não como uma camada adicional, mas como um componente estrutural e auditável. Nesse sentido, a segurança deve ser tratada como um requisito de engenharia intrínseco ao HPC, com impacto direto sobre a sustentabilidade, a interoperabilidade e a confiabilidade científica.

O desafio de equilibrar desempenho e segurança emerge, sobretudo, em sistemas multiusuário, nos quais fluxos intensivos de dados e múltiplas instâncias de processamento ocorrem simultaneamente. Esses ambientes são particularmente sensíveis à latência e à sobrecarga introduzida por mecanismos criptográficos tradicionais, exigindo soluções que mantenham a eficiência operacional sem sacrificar a integridade das informações. O objetivo central deste trabalho, portanto, é investigar como reduzir a superfície de ataque associada a credenciais persistentes, fluxos contínuos e acessos remotos, preservando o desempenho em clusters científicos e acadêmicos.

No eixo da **identidade**, o foco recai sobre a substituição de credenciais duradouras por permissões temporárias e contextuais, emitidas dinamicamente por provedores de confiança. Essa estratégia reduz o tempo de exposição das chaves e amplia a capacidade de revogação imediata, aspectos fundamentais em ambientes distribuídos e colaborativos. Modelos modernos de autenticação e autorização, como OAuth 2.1 e OpenID Connect, têm se mostrado adequados a cenários de e-Science e HPC (Elkhodr 2021). Elkhodr (Elkhodr 2021) argumenta que a identidade digital deve ser gerida de forma federada e descentralizada, com autenticação baseada em contexto e níveis de confiança ajustáveis conforme o perfil e o risco de cada transação. Essa concepção está alinhada à evolução das infraestruturas científicas, que demandam interoperabilidade entre instituições, laboratórios e provedores de serviço, formando uma verdadeira federação de confiança científica.

No domínio da **comunicação**, o desafio está em alcançar o equilíbrio entre eficiência e proteção. O alto volume de trocas entre nós de processamento torna inviável a aplicação de mecanismos uniformemente pesados de criptografia. Kim et al. (Kim 2021) demonstram que a adoção de criptografia seletiva e autenticação adaptativa permite reduzir a sobrecarga de tráfego, garantindo confidencialidade apenas nos canais críticos. Da mesma forma, Baig et al. (Baig et al. 2022) evidenciam que técnicas de detecção comportamental e isolamento dinâmico de tráfego, inspiradas em redes definidas por software (SDN), podem responder a ataques em tempo real, ajustando políticas de comunicação de maneira inteligente e não intrusiva. Em ambientes HPC, tais mecanismos demonstram potencial para preservar o desempenho enquanto reforçam a resiliência contra falhas e ameaças externas.

A **proveniência científica** surge como uma dimensão complementar, diretamente associada à confiabilidade dos resultados e à rastreabilidade dos processos de execução. Han et al. (Han et al. 2023) propõem o modelo PROV-IO+, uma extensão do padrão W3C PROV, voltada ao registro automático de execuções, usuários e parâmetros em fluxos de trabalho científicos distribuídos. Esse modelo assegura que cada leitura, escrita ou modificação em um experimento seja associada a um agente, tempo e contexto específicos, permitindo auditoria completa com impacto mínimo no desempenho. A incorporação de proveniência nos sistemas HPC não apenas reforça a segurança e a transparência, mas também atende a exigências regulatórias e éticas crescentes em áreas sensíveis, como saúde, biotecnologia e energia.

Por fim, a **governança de chaves e certificados** constitui o alicerce da confiança digital em sistemas distribuídos. Khalil et al. (Khalil et al. 2022) propõem uma infraestrutura de chaves públicas baseada em

blockchain (BB-PKI), que descentraliza a autoridade e elimina pontos únicos de falha, assegurando rastreabilidade e imutabilidade dos registros. Essa abordagem reflete a convergência entre HPC, IoT industrial e redes científicas globais, nas quais a confiabilidade das identidades digitais e o ciclo de vida dos certificados se tornam fatores críticos para a interoperabilidade e a transparência organizacional. A descentralização da governança de chaves amplia a resiliência do sistema e reforça a auditabilidade de operações em escala.

A motivação deste trabalho também se apoia em observações empíricas realizadas em laboratórios da Universidade de Brasília, onde a coexistência de múltiplos perfis de usuários, fluxos híbridos e aplicações com alta sensibilidade à latência evidenciou a dificuldade de implementar controles de segurança sem comprometer o desempenho. Esses desafios práticos, que refletem a realidade de centros de HPC no Brasil e no exterior, reforçam a importância de desenvolver soluções que sejam tecnicamente eficazes, mas também economicamente viáveis e operacionalmente simples de adotar.

Iniciativas internacionais de padronização e interoperabilidade em e-Science e HPC, como o projeto INDIGO IAM (Agostini et al. 2025), apontam nessa mesma direção. Essa plataforma, amplamente utilizada na comunidade WLCG, integra autenticação multifatorial, suporte à OpenID Federation e políticas de autorização baseadas no Open Policy Agent (OPA), consolidando um modelo de identidade federada aplicável a ecossistemas distribuídos. O sucesso dessa arquitetura demonstra que é possível construir infraestruturas científicas seguras e escaláveis com base em padrões abertos e interoperáveis.

A experiência observada em ambientes reais da UnB reflete, em escala local, os mesmos desafios enfrentados globalmente: a necessidade de harmonizar desempenho computacional, segurança criptográfica, rastreabilidade científica e governança institucional. Essa convergência de fatores motiva a formulação de uma abordagem integrada que una identidade, comunicação, proveniência e governança de chaves em um modelo coerente de segurança de alta performance. Mais do que uma solução técnica, trata-se de um esforço para redefinir o próprio conceito de confiança computacional na era da ciência distribuída, sustentando um ecossistema HPC mais robusto, transparente e preparado para os desafios do futuro.

1.3 OBJETIVOS

O objetivo central desta dissertação é formular, implementar e analisar um conjunto de diretrizes técnicas voltadas ao fortalecimento da segurança de autenticação, proteção de dados e comunicação em ambientes de Computação de Alto Desempenho (HPC). Além da revisão conceitual, o trabalho desenvolve um produto tecnológico aplicado: a criação e implantação de uma Autoridade Certificadora SSH (SSH-CA) operacional no cluster LAMNA/UnB, permitindo a substituição progressiva de chaves SSH estáticas por certificados efêmeros assinados internamente. Esse artefato serve como prova de conceito para avaliar a viabilidade prática de modelos modernos de identidade e de autenticação leve em um ambiente científico real. O foco recai sobre sistemas multiusuário, arquiteturas federadas e políticas de segurança compatíveis com desempenho, escalabilidade e auditabilidade.

A partir desse cenário, quatro questões de pesquisa orientam o estudo:

- Em que medida concessões temporárias baseadas em certificados SSH e arquiteturas de identidade

federada reduzem riscos associados ao uso de credenciais persistentes em clusters multiusuário? Essa questão envolve desafios de revogabilidade, confiança cruzada e escalabilidade em ecossistemas distribuídos.

- Quais modelos de comunicação segura integram-se melhor aos padrões de tráfego de aplicações paralelas intensivas, e qual o custo de sua adoção para latência, sincronização coletiva e *throughput* em sistemas HPC?

- De que maneira mecanismos de proveniência científica e rastreabilidade de workflows podem contribuir para a auditoria e a reprodutibilidade em ambientes de HPC, assegurando integridade dos dados e conformidade com normas de segurança e privacidade?

- Quais modelos de governança distribuída para chaves e certificados podem ser adotados por federações HPC interinstitucionais, conciliando redução de pontos únicos de falha, interoperabilidade?

Metodologicamente, a pesquisa integra quatro eixos analíticos correspondentes às perguntas acima. A revisão bibliográfica abrange publicações de 2020 a 2025, período de avanços expressivos em autenticação federada, tokenização, proveniência e soluções criptográficas para HPC, incluindo debates sobre transição pós-quântica(Cambou 2021, Vermeer et al. 2024) . A análise comparativa avalia métodos que tentam equilibrar segurança e desempenho considerando latência, sobrecarga criptográfica, escalabilidade organizacional e compatibilidade com bibliotecas científicas. O desenvolvimento do produto técnico: Autoridade certificadora para certificados SSH que permitem validar em prática, um subconjunto dessas diretrizes, especialmente no que diz respeito a concessões efêmeras, gestão de chaves, revogabilidade e adoção incremental.

Esses esforços se alinham a tendências recentes que buscam incorporar auditoria, rastreabilidade e conformidade regulatória desde o desenho dos workflows científicos. Estudos como o de Stampelou, Ladds e Kolocouris (2024) demonstram que workflows computacionais em HPC podem integrar trilhas de auditoria, versionamento e documentação sistemática sem comprometer o desempenho, promovendo reprodutibilidade e integridade dos dados científicos (Stampelou, Ladds e Kolocouris 2024).

A contribuição desta dissertação se concentra em três entregas principais. A primeira é uma sistematização crítica da literatura recente, organizada para servir de referência a administradores e pesquisadores que lidam com clusters multiusuário. A segunda é o conjunto de diretrizes técnicas para adoção gradual de um pacote de segurança leve baseado em identidade federada, certificados efêmeros e proveniência mínima, concebido para minimizar impactos em performance. A terceira é o artefato aplicado: a infraestrutura operacional da Autoridade Certificadora SSH, documentada, funcional e integrada ao cluster LAMNA, permitindo avaliar empiricamente usabilidade, desempenho e aderência às recomendações sugeridas.

O escopo técnico contempla clusters científicos voltados a simulações, processamento de dados e aprendizado de máquina, operando sob políticas de múltiplos usuários. Não se aplicam contextos embarcados ou ambientes com restrições energéticas extremas, embora se reconheça que mecanismos criptográficos para canais de alta taxa têm implicações computacionais relevantes. O trabalho não propõe novos algoritmos, mas consolida e aplica técnicas reconhecidas no ecossistema HPC.

Como estudo aplicado, reconhecem-se limitações naturais. Diferentes clusters adotam arquiteturas,

sistemas de agendamento e políticas institucionais distintas, o que exige adaptações locais das diretrizes. Além disso, o impacto da segurança varia conforme o perfil da aplicação, workloads tolerantes à latência não têm os mesmos requisitos que aplicações críticas sensíveis a variações de sincronização. Por isso, as recomendações são apresentadas como um conjunto parametrizável de opções ajustáveis a diferentes ambientes.

Finalmente, a pesquisa destaca a importância da governança e da ética no tratamento de dados e identidades. Trilhas de auditoria devem ser mínimas, controladas e alinhadas a políticas institucionais de privacidade. Da mesma forma, a adoção de identidade federada exige relações formais de confiança e verificações regulares de segurança entre instituições parceiras. Essa perspectiva assegura que a evolução da segurança não comprometa a privacidade dos usuários nem a integridade dos dados científicos.

1.3.1 Objetivos específicos

De forma mais detalhada, os objetivos específicos desta dissertação são os seguintes:

1. Mapear, organizar e analisar criticamente a literatura recente sobre segurança aplicada à Computação de Alto Desempenho (HPC), com ênfase em autenticação federada, comunicação segura, proveniência científica e governança distribuída de chaves e certificados, identificando tendências, lacunas e desafios emergentes na integração entre desempenho e proteção.
2. Avaliar comparativamente as propostas identificadas na literatura, discutindo seus benefícios, limitações e requisitos de implementação, bem como o impacto sobre latência, *throughput*, escalabilidade e gerenciamento de identidade em ambientes HPC multiusuário e federados.
3. Desenvolver, documentar e testar um sistema de autenticação adaptado do modelo PrivacyIDEA, porém criado localmente para funcionar como Autoridade Certificadora SSH (SSH-CA). O sistema foi desenvolvido para trocar chaves fixas por certificados temporários no cluster LAMNA/UnB, funcionando como uma prova de conceito das recomendações apresentadas. A implementação priorizou a compatibilidade, além da avaliação de custo, impacto operacional e desempenho em cenários típicos, com base em simulações controladas.
4. Propor um conjunto de diretrizes técnicas de baixo impacto operacional para adoção gradual em infraestruturas científicas, integrando autenticação temporária, canais de comunicação protegidos e mecanismos mínimos de proveniência com rastreabilidade auditável, de modo a favorecer a implementação incremental e compatível com sistemas já em operação.

1.4 ORGANIZAÇÃO DO TRABALHO

A dissertação está estruturada em cinco capítulos, organizados de modo a garantir a progressão lógica entre fundamentação teórica, metodologia, resultados e conclusões.

O **Capítulo 2** apresenta a revisão bibliográfica, articulando os quatro eixos centrais, identidade, comunicação segura, proveniência científica e governança de chaves, à luz das tendências mais recentes

observadas na literatura.

O **Capítulo 3** descreve a metodologia adotada, detalhando os critérios de busca, a categorização dos estudos e os cenários operacionais utilizados para guiar o desenvolvimento do artefato técnico, bem como o processo de validação experimental.

O **Capítulo 4** apresenta e discute os resultados obtidos, comparando o estado da arte com a implementação prática da Autoridade Certificadora SSH (SSH-CA). São analisados benefícios, limitações e implicações de desempenho, além de aspectos de segurança e viabilidade de adoção em ambientes reais.

Por fim, o **Capítulo 5** reúne as conclusões gerais do trabalho, destacando suas contribuições técnicas e científicas, as limitações identificadas e as recomendações para estudos futuros, incluindo a expansão para autenticação federada completa e integração com múltiplos fatores de autenticação.

De forma integrada, a dissertação reforça que segurança e desempenho em HPC são dimensões complementares de um mesmo sistema, cuja eficiência depende da integração equilibrada entre identidade federada, concessões efêmeras, comunicação segura orientada ao desempenho, proveniência científica e governança de chaves auditável. Essa abordagem contribui para a consolidação de um ecossistema HPC mais robusto, confiável e alinhado às demandas de interoperabilidade e colaboração científica contemporâneas.

2. REVISÃO BIBLIOGRÁFICA

Nos últimos anos, o debate sobre o equilíbrio entre segurança e desempenho em sistemas distribuídos tem ganhado relevância também na área de Computação de Alto Desempenho (HPC). Estudos sobre arquiteturas descentralizadas e modelos de verificação distribuída demonstram que a adoção de mecanismos robustos de autenticação e integridade pode ser alcançada sem comprometer a eficiência operacional. Pajooh et al. (2021) demonstraram que o uso de blockchain permissionado, como o Hyperledger Fabric, reduz vulnerabilidades em redes distribuídas mantendo impacto mínimo sobre o *throughput* e a latência, o que indica a viabilidade de incorporar camadas de segurança adaptativas em infraestruturas paralelas e de alto desempenho (Pajooh et al. 2021).

Embora o campo ainda esteja em desenvolvimento, observa-se um crescimento consistente nas pesquisas voltadas à autenticação, controle de credenciais e governança criptográfica em infraestruturas de HPC. Estudos recentes apontam que princípios clássicos de segurança, como autenticação, autorização e trilhas de auditoria, vêm sendo reformulados para operar com baixa sobrecarga em sistemas paralelos e distribuídos. Alam et al. (2024) destacam que a adoção de arquiteturas de *Single Sign-On* federado e princípios de *Zero Trust* possibilita combinar desempenho e segurança em ambientes híbridos de inteligência artificial e HPC, com base em protocolos abertos como OAuth 2.x e OpenID Connect (Alam et al. 2024).

A Figura 2.1 apresenta a arquitetura de autenticação federada e o modelo *Zero Trust* proposto por Alam et al. (2024). Nessa estrutura, ocorre a integração entre provedores de identidade institucionais e serviços em nuvem, que são responsáveis pela emissão e validação de credenciais temporárias utilizadas durante os processos de autenticação SSH e de certificação interna dos nós do cluster. A representação evidencia a separação entre zonas de acesso segmentadas, denominadas *Federated Domain Services* (FDS), *Secure Workflow Service* (SWS) e *Managed Data Center* (MDC), que operam em diferentes níveis de confiança para reduzir a superfície de ataque e otimizar o isolamento de processos. Essa abordagem demonstra como fluxos de autenticação distribuídos podem ser estruturados de forma eficiente, preservando a integridade e o desempenho do ambiente HPC.

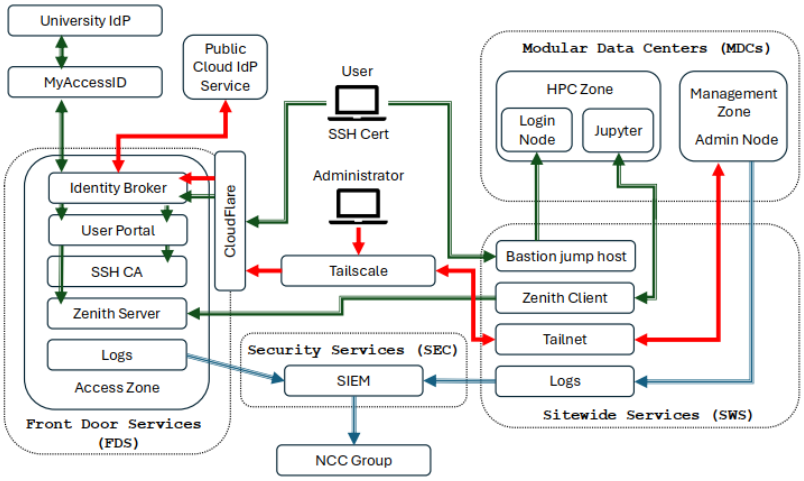


Figura 2.1: Arquitetura de autenticação federada e modelo *Zero Trust* proposto por Alam et al. (2024).

De forma complementar, Elkhodr (2021) analisa modelos de gestão de identidade digital e mostra como a descentralização da autenticação e o uso de tokens efêmeros podem reduzir vulnerabilidades em sistemas distribuídos (Elkhodr 2021). Trabalhos mais recentes, como o de Agostini et al. (2025), reforçam esse avanço ao apresentar a evolução do INDIGO IAM, que implementa autenticação federada, delegação de credenciais e interoperabilidade entre provedores científicos, tornando a segurança um componente estrutural nas operações distribuídas (Agostini et al. 2025).

Além dessas abordagens técnicas, diretrizes normativas e referenciais internacionais também têm moldado o desenvolvimento de políticas de segurança para infraestruturas científicas de alto desempenho. As publicações do *National Institute of Standards and Technology* (NIST), especialmente a *NIST Special Publication 800-223 – Securing High Performance Computing Environments* e a *NIST Special Publication 800-234 – Security Guidelines for Scientific Computing and Research Infrastructures*, definem um arcabouço abrangente de práticas voltadas à autenticação federada, segmentação de redes, controle de identidade e gestão de chaves em ecossistemas HPC (Standards e Technology 2024, Standards e Technology 2025). Essas normas complementam a literatura científica ao fornecer parâmetros operacionais e de conformidade que orientam tanto políticas de acesso quanto estratégias de auditoria, reforçando a convergência entre desempenho, segurança e governança digital em ambientes de pesquisa colaborativa.

A evolução arquitetural dos sistemas HPC também ampliou a superfície de ataque e introduziu novos desafios de segurança. Pleiter (2020) argumenta que a presença de múltiplos tipos de processadores, bibliotecas especializadas e topologias complexas de comunicação exige estratégias criptográficas adaptativas e mecanismos de controle de acesso compatíveis com o paralelismo extremo (Pleiter 2020). Nesse contexto, Aguilera (2024) propõe o uso de links criptografados de alta taxa com chaves pré-compartilhadas, que minimizam a sobrecarga criptográfica em ambientes de alto desempenho, assegurando confidencialidade e integridade nas comunicações entre nós (Aguilera et al. 2024).

2.1 DESAFIOS ESTRUTURAIS E VULNERABILIDADES

A diversidade de componentes presentes em clusters modernos, incluindo sistemas operacionais distintos, bibliotecas otimizadas, filas de execução e múltiplos *middlewares*, torna os ambientes de Computação de Alto Desempenho (HPC) particularmente suscetíveis a falhas de controle de acesso. Lu et al. (Lu et al. 2022) identificaram a vulnerabilidade denominada *Missing Permission Check* (MPC), que ocorre quando verificações de permissão não são corretamente aplicadas, permitindo a execução indevida de operações privilegiadas por usuários não autorizados. Essa falha decorre da ausência de validações consistentes em diferentes pontos do fluxo de autorização e pode comprometer tanto a integridade dos dados quanto a confiabilidade operacional do sistema.

A Figura 2.2 apresenta os quatro mecanismos de verificação de permissão (M1–M4) analisados por Lu et al. (2022). Cada mecanismo representa uma variação no fluxo de controle entre usuários, aplicações e servidores, evidenciando como a ausência de verificações completas pode gerar lacunas de segurança em diferentes camadas do sistema. Essa visualização auxilia na compreensão das origens da vulnerabilidade MPC, mostrando que pequenos desvios nos fluxos de autorização podem permitir a execução de operações críticas sem a devida validação.

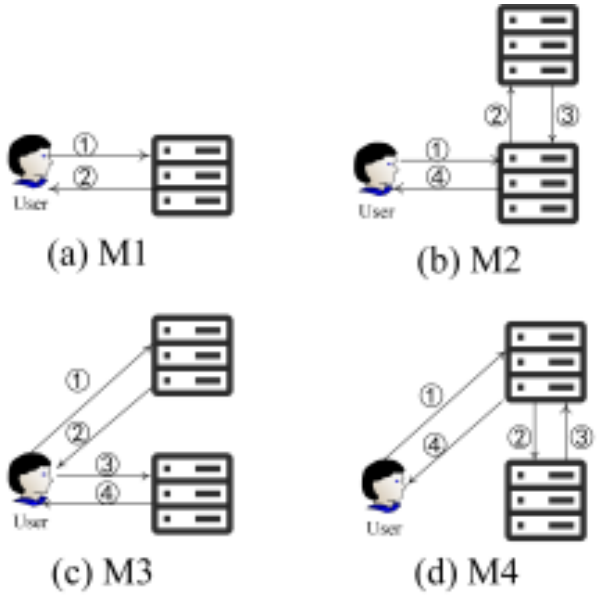


Figura 2.2: Mecanismos distintos de verificação de permissão (M1–M4) e seus respectivos fluxos de controle entre usuários e servidores. Fonte: Lu et al. (2022).

Para enfrentar o problema identificado, Lu et al. propuseram a ferramenta MPChecker, projetada para realizar análises híbridas de logs e fluxos de dados, com o objetivo de detectar violações de permissão em tempo real. AEsse processo possibilita a detecção automatizada de falhas e contribui para a implementação de políticas de segurança proativas em clusters HPC.

O estudo conduzido por Lu et al. demonstra a importância de mecanismos de observabilidade contínua, capazes de associar métricas de desempenho e segurança em tempo real. Essa integração é fundamental para antecipar falhas, reduzir a superfície de ataque e aprimorar a confiabilidade de sistemas de HPC.

Além das vulnerabilidades estruturais, pesquisas recentes destacam a necessidade de detectar anomalias em fluxos de comunicação paralela. Pequenas variações nos padrões de tráfego, na sincronização entre processos MPI ou no comportamento das filas de execução podem indicar falhas operacionais ou ataques direcionados (Blaschke 2024). Tais observações exigem correlação contínua entre métricas distribuídas, registros de eventos e políticas de acesso (Liang 2024). Estudos como o de Rinn et al. (Rinn 2024) demonstram que a análise combinada de indicadores de desempenho e segurança permite identificar desvios de tráfego que sinalizam desde congestionamentos até comportamentos maliciosos, reforçando a necessidade de estratégias de monitoramento e resposta integradas em ambientes HPC.

Koleini e Pahlevanzadeh (Koleini e Pahlevanzadeh 2024) reforçam que o principal desafio é equilibrar segurança e desempenho, já que mecanismos mais rígidos podem impactar negativamente aplicações paralelas. Soluções adaptativas que ajustam políticas de proteção conforme o estado da aplicação, carga, sensibilidade dos dados e padrões de uso aparecem como alternativas promissoras. Esse tipo de abordagem, baseada em observabilidade contínua, tem potencial para oferecer proteção dinâmica sem degradar o throughput dos sistemas.

2.2 AUTENTICAÇÃO, CREDENCIAIS E CONFIANÇA

A autenticação permanece uma das áreas mais críticas da segurança em ambientes de Computação de Alto Desempenho (HPC), em grande parte devido ao uso histórico de chaves SSH permanentes e credenciais estáticas. Pokhachevskiy (Pokhachevskiy 2020) demonstrou que mecanismos frágeis de autenticação, especialmente implementações vulneráveis de Active Directory sem validação mútua, podem comprometer múltiplos nós simultaneamente. A necessidade de substituir credenciais fixas por mecanismos temporários aparece como consenso na literatura recente (Díaz 2020).

Díaz et al. (Díaz 2020) propuseram o *eToken*, uma solução baseada em criptografia de curvas elípticas que utiliza concessões temporárias para substituir chaves persistentes, mantendo compatibilidade com cenários híbridos que integram HPC e nuvem. O sistema é estruturado de modo a reduzir a exposição prolongada de credenciais, aumentar a rastreabilidade e facilitar a revogação dinâmica de permissões.

A Figura 2.3 apresenta a arquitetura geral do sistema de autenticação proposto por Díaz et al. (2020). Nessa estrutura, o usuário solicita um *eToken* ao servidor de autenticação, que emite uma credencial temporária utilizada para estabelecer sessões seguras com o servidor *gateway*. Esse servidor provê acesso a serviços críticos, como o SSH e o HDFS, sob políticas centralizadas de autorização e auditoria. Essa representação evidencia como a autenticação por tokens efêmeros pode ser implementada em fluxos de comunicação HPC sem comprometer o desempenho operacional.

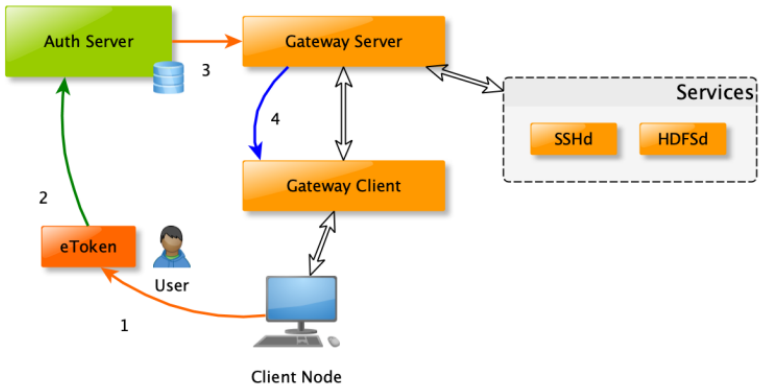


Figura 2.3: Elementos do sistema de autenticação e comunicação proposto por Díaz et al. (2020). O usuário obtém um *eToken* temporário do servidor de autenticação, utilizado para estabelecer sessão segura com o servidor *gateway*, que provê acesso a serviços como SSHd e HDFSd. Fonte: Díaz et al. (2020).

A comunicação entre os componentes do sistema é detalhada na Figura 2.4, que mostra a integração multiprotocolo via *Message Queuing Telemetry Transport* (MQTT). Esse protocolo atua como intermediário entre o cliente, os servidores de autenticação e os módulos de configuração, garantindo interoperabilidade e baixa latência na troca de mensagens. O uso do MQTT permite compatibilidade com diferentes camadas de rede e facilita a integração entre domínios federados.

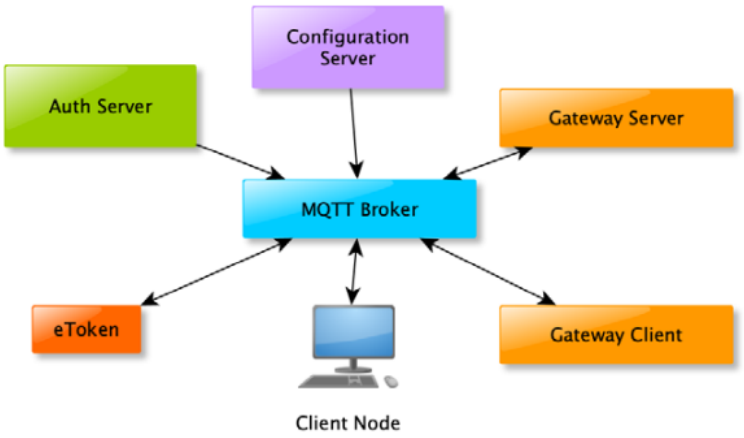


Figura 2.4: Interconexão entre os componentes do sistema de autenticação multiprotocolo via *Message Queuing Telemetry Transport* (MQTT). Fonte: Díaz et al. (2020).

A Figura 2.5 ilustra o esquema criptográfico utilizado para proteger a chave de sessão (*Session Key*) no modelo proposto. O processo combina funções de acordo de chaves (KA), derivação (KDF), autenticação de mensagem (MAC) e encriptação (ENC), formando uma cadeia segura de operações que garante confidencialidade e integridade durante a comunicação. Esse nível de detalhamento demonstra a preocupação dos autores em balancear robustez criptográfica e eficiência computacional, requisito essencial para operações de alta performance.

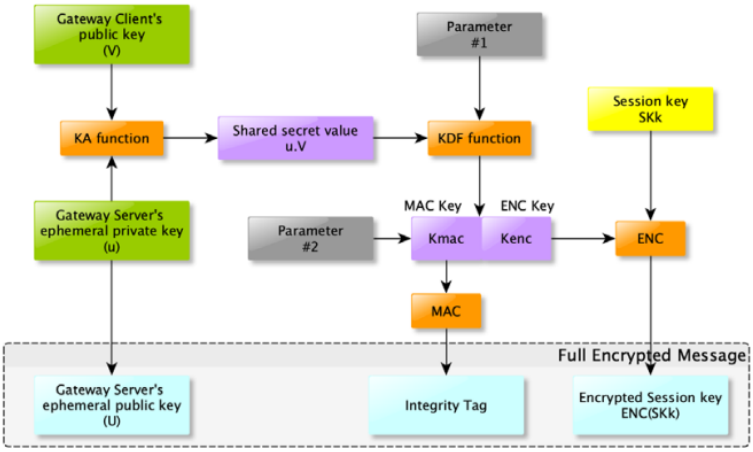


Figura 2.5: Esquema de encriptação da chave de sessão (*Session Key*) no modelo de Díaz et al. (2020), com uso de funções de acordo de chaves (KA), derivação (KDF), autenticação de mensagem (MAC) e encriptação (ENC). Fonte: Díaz et al. (2020).

Por fim, a Figura 2.6 apresenta o diagrama de sequência de mensagens entre os principais elementos do sistema, evidenciando as etapas de autenticação, verificação de listas de controle de acesso (ACL) e troca segura de chaves utilizando criptografia ECIES. Esse diagrama permite visualizar a interação entre cliente, servidores e serviços intermediários durante o processo de autenticação e autorização, destacando a importância da validação contínua de cada transação dentro do fluxo operacional.

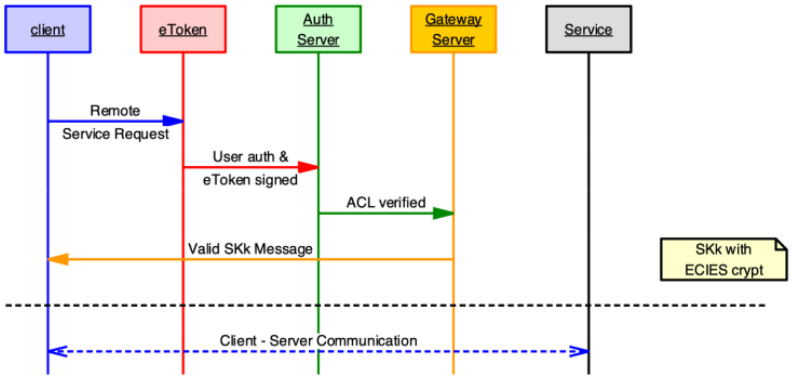


Figura 2.6: Diagrama de sequência de mensagens entre os elementos do sistema proposto por Díaz et al. (2020), destacando as etapas de autenticação, verificação de ACL e troca segura de chaves via ECIES. Fonte: Díaz et al. (2020).

De forma complementar, Alam et al. (Alam et al. 2024) argumentam pela adoção de arquiteturas *Zero Trust* integradas a sistemas de *Single Sign-On*, nas quais cada solicitação de acesso é verificada de maneira independente do contexto institucional. Em ambientes federados, esse modelo amplia a granularidade do controle e reduz os riscos associados à confiança implícita.

Soluções multiprotocolo (Díaz 2020) demonstram abordagens compatíveis com diferentes padrões de autenticação e federação em HPC e nuvem. Além disso, pipelines de execução com credenciais segregadas (Blaschke 2024) reforçam a tendência de arquiteturas unificadas que conciliam múltiplos métodos de

autenticação em fluxos de trabalho paralelos. A literatura recente converge para a adoção de identidade federada, delegação limitada e mecanismos de revogação ágil como fundamentos indispensáveis para a operação segura e escalável de ambientes de Computação de Alto Desempenho (Ritchie 2023).

2.3 COMUNICAÇÃO SEGURA E DESEMPENHO ADAPTATIVO

A comunicação entre nós representa uma das áreas mais sensíveis em clusters HPC. Aplicações paralelas dependem de sincronização precisa e troca intensiva de dados, o que torna qualquer camada adicional de segurança potencialmente custosa. Saxena e Singh (Saxena e Singh 2021) propuseram o modelo OSC-MC, que utiliza análise preditiva para detectar anomalias e otimizar conexões entre máquinas virtuais, reduzindo consumo de banda e energia. O estudo demonstra que segurança adaptativa, guiada por telemetria, pode coexistir com alto desempenho.

Gamblin e Katz (Gamblin e Katz 2023) analisam as dificuldades de integrar pipelines de automação segura (CI/CD) em supercomputadores, propondo zonas controladas de execução que permitem verificações seguras sem comprometer a estabilidade do cluster. Zhou et al. (Zhou, Zhou e Hoppe 2022) mostram que o uso de containers especializados como Singularity e Apptainer fornece isolamento leve, padroniza ambientes de execução e reduz riscos de ataques laterais.

Modelos híbridos que combinam criptografia leve com detecção preditiva baseada em aprendizado de máquina aparecem como solução promissora para alcançar proteção eficiente em aplicações sensíveis à latência. Pesquisas recentes sugerem que políticas de proteção adaptadas à carga, comportamento e padrões de anomalia podem reduzir significativamente o custo da criptografia em sistemas paralelos (Kamal e Mashaly 2025). Do ponto de vista do tráfego, desvios sutis identificados na interconexão de alta velocidade também são indicadores úteis para proteção dinâmica (Wang 2025).

2.4 PROVENIÊNCIA CIENTÍFICA E RASTREABILIDADE

A rastreabilidade é um elemento central para a auditoria e a reprodutibilidade em workflows paralelos de Computação de Alto Desempenho (HPC). Em ambientes onde múltiplos processos interagem de forma simultânea, registrar a origem, o contexto e a execução de cada etapa torna-se essencial para garantir integridade, confiabilidade e transparência científica. Han et al. (Han et al. 2023) apresentaram o PROV-IO$^+$, um *framework* compatível com o padrão W3C PROV, desenvolvido especificamente para registrar atividades de forma estruturada e com sobrecarga mínima. O sistema amplia o modelo tradicional de proveniência, permitindo anotações semânticas detalhadas e o registro automático de agentes, dados e processos.

A Figura 2.7 apresenta a visão geral do modelo PROV-IO$^+$ proposto por Han et al. (2023). O esquema classifica as informações em quatro superclasses: *Entity*, *Activity*, *Agent* e *Extensible Class*. Cada uma delas representa um componente essencial do processo científico: as entidades correspondem a objetos de dados; as atividades descrevem ações ou transformações realizadas; os agentes representam usuários,

sistemas ou serviços envolvidos; e as classes extensíveis permitem adaptar o modelo a diferentes domínios científicos. Os novos conceitos introduzidos pelo PROV-IO$^+$, destacados em azul, expandem as possibilidades de interoperabilidade e integração entre plataformas científicas. Essa estrutura modular possibilita que sistemas HPC registrem automaticamente o histórico de execução de tarefas, garantindo rastreabilidade com impacto mínimo no desempenho operacional.

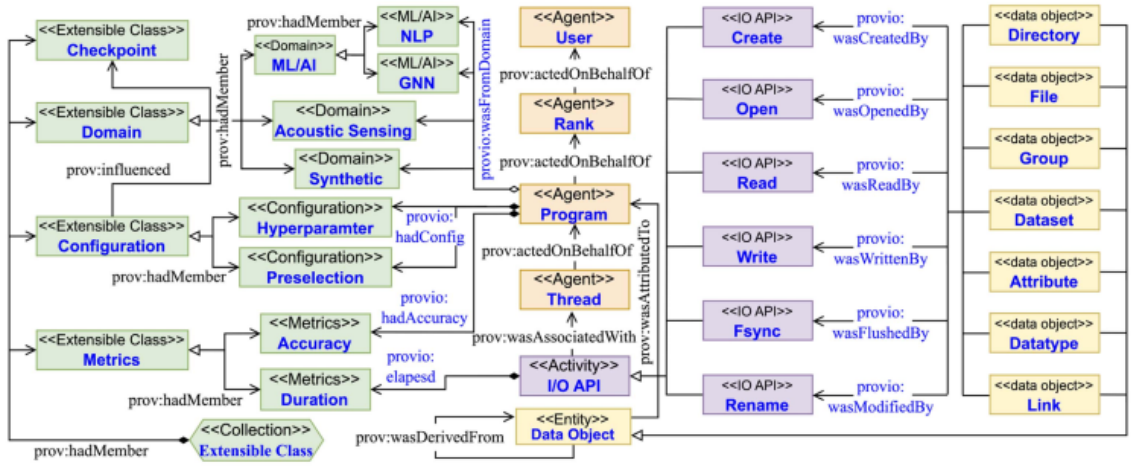


Figura 2.7: Visão geral do modelo PROV-IO$^+$, proposto por Han et al. (2023), que classifica informações em quatro superclasses: *Entity*, *Activity*, *Agent* e *Extensible Class*. Os novos conceitos do modelo são destacados em azul. Fonte: Han et al. (2023).

Além da modelagem conceitual, o PROV-IO$^+$ inclui representações formais baseadas em RDF/Turtle, que permitem interoperabilidade entre sistemas e padronização de registros de proveniência. O código mostra um exemplo de fragmento de proveniência (*Provenance Snippet*) gerado nesse formato. O exemplo demonstra como diferentes agentes, programas, APIs e objetos de dados são relacionados entre si no modelo, formando uma trilha verificável de execução. Essa representação permite que cada elemento de um experimento seja identificado e auditado individualmente, o que é fundamental para a reprodutibilidade de resultados e para a conformidade com normas de integridade científica.

```
<prov:User>
    <rdfs:subClassOf> <prov:Agent> .
</prov:User>

<prov:Program>
    <rdfs:subClassOf> <prov:Agent> .
</prov:Program>

<prov:ToAPI>
    <rdfs:subClassOf> <prov:Activity> .
</prov:ToAPI>

<prov:DataObject>
    <rdfs:subClassOf> <prov:Entity> .
</prov:DataObject>
```

```
16
17 <Bob> a <prov:User> .
18
19 <xpicto_uni_h5.exe-a1> a <prov:Program> ;
20     <prov:actedOnBehalfOf> <Bob> .
21
22 <H5Dcreate2-b1> a <prov:ToAPI> ;
23     <rdf:type> <prov:Create> ;
24     <prov:wasAssociatedWith> <xpicto_uni_h5.exe-a1> .
25
26 </Timestamp_0> a <prov:DataObject> ;
27     <rdf:type> <prov:Dataset> ;
28     <prov:wasAttributedTo> <xpicto_uni_h5.exe-a1> ;
29     <prov:wasCreatedBy> <H5Dcreate2-b1> .
```

Listing 2.1: Exemplo de representação PROV-O do fluxo de autenticação

Padovani et al. (Padovani, Anantharaj e Fiore 2025) complementam essa discussão ao demonstrar que auditorias contínuas podem ser incorporadas aos workflows científicos de forma automatizada, fortalecendo a confiabilidade dos experimentos e ampliando o controle sobre os processos executados. De modo semelhante, Bountris et al. (Bountris, Thamsen e Leser 2025) exploram modelos de proveniência associados a logs estruturados e registros criptográficos, que permitem identificar inconsistências em pipelines complexos sem adicionar custos computacionais expressivos.

A literatura recente aponta para a integração da proveniência científica com políticas de acesso, mecanismos criptográficos e autenticação federada, consolidando-a como parte integrante do perímetro de segurança em ambientes HPC. Essa integração permite articular confiabilidade, auditoria e reprodutibilidade de forma sinérgica, transformando a proveniência em um componente estratégico tanto da segurança quanto da governança científica.

2.5 CRIPTOGRAFIA, DESCENTRALIZAÇÃO E TRANSIÇÃO PÓS-QUÂNTICA

A necessidade de proteger grandes volumes de dados com baixa latência torna a escolha dos algoritmos criptográficos um fator crítico em ambientes de Computação de Alto Desempenho (HPC). Bica et al. (Bica 2020) propuseram uma infraestrutura de autenticação descentralizada baseada em tecnologias de registro distribuído (*Distributed Ledger Technology* – DLT), como o *blockchain*, para gerenciar certificados digitais e reduzir a dependência de autoridades centrais. O modelo utiliza autenticação multipartes, na qual diversas entidades cooperam na validação de credenciais, reforçando a resiliência contra comprometimentos individuais e eliminando pontos únicos de falha. Além disso, o uso de consenso distribuído permite validar transações de autenticação de forma transparente e auditável, tornando o processo mais confiável e escalável.

Walid et al. (Walid 2024) realizaram uma análise comparativa entre diferentes esquemas de criptografia baseados em atributos (*Attribute-Based Encryption* – ABE) aplicáveis a cenários de alto desempenho. O estudo avaliou métricas como latência de descriptografia, complexidade computacional e custo energético,

demonstrando que a integração de mecanismos resistentes a ataques quânticos pode equilibrar segurança e eficiência em fluxos de dados intensivos.

A Figura 2.8 apresenta a comparação realizada por Walid et al. (2024) entre os principais esquemas de ABE aplicáveis a sistemas HPC. Observa-se que abordagens híbridas, que combinam criptografia simétrica e assimétrica, proporcionam maior escalabilidade e menor impacto em desempenho quando aplicadas a sistemas paralelos de alto desempenho. Esse tipo de arquitetura é particularmente relevante para clusters científicos que manipulam dados sensíveis, como os utilizados em bioinformática, climatologia e simulações físicas complexas.

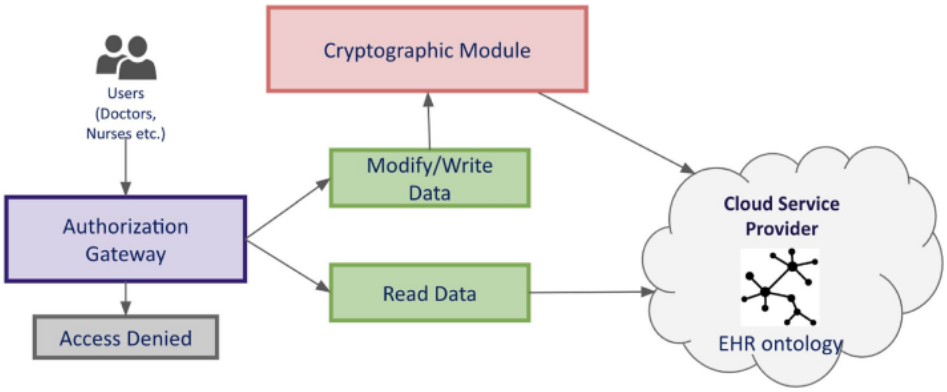


Figura 2.8: Comparação entre esquemas de criptografia baseados em atributos (ABE) para HPC, conforme Walid et al. (2024).

Alotaibi et al. (Alotaibi 2024) propuseram um aprimoramento do protocolo MQTT, amplamente utilizado em sistemas de Internet das Coisas (IoT) integrados a plataformas HPC, incorporando mecanismos de criptografia distribuída e autenticação baseada em tokens temporários. Essa modificação fortalece a troca de chaves e a validação de identidade entre dispositivos e nós de processamento, mitigando ataques de injeção e de comunicação.

A Figura 2.9 ilustra a fase de ataque de autenticação no protocolo MQTT tradicional, destacando como agentes maliciosos podem explorar brechas durante o estabelecimento inicial de conexão para obter acesso não autorizado. Esse tipo de vulnerabilidade é comum em implementações que não empregam validação mútua de certificados ou que mantêm chaves estáticas em memória.

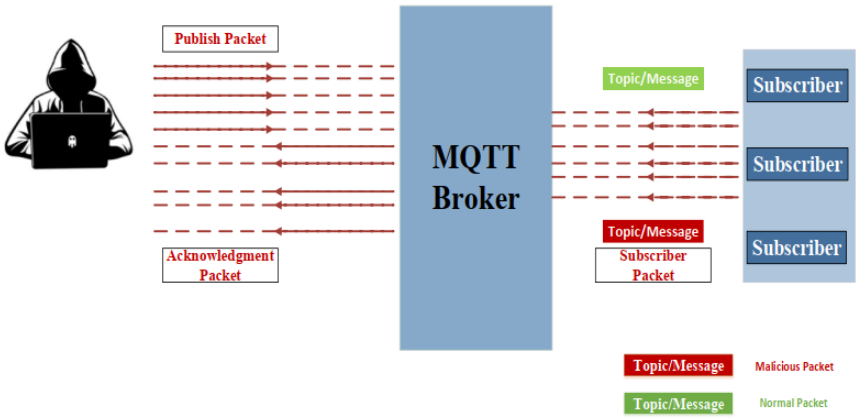


Figura 2.9: Fase de ataque de autenticação no protocolo MQTT. Fonte: Alotaibi et al. (2024).

Na sequência, a Figura 2.10 apresenta a fase de ataque de comunicação, em que mensagens legítimas são interceptadas ou modificadas durante a transmissão. Alotaibi et al. (2024) demonstram que, ao incorporar criptografia distribuída e autenticação baseada em tokens temporários, é possível eliminar esses vetores de ataque, garantindo integridade e sigilo das trocas de dados entre dispositivos e servidores de processamento.

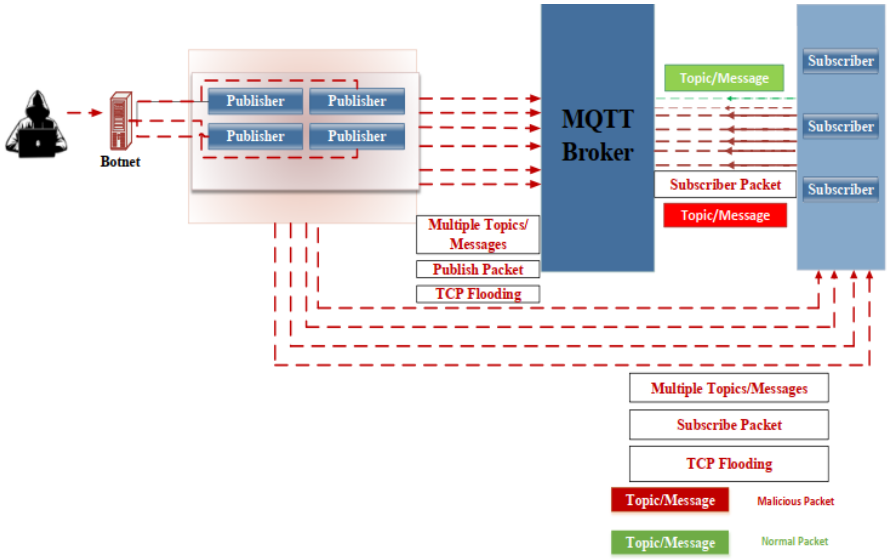


Figura 2.10: Fase de ataque de comunicação no protocolo MQTT. Fonte: Alotaibi et al. (2024).

Han et al. (Han 2025) desenvolveram um *framework* escalável de controle de acesso seguro para dispositivos IoT operando em ambientes de HPC. O sistema integra autenticação baseada em confiança e verificação de integridade distribuída, adotando um esquema de autorização hierárquica e dinâmica. Essa abordagem permite ajustar privilégios de acesso conforme o contexto, reduzindo significativamente o risco de comprometimento de nós periféricos e assegurando a continuidade operacional de redes científicas e de sensores em larga escala.

Nowrozy et al. (Nowrozy, Ahmed e Wang 2025) introduziram um modelo tripartite de autenticação

que combina ontologias semânticas e aprendizado de máquina para aprimorar a gestão de identidade e a detecção de comportamentos anômalos. Nesse sistema, três agentes — usuário, serviço e auditor — cooperam para verificar a validade das credenciais e a consistência das operações executadas. Essa estrutura aumenta a confiabilidade e a resiliência de infraestruturas distribuídas, ao mesmo tempo em que reduz falsos positivos e melhora a eficiência do processo de verificação.

Em conjunto, esses estudos demonstram que a incorporação de algoritmos de criptografia pós-quântica, autenticação distribuída e validação baseada em confiança é essencial para garantir privacidade, integridade e continuidade operacional em sistemas de Computação de Alto Desempenho. O movimento em direção a infraestruturas seguras, interoperáveis e auditáveis representa uma transição de paradigma: de uma segurança reativa, aplicada após o fato, para uma segurança integrada ao próprio ciclo de execução científica, fundamentada em princípios de descentralização, verificabilidade e resiliência.

2.6 GOVERNANÇA E ECOSSISTEMAS DE CONFIANÇA DIGITAL

A governança da segurança em ambientes de alto desempenho (HPC) requer políticas unificadas de identidade, controle de privilégios e mecanismos auditáveis de autenticação entre múltiplos domínios. Rinn et al. (Rinn 2024) analisam o ambiente federado Leonhard Med, projetado para pesquisas seguras e reprodutíveis, destacando a importância da confiança e da interoperabilidade em ecossistemas científicos distribuídos. Li et al. (Li 2021) propõem uma plataforma escalável e interoperável voltada à integração de dados em HPC, unindo segurança e governança distribuída por meio de identidades federadas e auditoria contínua.

Choi et al. (Choi 2023) exploram tecnologias de interoperabilidade que permitem o compartilhamento de dados entre sistemas heterogêneos, garantindo integridade e rastreabilidade em arquiteturas multiusuário. Da mesma forma, Rosenfield et al. (Rosenfield 2022) destacam o papel da governança colaborativa no Consórcio de HPC contra a COVID-19, evidenciando como políticas padronizadas de identidade e automação segura facilitam o uso ético e rastreável de recursos distribuídos. Esses avanços demonstram que a convergência entre governança digital e infraestrutura federada de identidade tende a consolidar um novo modelo de ecossistema HPC mais seguro, interoperável e auditável.

2.7 SÍNTESE DA LITERATURA

A literatura analisada evidencia quatro frentes predominantes no avanço da segurança em ambientes de computação de alto desempenho (HPC). A primeira refere-se à **autenticação federada e uso de tokens efêmeros**, que substituem credenciais estáticas e ampliam a rastreabilidade do acesso. Alam et al. (Alam et al. 2024) destacam que a integração de identidade federada, protocolos como OpenID Connect e abordagens de *zero trust* em infraestruturas distribuídas melhora significativamente a interoperabilidade e a revogabilidade de credenciais, tornando o acesso a múltiplos domínios mais seguro e auditável.

A segunda linha envolve **comunicação segura adaptativa**, que combina criptografia leve com detec-

ção preditiva orientada por telemetria. Aguilera (Aguilera et al. 2024) e Saxena e Singh (Saxena e Singh 2021) propõem modelos híbridos de criptografia e comunicação dinâmica para HPC e nuvem, reduzindo latência sem comprometer a proteção dos dados. Essa perspectiva converge com a visão de Koleini e Pahlevanzadeh (Koleini e Pahlevanzadeh 2024), que enfatizam o papel da automação inteligente na mitigação de ameaças em larga escala.

A terceira frente aborda a **proveniência científica e a rastreabilidade de workflows**, essencial para a integridade dos dados e a reprodutibilidade científica. Pouchard et al. (Pouchard, Islam e Nicolae 2022) e Padovani et al. (Padovani, Anantharaj e Fiore 2025) discutem estratégias para integrar mecanismos FAIR e proveniência contínua diretamente aos workflows de HPC, minimizando sobrecarga computacional e facilitando auditoria automatizada. Essa integração é reforçada por Bountris et al. (Bountris, Thamsen e Leser 2025), que apresentam modelos híbridos de gestão de proveniência para execução distribuída e análise em tempo real.

Por fim, a literatura converge para a importância da **criptografia resiliente e governança distribuída**, garantindo interoperabilidade, auditabilidade e conformidade regulatória. Gioiosa et al. (Gioiosa et al. 2025) demonstram a viabilidade de soluções compatíveis com o GDPR em ambientes de HPC em nuvem, enquanto Rinn (Rinn 2024) destaca a necessidade de estruturas federadas de governança e identidade para garantir transparência em ecossistemas científicos colaborativos. Gamblin e Katz (Gamblin e Katz 2023) complementam essa perspectiva, evidenciando que práticas de automação segura e integração contínua são fundamentais para manter a integridade operacional e a confiabilidade dos sistemas de HPC modernos.

De modo geral, os estudos indicam que o campo evolui para uma *arquitetura de confiança integrada ao ciclo de execução*, na qual segurança e desempenho passam a ser tratados de forma conjunta. Esse movimento converge com as diretrizes propostas pelo *National Institute of Standards and Technology*, em especial nas publicações *NIST SP 800-223* e *NIST SP 800-234*, que consolidam princípios de controle de identidade, segmentação lógica e auditoria contínua como elementos estruturais de ambientes HPC (Standards e Technology 2024, Standards e Technology 2025). A correspondência entre os achados científicos e os referenciais normativos internacionais reforça o alinhamento das práticas analisadas com os padrões mais recentes de segurança e governança para infraestruturas de pesquisa distribuída.

3. METODOLOGIA

A segurança em sistemas de Computação de Alto Desempenho (High Performance Computing, HPC) é um campo que ainda está em consolidação dentro da ciência da computação. Embora supercomputadores sejam essenciais para simulação científica, inteligência artificial e análise de grandes volumes de dados, o debate sobre sua proteção, integridade e resiliência permanece relativamente recente e disperso (Koleini e Pahlevanzadeh 2024, Díaz 2020). A literatura disponível tende a se distribuir entre subáreas como segurança de sistemas distribuídos, autenticação federada, comunicação segura e governança de identidades, evidenciando o caráter interdisciplinar e dinâmico do tema.

Pesquisas recentes indicam que muitas práticas de segurança adotadas em HPC derivam de modelos originalmente concebidos para nuvem e infraestruturas distribuídas convencionais, o que exige adaptações cuidadosas para contextos com exigência de baixa latência, paralelismo intenso e isolamento entre múltiplos usuários (Gamblin e Katz 2023). Além disso, estudos que exploram a integração entre identidade federada, autenticação baseada em certificados e políticas de confiança sugerem que a segurança em HPC deve ser tratada de forma multidimensional, articulando aspectos técnicos, organizacionais e regulatórios (Alam et al. 2024).

Nesse contexto, diretrizes normativas publicadas pelo *National Institute of Standards and Technology* (NIST) tornaram-se referência para orientar a consolidação da segurança em ambientes de alto desempenho. As publicações *NIST Special Publication 800-223, Securing High Performance Computing Environments* e *NIST Special Publication 800-224, Security Guidelines for Scientific Computing and Research Infrastructures* estabelecem princípios para controle de identidade, segmentação de redes, gestão de chaves criptográficas e auditoria contínua de fluxos computacionais (Standards e Technology 2024, Standards e Technology 2025). Essas diretrizes compõem o arcabouço metodológico que inspira esta pesquisa, ao propor a tradução prática de recomendações internacionais para o contexto científico e operacional de um cluster multiusuário, buscando equilíbrio entre desempenho e segurança de modo verificável.

Grande parte da produção científica sobre segurança em HPC aparece na forma de estudos de caso aplicados a domínios específicos, como *workflows* biomédicos, infraestruturas com dados sensíveis e ambientes sujeitos a normas de privacidade. Trabalhos recentes incluem iniciativas voltadas à análise segura de dados clínicos, à adoção de princípios FAIR em fluxos científicos complexos e à consolidação de arquiteturas voltadas à proteção de dados médicos e regulatórios (Blaschke 2024). Mesmo quando não tratam diretamente de segurança, esses estudos evidenciam que autenticação, controle de acesso, proveniência e conformidade regulatória se tornaram componentes essenciais na operação prática de supercomputadores em cenários críticos.

Além disso, pesquisas que abordam integração de dados sensíveis e colaboração entre centros científicos indicam que identidades federadas, auditoria de acessos e políticas robustas de privacidade são condições necessárias para participação em consórcios internacionais (Gioiosa et al. 2025). Em paralelo, estudos que analisam a exposição de recursos HPC por meio de APIs, portais científicos e serviços remotos mostram que, ao tratar HPC como serviço, amplia-se a superfície de ataque e cresce a necessidade de arquiteturas de segurança explícitas e auditáveis (Han et al. 2023).

Diante desse cenário, esta pesquisa, de natureza aplicada e com enfoque predominantemente qualitativo, adota uma metodologia híbrida que combina mapeamento bibliográfico sistematizado, revisão integrativa de escopo e pesquisa experimental voltada ao desenvolvimento tecnológico. O objetivo é, por um lado, mapear e interpretar criticamente o estado da arte sobre segurança em HPC, identificando lacunas conceituais e práticas. Por outro lado, busca-se propor e implementar um artefato técnico que funcione como prova de conceito para a aplicação e validação preliminar das diretrizes levantadas.

O artefato desenvolvido consiste em um sistema de autenticação baseado em certificados SSH emitidos por uma autoridade certificadora interna, aplicado a um ambiente de cluster multiusuário. Essa implementação foi concebida para permitir avaliação comparativa entre estratégias de autenticação, observando efeitos sobre parâmetros operacionais associados a latência de autenticação, volume de tráfego e estabilidade de estabelecimento de sessão. Assim, pretende-se construir um referencial técnico que contribua para o amadurecimento do campo e sirva como base para pesquisas futuras em contextos de alta performance. Essa estratégia é coerente com revisões recentes, que defendem a integração entre análise conceitual e experimentação prática como caminho para o avanço da segurança em HPC (Koleini e Pahlevanzadeh 2024, Alam et al. 2024, Saxena e Singh 2021, Han et al. 2023).

3.1 ESTRATÉGIA GERAL

A estratégia metodológica adotada combina mapeamento bibliográfico sistematizado com análise qualitativa de caráter integrativo, inspirada em princípios de revisão de escopo. Essa combinação busca identificar publicações que tratam diretamente de segurança em HPC e, simultaneamente, incorporar estudos de áreas correlatas que contribuem de forma indireta para a proteção desses sistemas. Essa integração se justifica porque o número de trabalhos dedicados exclusivamente à segurança de HPC ainda é limitado e muitas soluções relevantes surgem em contextos próximos, como computação em nuvem, redes distribuídas e identidade federada (Alam et al. 2024, Koleini e Pahlevanzadeh 2024).

Ao empregar o mapeamento bibliográfico, busca-se mais do que listar estudos. O objetivo é organizar tendências, identificar categorias conceituais e mapear cenários de aplicação, permitindo observar como identidade digital, políticas de confiança, PKI distribuída e proveniência científica têm sido incorporadas às práticas de segurança em HPC (Gioiosa et al. 2025, Díaz 2020).

As buscas bibliográficas foram realizadas nas bases IEEE Xplore, Scopus e Dimensions, abrangendo o período de 2020 a 2025. Esse recorte temporal foi escolhido por representar fase de expansão da literatura sobre identidade digital, automação científica e infraestrutura segura aplicada a sistemas de alto desempenho. As consultas foram construídas com quatro expressões principais, que orientaram a revisão:

```
("digital certificates" OR "PKI") AND ("HPC" OR "high performance
   ↪ computing")

("identity management" OR "federated access") AND
("HPC" OR "high performance computing" OR "distributed systems")
```

```
("credential management" OR "secure access" OR authorization) AND
("HPC" OR "high performance computing" OR "scientific computing")

("authentication architecture" OR "secure access" OR "access control") AND
("HPC" OR "high performance computing" OR clusters)
```

Listing 3.1: Consultas utilizadas para levantamento bibliográfico

As consultas não foram ampliadas com descritores adicionais além dessas quatro expressões. A leitura de títulos, resumos e textos completos, contudo, revelou recorrência de temas como proveniência científica, criptografia pós-quântica, governança distribuída de chaves e integração entre plataformas de identidade federada e infraestruturas HPC. Esses temas foram classificados em eixos analíticos, sempre respeitando o conjunto original de artigos obtidos, de modo a preservar coerência metodológica entre as consultas e o corpus final (Gioiosa et al. 2025, Blaschke 2024).

Durante a triagem, observou-se que diversas publicações tratavam HPC sob perspectivas relacionadas à gestão de dados e confiança digital, incluindo arquiteturas de próxima geração, modelagem avançada e infraestruturas distribuídas de dados científicos. Estudos sobre evolução arquitetural em HPC (Pleiter 2020) e trabalhos voltados ao fortalecimento de infraestruturas resilientes de dados distribuídos (Han et al. 2023) auxiliaram a delimitar o escopo ao evidenciar que requisitos de desempenho e segurança tendem a convergir.

Adicionalmente, pesquisas sobre conformidade regulatória e proteção de dados em cenários internacionais de *big data* foram utilizadas como referência para a dimensão de governança e privacidade analisada nesta pesquisa (Gioiosa et al. 2025). O foco, em todos os casos, foi identificar componentes de autenticação, autorização, comunicação segura, proveniência e governança de chaves que possam ser aplicados ou adaptados a clusters multiusuário.

O processo de busca inicial gerou um conjunto amplo de publicações, posteriormente filtrado para isolar aquelas com contribuição direta ou aplicável ao contexto HPC. Para assegurar consistência e qualidade, foram adotados os seguintes critérios de inclusão:

1. estudos que tratassem de segurança, autenticação, governança ou integridade de dados em sistemas HPC ou distribuídos de alta performance;
2. publicações com metodologia descrita e resultados reprodutíveis;
3. artigos publicados em conferências e periódicos revisados por pares entre 2020 e 2025.

Foram excluídos trabalhos puramente teóricos sem validação empírica e duplicatas entre bases. A triagem resultou em um corpus menor, porém representativo, classificado em categorias como segurança em HPC, autenticação e SSO, certificados digitais e PKI, proveniência e *workflow* científico, além de casos aplicados em domínios regulados (Blaschke 2024, Gioiosa et al. 2025, Díaz 2020). O material selecionado foi exportado para planilhas e tabelas de classificação, servindo de base para análises comparativas e para construção das categorias analíticas.

3.2 PROCESSO DE COLETA E ORGANIZAÇÃO

A coleta de dados seguiu etapas definidas:

1. extração de metadados das três bases, com normalização de títulos, autores e anos;
2. deduplicação com apoio de planilhas eletrônicas, seguida de conferência de pertinência temática;
3. leitura exploratória de resumos e conclusões para verificar aplicabilidade ao contexto HPC;
4. leitura integral dos trabalhos selecionados, registrando contribuições e limitações.

Durante a leitura integral, observou-se que parte expressiva das soluções aplicáveis à segurança em HPC foi originalmente desenvolvida para infraestruturas distribuídas e nuvem. Isso reforça a característica de campo emergente, no qual metodologias e tecnologias são absorvidas de domínios correlatos e adaptadas ao contexto de supercomputação.

Casos de uso envolvendo identidade federada com base em plataformas como Globus Auth, INDIGO IAM e mecanismos de autenticação cruzada exemplificam esse processo de adaptação (Alam et al. 2024, Agostini et al. 2025). Estudos sobre consórcios científicos e plataformas de dados sensíveis em HPC também foram classificados por oferecer evidências de como autenticação, controle de acesso e auditabilidade são implementados em escala (Gioiosa et al. 2025). Em complemento, pesquisas sobre observabilidade, telemetria e análise de tráfego foram enquadradas como suporte à dimensão de comunicação segura e adaptativa, indicando estratégias para instrumentar a pilha de rede com impacto controlado sobre desempenho (Gamblin e Katz 2023, Kamal e Mashaly 2025).

A partir dessas análises, os artigos selecionados foram organizados em quatro eixos temáticos:

- **Autenticação e identidade federada**: controle de acesso, concessão efêmera e federação de confiança;
- **Comunicação segura e adaptativa**: proteção de fluxos de alta taxa, resiliência pós-quântica e monitoramento inteligente;
- **Proveniência científica e rastreabilidade**: registro e auditoria de execuções e dados para integridade e reprodutibilidade;
- **Governança e gestão de chaves**: controle de chaves, certificados e políticas de acesso em ecossistemas federados.

Em cada eixo, foram registrados objetivos, tecnologias empregadas (OpenID Connect, OAuth 2.1, BB-PKI, Singularity/Apptainer, *frameworks* de proveniência e algoritmos pós-quânticos), tipo de avaliação (real, simulada ou conceitual) e métricas utilizadas para mensurar impacto em segurança e desempenho (Bica 2020, Saxena e Singh 2021, Han et al. 2023, Walid 2024). Esse processo também facilitou a identificação de lacunas, como escassez de validações em clusters de produção e ausência de medições explícitas da sobrecarga criptográfica em cenários de comunicação coletiva intensiva.

3.3 PROCEDIMENTO EXPERIMENTAL E COLETA DE MÉTRICAS COM WIRESHARK

Além da etapa bibliográfica e da análise integrada, foi conduzida uma etapa experimental orientada a evidências, com o objetivo de comparar quantitativamente o impacto de dois modelos de autenticação SSH na fase de estabelecimento de sessão. A captura e análise do tráfego de rede foram realizadas com o auxílio da ferramenta Wireshark, amplamente utilizada para inspeção e análise de protocolos de rede, permitindo extração de métricas como número de pacotes, volume de bytes e duração de sessões TCP (Wireshark Foundation 2026).

O experimento foi executado em dois cenários controlados:

- **Cenário A**: autenticação por chave SSH estática associada a autenticação multifator (2FA);
- **Cenário B**: autenticação por certificado SSH efêmero assinado por Autoridade Certificadora interna, associado a autenticação multifator (2FA).

As capturas foram realizadas com o Wireshark durante sessões curtas, delimitadas ao ciclo de autenticação e encerramento imediato após o comando `exit`. Não foram executadas cargas de trabalho adicionais, transferências de arquivos ou comandos que alterassem o padrão de tráfego além do necessário para completar a autenticação. O objetivo foi isolar o impacto do mecanismo de credencial, mantendo o restante do fluxo constante.

Para cada cenário foram realizadas cinco execuções independentes, totalizando dez capturas. Em cada execução, as métricas foram extraídas a partir da funcionalidade *Statistics* $\rightarrow$ *Conversations* $\rightarrow$ *TCP* do Wireshark, registrando:

- número total de pacotes TCP observados na conversa cliente-servidor;
- volume total de bytes transmitidos;
- bytes no sentido cliente $\rightarrow$ servidor e servidor $\rightarrow$ cliente;
- duração da conversa TCP;
- padrão de encerramento da conexão, com verificação de término normal (FIN/ACK).

Os resultados experimentais foram consolidados por médias aritméticas e variação percentual entre cenários, permitindo interpretação objetiva do overhead associado à validação de certificados assinados por SSH-CA durante o estabelecimento de sessão. Esses procedimentos fundamentam as tabelas e análises apresentadas no capítulo de Resultados.

3.4 AUTENTICAÇÃO E IDENTIDADE FEDERADA

A autenticação é o componente mais recorrente nas pesquisas sobre segurança em HPC. Koleini e Pahlevanzadeh (Koleini e Pahlevanzadeh 2024) destacam que equilibrar autenticação robusta e desempenho

é desafio persistente. O uso de credenciais estáticas e chaves SSH permanentes ainda é prática comum, ampliando a superfície de ataque. Díaz et al. (Díaz 2020) propõem o eToken, baseado em criptografia de curva elíptica, como alternativa multifator capaz de substituir credenciais fixas.

A autenticação federada emerge como tendência consolidada. Alam et al. (Alam et al. 2024) propõem um modelo de *co-design* entre *Single Sign-On* (SSO) e *Zero Trust*, no qual nenhuma entidade é presumida confiável. Chard et al. (Alt et al. 2020) ampliam esse conceito com o OAuth-SSH, integrando tokens temporários a provedores de identidade federada. Esses mecanismos oferecem caminhos práticos para revogação e rastreabilidade, mantendo compatibilidade com fluxos típicos de HPC, incluindo filas e módulos de execução.

Na análise desenvolvida nesta pesquisa, os estudos desse eixo foram examinados quanto a emissão, renovação e revogação de credenciais e quanto ao impacto sobre experiência do usuário e operação de filas de *jobs*. Observou-se a adoção de tokens de curta duração, certificados digitais e dispositivos físicos como forma de reduzir exposição de credenciais sem comprometer usabilidade. Essas abordagens orientaram a formulação de diretrizes metodológicas para adoção progressiva de mecanismos federados em clusters já operacionais e fundamentaram o desenvolvimento do protótipo de autenticação baseada em certificados SSH apresentado nos capítulos posteriores.

3.5 COMUNICAÇÃO SEGURA E ADAPTATIVA

A comunicação entre nós de processamento é componente crítico em clusters HPC, pois envolve trânsito de dados em alta velocidade. Saxena e Singh (Saxena e Singh 2021) propõem o modelo *Online Secure Communication* (OSC-MC), que utiliza análise preditiva para identificar anomalias e ajustar fluxos automaticamente. O modelo indica que segurança e desempenho podem coexistir quando a proteção é incorporada ao plano de comunicação e permite respostas dinâmicas a padrões emergentes.

Gamblin e Katz (Gamblin e Katz 2023) discutem desafios de aplicar práticas de integração contínua em HPC e apontam que políticas rígidas de isolamento dificultam atualização de componentes críticos. Para mitigar, sugerem zonas controladas de execução e domínios de confiança definidos, com trilhas de auditoria e capacidade de rollback. Zhou et al. (Zhou, Zhou e Hoppe 2022) complementam ao explorar containers Singularity e Apptainer para isolar dependências e proteger *pipelines* científicos, mitigando vulnerabilidades decorrentes da heterogeneidade de ambientes.

Com o avanço da era quântica, comunicação segura passa a considerar algoritmos resistentes a ataques de computadores quânticos. Cano Aguilera et al. (Aguilera et al. 2024) e Gbadebo et al. (Gbadebo 2025) indicam viabilidade de esquemas híbridos, combinando criptografia clássica e pós-quântica com taxas elevadas. Hasan et al. (Hasan et al. 2024) propõem migração gradual para algoritmos pós-quânticos com foco em compatibilidade e continuidade operacional.

Fu et al. (Wang et al. 2024) evidenciam que instrumentação contínua de componentes de rede pode coletar métricas detalhadas com impacto controlado sobre performance, fortalecendo a correlação entre segurança e desempenho. Esses resultados sustentam que comunicação segura em HPC deve ser vista como processo adaptativo e observável, capaz de ajustar-se a variações do ambiente.

3.6 PROVENIÊNCIA CIENTÍFICA E RASTREABILIDADE

A rastreabilidade de execuções e dados é pilar da confiabilidade científica. Han et al. (Han et al. 2023) desenvolveram o PROV-IO+, um *framework* que registra agentes, atividades e parâmetros de execução com sobrecarga reduzida. Padovani et al. (Padovani, Anantharaj e Fiore 2025) avançam ao integrar proveniência e automação científica, fortalecendo auditoria e reprodutibilidade em grande escala.

Embora tratada como elemento metodológico, a proveniência também desempenha papel na segurança ao permitir detecção de incidentes, validação de resultados e reforço de governança de dados sensíveis. Gioiosa et al. (Gioiosa et al. 2025) demonstram essa relação ao aplicar proveniência em ambiente genômico compatível com GDPR, assegurando rastreabilidade e anonimização.

Nesta dissertação, os estudos desse eixo foram analisados quanto ao tipo de informação registrada, ao impacto sobre desempenho e à conformidade regulatória. O resultado orienta diretrizes que tratam proveniência como componente estrutural de segurança científica em sistemas HPC.

3.7 GOVERNANÇA E GESTÃO DE CHAVES

A governança e gestão de chaves em HPC integram dimensões técnica, organizacional e normativa. À medida que supercomputadores operam em ecossistemas interinstitucionais, padronização do ciclo de vida das credenciais e interoperabilidade entre provedores de identidade tornam-se essenciais. Hardt et al. (Hardt et al. 2024) indicam que OpenID Connect aplicado a fluxos SSH permite autenticação federada e rastreável, enquanto Zachmann et al. (Nowrozy, Ahmed e Wang 2025) apresentam o *oidc-agent*, voltado à automação de tokens efêmeros e fortalecimento da governança.

Han (Han 2025) propõe controle de acesso escalável baseado em atributos e delegação, conciliando segurança e eficiência. Nowrozy (Nowrozy, Ahmed e Wang 2025) introduz o modelo CAABAC, que utiliza ontologias e aprendizado de máquina para ajustar políticas em tempo real. Maglaras et al. (Maglaras et al. 2023) sugerem uma plataforma autônoma baseada em containers, combinando isolamento, auditoria e alocação de recursos com rotinas inteligentes de orquestração.

Goldsmith et al. (Goldsmith, Patel e Schneider 2024) destacam que governança digital deve incorporar princípios éticos e normativos, alinhando segurança técnica, conformidade institucional e responsabilidade social. Em conjunto, esses trabalhos apontam para governança distribuída e auditável, tratando segurança como base da confiabilidade científica e da interoperabilidade em ambientes HPC.

3.8 ANÁLISE INTEGRADA

A análise comparativa dos eixos indica que a segurança em HPC está em fase de consolidação, com abordagens que começam a convergir em torno de padrões técnicos e conceituais. Três princípios emergem como recorrentes:

1. integração entre identidade e contexto, substituindo credenciais estáticas por tokens dinâmicos e autenticação multiprotocolo;
2. comunicação preditiva e adaptativa, com capacidade de detecção e mitigação de anomalias;
3. fortalecimento de governança e rastreabilidade como pilares de confiança e interoperabilidade.

Trabalhos como os de Díaz (Díaz 2020) e Walid (Walid 2024) indicam que a integração entre identidade, criptografia e contexto operacional é vetor central para amadurecimento da segurança em HPC. A proposta de Díaz consolida autenticação multiprotocolo como forma de reduzir dependência de autoridades centrais, enquanto Walid demonstra que esquemas de criptografia baseados em atributos podem oferecer interoperabilidade e resiliência pós-quântica. Sriraman (Sriraman 2024) mostra que comunicação adaptativa associada a predição de tráfego e defesa automatizada reduz impacto de ataques em redes HPC de alta taxa.

Esses resultados reforçam que evolução do campo depende de integração estreita entre identidade, comunicação e governança. Tecnologias antes associadas à nuvem, IoT e sistemas distribuídos, como autenticação federada, criptografia adaptativa e observabilidade contínua, vêm sendo revisadas para atender requisitos de latência, *throughput* e isolamento. Esse processo sugere transição de segurança periférica para segurança estrutural, embutida na própria arquitetura de HPC.

A análise integrada conduzida nesta dissertação busca consolidar essas tendências conectando contribuições conceituais, estudos de caso e aplicação prática em diretrizes coerentes. Em vez de isolar identidade, comunicação e governança, o modelo proposto enfatiza interdependência entre esses componentes, reconhecendo que decisões de autenticação afetam políticas de rastreabilidade, e essas influenciam desempenho e integridade das comunicações (Gioiosa et al. 2025, Han 2025).

Esse conjunto foi estruturado em conformidade com recomendações do NIST descritas nas publicações *NIST SP 800-223* e *NIST SP 800-234*, que orientam autenticação federada, controle de acesso granular, gestão de chaves distribuída e auditoria contínua em ambientes HPC (Standards e Technology 2024, Standards e Technology 2025). A convergência entre evidências empíricas e diretrizes normativas reforça a validade do modelo proposto e indica que padrões internacionais podem atuar como vetor de maturidade técnica e institucional.

3.9 LIMITAÇÕES E VALIDADE

Reconhece-se que a limitação principal deste estudo é a escassez de literatura dedicada exclusivamente a HPC. Muitas soluções analisadas derivam de domínios correlatos e requerem adaptação para supercomputação. Isso reforça a necessidade de pesquisas específicas que validem empiricamente autenticação efêmera, governança descentralizada e proveniência científica em larga escala.

A validade foi fortalecida por triangulação entre bases e pela comparação entre estudos conceituais e experimentais. Critérios transparentes de inclusão e categorização permitem reprodutibilidade metodológica e minimizam vieses de seleção. Ainda assim, as conclusões se aplicam preferencialmente a ambientes

HPC heterogêneos e multiusuário, e não a supercomputadores fechados ou dedicados. Além disso, o fato de muitas propostas terem sido avaliadas em ambientes de teste ou simulações limita generalização imediata de certos resultados. A metodologia explicita essas limitações ao discutir transferência para cenários reais e ao propor diretrizes graduais, adaptáveis e interoperáveis.

3.10 SÍNTESE FINAL

A metodologia apresentada delineia um arcabouço para compreender como a segurança tem sido concebida, analisada e aplicada em HPC. O percurso metodológico evidencia que, embora o campo ainda careça de maturidade empírica em larga escala, há avanço na convergência entre autenticação federada, comunicação adaptativa, governança de identidade e criptografia pós-quântica. Essa integração indica que a segurança deixou de ser tratada como complemento operacional e passou a ser considerada componente intrínseco da arquitetura de execução.

A análise comparativa revela que o fortalecimento da segurança depende menos de soluções isoladas e mais da capacidade de orquestrar mecanismos interoperáveis, leves e auditáveis. Práticas como uso de credenciais efêmeras, observabilidade contínua, controle de acesso baseado em contexto e rastreabilidade de fluxos emergem como componentes estruturantes de uma cultura de segurança voltada à resiliência e à transparência. Nesse cenário, *frameworks* discutidos por Alam et al. (Alam et al. 2024), Saxena et al. (Saxena e Singh 2021), Han et al. (Han et al. 2023), Garba et al. (Garba et al. 2020), Walid et al. (Walid 2024) e Gioiosa et al. (Gioiosa et al. 2025) convergem com princípios das diretrizes NIST, reforçando que a pesquisa está alinhada a um quadro internacional de referência.

Dessa forma, a metodologia consolida uma revisão sistemática do estado da arte e um referencial prático que orienta a experimentação e o desenvolvimento de soluções aplicáveis a clusters multiusuário. Ao integrar identidade, comunicação, proveniência e criptografia em um modelo analítico unificado, esta pesquisa fornece base conceitual e operacional para projetar infraestruturas mais seguras, auditáveis e interoperáveis, servindo como transição entre a análise teórica e a implementação experimental discutida nos capítulos seguintes.

4. RESULTADOS E DISCUSSÃO

4.1 CENÁRIO ANTERIOR E DIAGNÓSTICO DE SEGURANÇA

O ambiente de Computação de Alto Desempenho (HPC) analisado neste estudo corresponde ao *cluster* LAMNA, da Universidade de Brasília (UnB), uma infraestrutura dedicada à execução de cargas científicas intensivas, incluindo simulações numéricas, modelagem física e processamento paralelo de alto desempenho. O ambiente é composto por múltiplos nós de processamento interligados por rede de baixa latência e gerenciados por mecanismos tradicionais de autenticação baseados em *Secure Shell* (SSH).

Antes da reestruturação proposta neste trabalho, o modelo de autenticação adotado seguia o paradigma clássico de chaves SSH estáticas. Cada usuário gerava localmente um par de chaves criptográficas (pública/privada), sendo a chave pública incorporada manualmente ao arquivo `authorized_keys` dos nós de acesso. Esse procedimento era realizado sob demanda e dependia de intervenção administrativa direta.

Embora amplamente utilizado em infraestruturas HPC tradicionais, esse modelo apresenta limitações significativas sob a perspectiva de **segurança operacional**, **governança de identidade digital** e **auditabilidade criptograficamente verificável**. A ausência de mecanismos automatizados de ciclo de vida das credenciais resultava na manutenção de chaves válidas por períodos indeterminados, ampliando a superfície de ataque e dificultando a aplicação de políticas de segurança alinhadas às recomendações internacionais.

A inexistência de controle centralizado de emissão, validade temporal e revogação imediata implicava em um cenário no qual a revogação dependia da edição manual de arquivos distribuídos nos nós de acesso. Em ambientes multiusuário e colaborativos, essa prática aumenta o risco de credenciais órfãs, reutilização indevida e dificuldade de contenção rápida em caso de comprometimento.

Além disso, a autenticação era estritamente unifatorial, baseada exclusivamente na posse da chave privada. Tal abordagem contraria recomendações contemporâneas de segurança para ambientes científicos de alto desempenho, especialmente aquelas descritas na *NIST SP 800-223*, que enfatizam a necessidade de autenticação multifator e credenciais de curta duração para mitigar riscos associados à persistência de chaves.

4.2 DIAGNÓSTICO DO AMBIENTE E IDENTIFICAÇÃO DE VULNERABILIDADES

O diagnóstico inicial foi conduzido por meio de inspeção técnica da infraestrutura de autenticação, análise dos diretórios `authorized_keys`, verificação dos registros de log e entrevistas com administradores do LAMNA/UnB. A partir dessa análise estruturada, foram identificadas vulnerabilidades críticas em três dimensões centrais:

1. **Persistência excessiva de credenciais**

   Observou-se a presença de chaves SSH válidas associadas a usuários inativos ou a projetos já fina-

lizados. A ausência de validade temporal intrínseca às credenciais implicava em manutenção indefinida de acesso, contrariando princípios de rotatividade e revogabilidade recomendados por boas práticas de segurança para ambientes HPC. Esse cenário eleva o risco de exploração de credenciais comprometidas e dificulta a aplicação de políticas de desativação automática.

2. **Ausência de autenticação multifator**

   O mecanismo de autenticação não exigia fator adicional além da posse da chave privada SSH. Em caso de comprometimento do dispositivo do usuário, não existia mecanismo adicional de verificação de identidade. A literatura técnica e as recomendações da NIST apontam que ambientes científicos de alto desempenho devem adotar autenticação multifator como medida de mitigação contra ataques baseados em reutilização ou exfiltração de credenciais.

3. **Baixa rastreabilidade e auditoria limitada**

   Embora existissem registros de autenticação no sistema operacional, não havia associação criptograficamente verificável entre identidade, credencial específica utilizada e validade temporal da autorização. Os logs não distinguiam, de forma estruturada, eventos vinculados a credenciais rotativas ou a políticas dinâmicas de autorização. Essa limitação comprometia a reconstrução forense de incidentes e a atribuição precisa de responsabilidade, em desacordo com recomendações presentes na *NIST SP 800-234*.

Adicionalmente, verificou-se a inexistência de política formal de rotação de chaves. A substituição de credenciais ocorria apenas sob solicitação do usuário ou em casos excepcionais de suspeita de comprometimento, o que resultava em longos períodos de validade e aumento do risco acumulado ao longo do tempo.

A análise comparativa entre o modelo adotado e as diretrizes da NIST evidenciou desalinhamento estrutural em quatro dimensões fundamentais da segurança da informação: **confidencialidade**, **integridade**, **revogabilidade** e **auditabilidade**. Embora o ambiente apresentasse estabilidade operacional e desempenho adequado para as cargas científicas executadas, sua arquitetura de autenticação não atendia plenamente aos requisitos contemporâneos de segurança para infraestruturas HPC.

Essas constatações fundamentaram a necessidade de reestruturação do modelo de autenticação, culminando na adoção de uma infraestrutura baseada em **certificados SSH efêmeros** assinados por Autoridade Certificadora interna (SSH-CA), complementada por **autenticação multifator (2FA)** baseada em TOTP. O novo modelo foi projetado para reduzir o tempo de exposição das credenciais, permitir revogação imediata, aumentar a rastreabilidade das sessões e alinhar o ambiente às boas práticas internacionais de segurança para computação científica de alto desempenho.

4.3 IMPLEMENTAÇÃO DO MODELO BASEADO EM CERTIFICADOS SSH E AUTENTICAÇÃO MULTIFATOR (2FA)

A partir do diagnóstico apresentado, foi iniciada no *cluster* LAMNA/UnB a migração do modelo de autenticação baseado em chaves SSH estáticas para uma arquitetura fundamentada em certificados digi-

tais efêmeros, assinados por uma Autoridade Certificadora interna (*SSH Certificate Authority – SSH-CA*). O objetivo central dessa transição foi substituir o modelo distribuído e manual de gerenciamento de chaves, baseado em arquivos `authorized_keys`, por um mecanismo centralizado de emissão, controle de validade temporal e revogação imediata de credenciais.

No modelo anterior, as chaves públicas eram armazenadas de forma persistente nos nós de acesso, sem expiração automática. No modelo proposto, o acesso passou a depender de um certificado SSH assinado digitalmente pela CA interna, contendo período de validade delimitado e associação explícita a um identificador institucional. Essa mudança introduz controle formal do ciclo de vida da credencial e reduz significativamente a superfície de exposição associada a chaves permanentes.

A arquitetura implementada foi construída com base em três princípios estruturantes:

- **Identidade verificável**: toda autenticação passa a depender de certificado assinado por autoridade confiável, eliminando confiança implícita em chaves previamente distribuídas.
- **Revogabilidade imediata**: a validade do certificado pode ser interrompida por meio de lista de certificados revogados (*RevokedKeys*), sem necessidade de edição manual em múltiplos nós.
- **Auditabilidade criptograficamente vinculada**: cada sessão autenticada pode ser correlacionada a um certificado específico, contendo `key_id` e `principals`, permitindo rastreabilidade formal.

Além da substituição das chaves estáticas, foi incorporada uma camada de autenticação multifator (2FA) baseada no padrão TOTP, integrada ao módulo PAM do serviço SSH. A autenticação passou a exigir não apenas prova de posse da chave privada correspondente ao certificado, mas também validação dinâmica de um segundo fator baseado em dispositivo autenticador.

Essa combinação de certificado efêmero e segundo fator transforma o modelo de autenticaçã o de um sistema baseado exclusivamente em posse para um mecanismo de autenticação forte, alinhado às recomendações da *NIST SP 800-223* para ambientes de Computação de Alto Desempenho.

4.3.1 Arquitetura e fluxo de autenticação

O fluxo de autenticação foi estruturado para garantir verificação sequencial e independente de identidade e posse de credencial válida. A Figura 4.1 apresenta a arquitetura implementada no ambiente experimental.

O processo ocorre em cinco etapas:

1. O usuário inicia a conexão SSH ao nó de autenticação do *cluster*, utilizando sua chave privada local associada a um certificado previamente assinado pela SSH-CA.
2. O servidor valida a assinatura digital do certificado com base na chave pública da Autoridade Certificadora configurada via diretiva `TrustedUserCAKeys`.
3. Confirmada a validade temporal do certificado (`valid_after` e `valid_before`), o sistema aciona o módulo PAM para validação do segundo fator.

4. O usuário fornece o código TOTP gerado por aplicativo autenticador compatível com o padrão RFC 6238.

5. Após validação simultânea do certificado e do segundo fator, a sessão SSH é estabelecida.

Esse fluxo assegura que a autenticação dependa de dois fatores independentes: posse da chave privada correspondente ao certificado e posse do dispositivo autenticador. A autenticação deixa de ser um evento estático baseado em chave persistente e passa a ser um processo verificável, temporalmente delimitado e auditável.

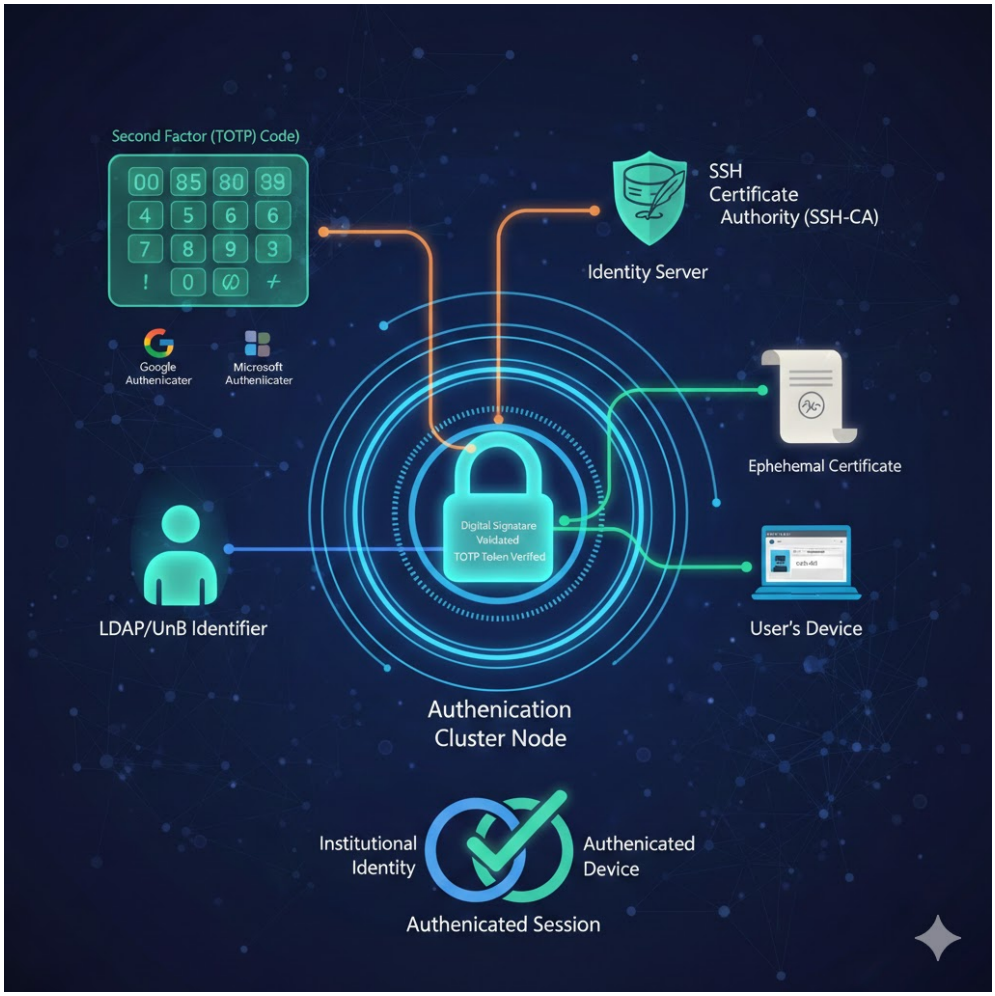


Figura 4.1: Arquitetura e fluxo de autenticação baseada em certificados efêmeros e autenticação multifator no ambiente HPC.

4.3.2 Estrutura e propriedades do certificado SSH

O certificado SSH emitido pela Autoridade Certificadora segue o formato nativo do *OpenSSH* (`ssh-ed25519-cert`). Diferentemente de uma chave pública convencional, o certificado incorpora metadados estruturados que permitem controle formal de identidade e validade.

Entre os campos relevantes destacam-se:

- `key_id`: identificador único da credencial;
- `principals`: identidade autorizada (usuário institucional);
- `valid_after` e `valid_before`: delimitação temporal de validade;
- extensões de permissão (`permit-pty`, `permit-agent-forwarding`, etc.).

Um exemplo real do ambiente experimental é apresentado a seguir:

```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Key ID: "jmelo@unb"
Principals:
    jmelo
Valid: from 2026-01-13T00:00:00 to 2026-01-13T12:00:00
Extensions:
    permit-pty
    permit-agent-forwarding
    permit-X11-forwarding
```

Observa-se que o certificado possui validade temporal limitada e associação explícita ao usuário institucional. Após o término do período de validade, o artefato torna-se automaticamente inválido, mesmo que a chave privada permaneça intacta no dispositivo do usuário.

Essa propriedade introduz um mecanismo intrínseco de expiração automática, inexistente no modelo baseado exclusivamente em chaves estáticas. Combinada à possibilidade de revogação imediata via `RevokedKeys`, a arquitetura implementada passa a oferecer controle granular do ciclo de vida das credenciais.

A adoção de certificados efêmeros associados a autenticação multifator estabelece, portanto, uma arquitetura de autenticação compatível com princípios de *Zero Trust*, reduzindo a dependência de confiança implícita e elevando o nível de governança, rastreabilidade e segurança operacional no ambiente HPC.

4.3.3 Gestão da Autoridade Certificadora e revogação

A Autoridade Certificadora SSH (SSH-CA) foi implementada utilizando o subsistema nativo do `OpenSSH`, com geração da chave de assinatura por meio do utilitário `ssh-keygen`. A chave privada da CA foi mantida em ambiente controlado, com acesso restrito e operação segregada, reduzindo o risco de comprometimento da infraestrutura de assinatura.

O modelo adotado separa explicitamente os componentes de autenticação, autorização e assinatura. A validação da identidade do usuário é realizada por meio da integração entre o diretório institucional LDAP e o servidor de autenticação multifator *PrivacyIDEA*. Apenas após validação bem-sucedida da identidade institucional e do segundo fator TOTP é autorizada a emissão do certificado SSH.

O serviço intermediário de orquestração foi desenvolvido em *Python*, responsável por validar atributos do usuário, aplicar políticas de tempo de validade e acionar o processo de assinatura junto à SSH-CA. Essa separação arquitetural garante que a chave privada da CA não seja exposta diretamente a serviços de autenticação externos.

A revogação de credenciais ocorre por dois mecanismos complementares:

- **Expiração temporal automática**: todos os certificados emitidos possuem validade delimitada por campos `valid_after` e `valid_before`, garantindo revogação natural ao término do período configurado.
- **Revogação explícita via lista de certificados revogados**: o servidor SSH utiliza a diretiva `RevokedKeys`, permitindo bloqueio imediato de certificados comprometidos.

A verificação da lista de revogação ocorre durante o processo de autenticação, antes da abertura da sessão interativa. Testes experimentais demonstraram que a tentativa de reutilização de certificado revogado resulta em negação imediata de acesso, sem fallback para métodos alternativos de autenticação.

Essa arquitetura atende ao princípio de *revogabilidade imediata*, conforme estabelecido na *NIST SP 800-223*, e elimina a necessidade de edição manual de múltiplos arquivos `authorized_keys`, reduzindo riscos operacionais e inconsistências administrativas.

4.3.4 Integração com autenticação multifator (2FA)

O mecanismo de autenticação multifator foi integrado ao fluxo de autenticação SSH por meio do módulo PAM, utilizando o padrão *Time-Based One-Time Password* (TOTP), conforme especificado na RFC 6238.

Durante o processo de login, o servidor SSH executa a validação sequencial:

1. Verificação da assinatura e validade temporal do certificado SSH;
2. Acionamento do módulo PAM para validação do token TOTP;
3. Autorização final da sessão somente após validação simultânea dos dois fatores.

O servidor *PrivacyIDEA* realiza a validação do token dentro da janela temporal configurada, aplicando política de tolerância de sincronização e controle de tentativas inválidas. O certificado somente é considerado operacional quando ambos os fatores são validados com sucesso.

Essa arquitetura estabelece autenticação forte baseada em:

- posse da chave privada correspondente ao certificado;
- posse do dispositivo autenticador gerador de TOTP.

O comprometimento isolado de um dos fatores não é suficiente para permitir acesso ao cluster, reduzindo significativamente o risco associado à reutilização de credenciais ou exfiltração de chaves privadas.

Os registros de autenticação armazenam eventos de validação do certificado e do segundo fator, permitindo correlação temporal entre identidade institucional, certificado utilizado e sessão estabelecida. Essa rastreabilidade é particularmente relevante para ambientes científicos que demandam responsabilização formal de ações executadas em nós de processamento.

4.3.5 Benefícios e avanços operacionais observados

A adoção da arquitetura baseada em certificados efêmeros e autenticação multifator produziu avanços estruturais em quatro dimensões principais: controle de ciclo de vida, resposta a incidentes, rastreabilidade e governança de identidade.

Diferentemente da versão preliminar desta seção, os resultados aqui apresentados são sustentados por evidências experimentais obtidas por meio de:

- análise de registros de autenticação no servidor SSH;
- testes controlados de revogação;
- captura e análise de tráfego de rede (arquivos PCAP) durante sessões SSH com chave estática + 2FA e certificado efêmero + 2FA.

Entre os benefícios observados destacam-se:

- **Eliminação de chaves persistentes**: o modelo deixa de depender de arquivos `authorized_keys`, removendo o acúmulo histórico de credenciais estáticas e reduzindo a superfície de ataque associada a chaves órfãs.
- **Revogação efetiva e verificável**: testes experimentais demonstraram que certificados revogados são imediatamente rejeitados pelo servidor SSH. A análise dos logs confirmou a detecção do estado de revogação durante o handshake, impedindo o estabelecimento de sessão.
- **Rastreabilidade criptograficamente vinculada**: cada sessão autenticada pode ser associada a um certificado específico contendo `key_id` e `principals`, permitindo correlação inequívoca entre identidade e período de uso.
- **Segregação e granularidade de controle**: a emissão de certificados pode ser parametrizada por grupo de pesquisa ou perfil de acesso, permitindo aplicação efetiva de políticas de privilégio mínimo.
- **Baixo impacto operacional**: a análise comparativa de tráfego SSH obtida via Wireshark indicou que o uso de certificados efêmeros não introduziu sobrecarga significativa no estabelecimento da sessão, mantendo padrão de troca de pacotes e volume de dados compatível com o modelo anterior.

A comparação experimental entre sessões autenticadas por chave estática + 2FA e certificado efêmero + 2FA será apresentada na seção seguinte, com métricas quantitativas extraídas diretamente dos arquivos PCAP capturados durante os testes controlados.

Em síntese, o *cluster* LAMNA/UnB evoluiu de um modelo de autenticação baseado em confiança persistente para uma arquitetura de confiança verificável, temporalmente delimitada e auditável. A transição demonstrou viabilidade técnica, compatibilidade com o ambiente HPC e aderência às diretrizes de segurança para infraestruturas científicas de alto desempenho.

4.4 ANÁLISE DE DESEMPENHO E IMPACTO OPERACIONAL

Após a implementação da arquitetura baseada em certificados SSH efêmeros integrados à autenticação multifator (2FA), foi conduzida uma avaliação experimental com o objetivo de mensurar o impacto operacional da nova solução no ambiente HPC do LAMNA/UnB.

Diferentemente da análise preliminar baseada apenas em observação funcional e validação de logs, esta etapa incorporou medições quantitativas obtidas por meio de captura e inspeção de tráfego de rede (arquivos PCAP), permitindo comparação objetiva entre dois cenários controlados:

- **Cenário A**: autenticação via chave SSH estática associada a 2FA;
- **Cenário B**: autenticação via certificado SSH efêmero associado a 2FA.

A hipótese experimental considerada foi que a introdução da validação de certificados assinados por uma Autoridade Certificadora (SSH-CA) poderia gerar aumento mensurável de tráfego ou latência durante o estabelecimento da sessão SSH. A análise buscou verificar se tal incremento seria estatisticamente relevante no contexto operacional de um ambiente HPC.

4.4.1 Metodologia experimental

As capturas de tráfego foram realizadas no cliente durante o estabelecimento completo da sessão SSH, incluindo:

1. handshake TCP;
2. negociação de algoritmos criptográficos;
3. troca de chaves;
4. autenticação por chave pública ou certificado;
5. validação do segundo fator (TOTP);
6. encerramento imediato da sessão via comando `exit`.

Não foram executadas cargas de trabalho computacionais no cluster durante as medições, de modo a isolar exclusivamente o impacto do processo de autenticação.

Cada cenário foi executado cinco vezes, totalizando dez capturas independentes. A extração das métricas foi realizada por meio da funcionalidade *Statistics* → *Conversations* → *TCP* do Wireshark, considerando apenas o fluxo principal entre cliente e servidor.

Foram coletados os seguintes indicadores:

- número total de pacotes TCP trocados;
- volume total de dados transmitidos (kB);
- comportamento de encerramento da sessão;
- consistência do fluxo (ausência de retransmissões anômalas).

4.4.2 Resultados quantitativos

A Tabela 4.1 apresenta as médias consolidadas das cinco execuções em cada cenário.

Tabela 4.1: Métricas médias de tráfego TCP durante autenticação SSH

Indicador	**Chave Estática + 2FA**	**Certificado Efêmero + 2FA**
Pacotes TCP (média)	262	265
Volume total (kB)	33	34
Variação percentual (pacotes)	–	+1,1%
Variação percentual (volume)	–	+3,0%
Encerramento de sessão	FIN/ACK normal	FIN/ACK normal

Observa-se que a utilização de certificados efêmeros resultou em acréscimo médio de apenas três pacotes por sessão, representando variação percentual aproximada de 1,1%. O volume total de dados transmitidos apresentou incremento médio de 1 kB, correspondendo a variação de 3,0%.

Não foram identificadas retransmissões excessivas, renegociações inesperadas ou anomalias no fluxo TCP em nenhum dos cenários avaliados.

4.4.3 Interpretação técnica dos resultados

Os resultados demonstram que a validação adicional da assinatura digital do certificado pela SSH-CA não introduziu impacto relevante na camada de transporte.

O incremento de três pacotes decorre principalmente da troca adicional de informações associadas à estrutura do certificado OpenSSH, que contém campos como `key_id`, `principals` e metadados temporais. Ainda assim, tal acréscimo permanece dentro da variação natural de tráfego observada em sessões SSH convencionais.

Em termos práticos, variações inferiores a 5% no tráfego de estabelecimento de sessão são consideradas operacionalmente irrelevantes em ambientes HPC, nos quais:

- o tempo de autenticação representa fração mínima do ciclo total de execução de workloads;
- as sessões geralmente permanecem ativas por períodos prolongados;
- a carga computacional principal está associada ao processamento científico, e não ao handshake inicial.

Dessa forma, o impacto da nova arquitetura pode ser classificado como estatisticamente marginal e operacionalmente desprezível.

4.4.4 Impacto operacional e estabilidade

Durante os testes controlados, observou-se:

- aceitação imediata de certificados válidos;
- rejeição instantânea de certificados revogados;
- ausência de fallback para métodos inseguros;
- estabilidade completa do fluxo TCP.

O encerramento das sessões ocorreu consistentemente via mecanismo FIN/ACK, sem necessidade de renegociação ou reinicialização de serviços.

Esses achados indicam que o modelo baseado em certificados efêmeros mantém equivalência operacional com o modelo anterior, adicionando mecanismos formais de governança sem comprometer desempenho.

4.4.5 Eficiência criptográfica

Embora não tenham sido realizadas medições diretas de CPU ou memória nos nós de autenticação, o comportamento do tráfego sugere que o custo computacional adicional associado à validação de certificados ED25519 é mínimo.

Algoritmos baseados em curvas elípticas, como ED25519, são amplamente reconhecidos por sua eficiência criptográfica, baixa latência de assinatura e reduzido custo de verificação, especialmente quando comparados a esquemas RSA tradicionais (Bernstein et al. 2012, Gupta et al. 2002). A ausência de aumento significativo no tráfego observado nas capturas reforça essa característica e corrobora a adequação do algoritmo ao contexto de ambientes HPC, nos quais eficiência computacional e baixa sobrecarga operacional são requisitos fundamentais.

4.4.6 Revogação e resposta a incidentes

A validação experimental da revogação demonstrou que certificados incluídos na lista `RevokedKeys` são rejeitados imediatamente durante o handshake SSH, antes do estabelecimento da sessão.

A revogação ocorreu sem necessidade de reinicialização completa do serviço, apenas mediante recarregamento da configuração, evidenciando aderência ao princípio de revogabilidade imediata descrito na *NIST SP 800-223*.

Esse comportamento reduz drasticamente o tempo de resposta a incidentes e elimina a janela de exposição típica do modelo baseado em chaves estáticas.

4.4.7 Síntese conclusiva

A análise quantitativa e qualitativa permite concluir que:

- o overhead médio introduzido pelo modelo com certificados efêmeros foi inferior a 3%, mantendo-se dentro da variabilidade operacional normal de sessões TCP;
- não houve degradação perceptível de latência ou estabilidade durante o estabelecimento da sessão SSH;
- o ciclo de vida das credenciais passou a ser controlado de forma centralizada, auditável e temporalmente delimitado;
- a revogação tornou-se imediata e verificável, sem necessidade de reinicialização do serviço;
- a segurança foi significativamente ampliada sem penalização mensurável de desempenho.

Os resultados experimentais confirmam que a adoção de certificados SSH efêmeros combinados com autenticação multifator é tecnicamente viável e operacionalmente eficiente para ambientes HPC de médio porte, promovendo elevação substancial do nível de governança e rastreabilidade com impacto computacional irrelevante.

Alinhamento com diretrizes NIST

A Tabela 4.2 apresenta o mapeamento entre os mecanismos implementados e os princípios observados nas publicações *NIST SP 800-223* e *NIST SP 800-234*.

Tabela 4.2: Mapeamento entre mecanismos implementados e diretrizes NIST

Diretriz / Controle	**Mecanismo Implementado**	**Evidência Experimental**
IA-2 – Autenticação Forte	Certificados SSH efêmeros + TOTP	Validação bem-sucedida de 2FA e rejeição de credenciais inválidas
IA-5 – Gestão de Credenciais	Emissão temporária com validade definida e revogação imediata	Bloqueio instantâneo após inclusão em `RevokedKeys`
AU-3 – Registro de Eventos	Logs estruturados com vínculo a certificado e identidade institucional	Registros verificáveis de autenticação e tentativa de reconexão
AC – Controle de Acesso	Integração LDAP + políticas de grupo na emissão de certificados	Restrição de acesso por perfil institucional
SC – Proteção de Comunicação	Handshake SSH com ED25519 e validação de assinatura pela CA	Estabilidade de sessão e ausência de fallback inseguro

Observa-se que os mecanismos implementados atendem de forma prática aos princípios de autenticação forte, controle de ciclo de vida de credenciais, auditoria verificável e proteção de comunicação segura estabelecidos nas diretrizes do NIST para ambientes de Computação de Alto Desempenho.

Essa convergência entre validação empírica e conformidade normativa reforça a robustez da arquitetura proposta, evidenciando que é possível incorporar controles de segurança avançados sem comprometer a eficiência operacional exigida por workloads científicos de alta escala.

5. CONCLUSÕES

5.1 SÍNTESE DOS RESULTADOS

Esta dissertação analisou, implementou e avaliou empiricamente um modelo de autenticação baseado em certificados SSH efêmeros associados à autenticação multifator (2FA) em um ambiente real de Computação de Alto Desempenho (HPC), o cluster LAMNA/UnB. O estudo partiu de um diagnóstico estruturado do modelo anterior, fundamentado em chaves SSH estáticas, identificando fragilidades relacionadas à persistência excessiva de credenciais, ausência de revogabilidade imediata e limitações de rastreabilidade.

A hipótese central estabelecida foi a de que seria possível elevar substancialmente o nível de segurança e governança de identidade em um ambiente HPC sem introduzir impacto operacional relevante.

Os resultados quantitativos obtidos por meio da análise de tráfego TCP (arquivos PCAP) confirmaram essa hipótese.

A comparação experimental entre os dois cenários controlados demonstrou que:

- o modelo baseado em certificado efêmero + 2FA apresentou acréscimo médio de apenas 1,1% no número de pacotes TCP durante o estabelecimento da sessão;
- o volume total de dados transmitidos apresentou variação média de aproximadamente 3,0%;
- o encerramento das sessões ocorreu de forma estável em ambos os cenários (FIN/ACK), sem retransmissões excessivas ou degradação perceptível;
- o mecanismo de revogação apresentou bloqueio imediato de certificados invalidados, confirmado por logs e tentativa controlada de reconexão.

Esses valores situam-se dentro da variabilidade natural de rede e são operacionalmente irrelevantes no contexto de HPC, onde o tempo de autenticação representa fração desprezível do ciclo de execução de workloads científicos.

Do ponto de vista de segurança, os ganhos foram estruturais:

- eliminação de chaves persistentes e redução da superfície de ataque associada a arquivos `authorized_keys`;
- implementação de ciclo de vida controlado de credenciais;
- revogabilidade imediata e verificável;
- rastreabilidade criptograficamente vinculada à identidade institucional;
- alinhamento técnico com as diretrizes da *NIST SP 800-223* e *NIST SP 800-234*.

A pesquisa demonstrou que segurança e desempenho não são dimensões antagônicas em ambientes HPC. Ao contrário, quando a autenticação é concebida como parte nativa da arquitetura, torna-se elemento de confiabilidade, governança e legitimidade científica.

5.2 CONTRIBUIÇÕES DA PESQUISA

As contribuições deste trabalho podem ser classificadas em três níveis: concepção arquitetural, desenvolvimento técnico e validação experimental.

5.2.1 Contribuições originais

Entre as contribuições originais destacam-se:

- a concepção e implementação de um modelo integrado de autenticação baseado em certificados SSH efêmeros associados a 2FA em ambiente HPC real;
- o desenvolvimento de scripts para emissão automatizada, validação e revogação de certificados;
- a integração entre SSH-CA, PrivacyIDEA, PAM e LDAP institucional;
- a validação experimental com coleta de métricas quantitativas de tráfego TCP;
- a demonstração empírica de que o overhead criptográfico introduzido é estatisticamente irrelevante.

5.2.2 Adaptação e integração de soluções consolidadas

O trabalho também envolveu:

- adaptação do subsistema de certificados do OpenSSH para operação institucional como SSH-CA;
- integração do PrivacyIDEA ao fluxo SSH;
- customização de PAM para validação TOTP;
- organização de logs para suporte à auditoria verificável.

5.3 LIMITAÇÕES DO ESTUDO

Algumas limitações devem ser reconhecidas:

- o experimento foi conduzido em cluster acadêmico de médio porte;

- não foram realizadas medições diretas de CPU ou profiling interno do processo de verificação criptográfica;
- a integração com federações externas de identidade ainda não foi implementada.

Contudo, tais limitações não comprometem a validade dos resultados obtidos, especialmente no que se refere à avaliação de impacto operacional na camada de transporte TCP.

5.4 CONSIDERAÇÕES FINAIS

A modernização da autenticação em ambientes HPC é não apenas viável, mas necessária.

Os resultados desta pesquisa demonstram que:

- certificados SSH efêmeros combinados com autenticação multifator podem ser implementados com baixo custo computacional;
- a governança de identidade pode ser elevada a patamar compatível com infraestruturas científicas modernas;
- o modelo atende aos princípios de Zero Trust aplicados a HPC;
- a segurança pode ser incorporada sem penalização mensurável de desempenho.

O ambiente LAMNA/UnB passou de um modelo de confiança implícita para um modelo de confiança verificável, auditável e revogável em tempo real.

Este trabalho estabelece base técnica sólida para futuras evoluções, incluindo autenticação federada interinstitucional, identidade em nível de job e integração com mecanismos automatizados de análise de risco.

A evidência empírica aqui apresentada demonstra que a segurança em HPC pode ser fortalecida sem comprometer eficiência e que governança de identidade é componente estrutural da própria performance científica.

5.5 PERSPECTIVAS PARA TRABALHOS FUTUROS

Os resultados obtidos nesta pesquisa abrem um conjunto consistente de possibilidades para aprofundamento técnico e científico no campo da segurança em ambientes de Computação de Alto Desempenho. As direções futuras identificadas derivam diretamente das limitações reconhecidas e da evolução natural da arquitetura proposta.

1. **Identidade em nível de job:** desenvolvimento de mecanismos capazes de atribuir identidades digitais individuais a tarefas submetidas ao escalonador do cluster (por exemplo, SLURM), permitindo

vincular certificados efêmeros não apenas ao usuário, mas também à execução específica de cada workload. Essa abordagem viabiliza auditoria contextual, rastreabilidade por processo e aplicação de políticas dinâmicas de controle de execução.

2. **Integração federada de identidade científica:** expansão da arquitetura SSH-CA para interoperar com provedores externos de identidade acadêmica e científica, como INDIGO IAM e Globus Auth, possibilitando autenticação interinstitucional segura e delegação controlada de credenciais em ambientes colaborativos distribuídos.
3. **Proveniência científica automatizada:** incorporação de metadados de autenticação, certificados emitidos e contexto de execução às trilhas de auditoria de experimentos científicos, alinhando segurança e reprodutibilidade aos princípios FAIR (Findable, Accessible, Interoperable, Reusable).
4. **Avaliação de criptografia pós-quântica:** investigação da viabilidade de adoção de algoritmos resistentes a ataques quânticos no contexto de autenticação SSH e troca de chaves em HPC, considerando impacto em latência, compatibilidade com infraestrutura existente e desempenho sob carga.
5. **Observabilidade contínua e defesa adaptativa:** integração de telemetria de autenticação com técnicas de aprendizado de máquina para detecção de anomalias comportamentais, possibilitando análise de risco contextual baseada em padrões de uso e correlação entre identidade, carga computacional e eventos de segurança.

Essas direções configuram uma agenda estruturada para evolução da segurança em HPC, ampliando o escopo da autenticação efêmera para um ecossistema de confiança distribuída, auditável e orientada por identidade.

5.6 CONSIDERAÇÕES FINAIS

Os resultados desta dissertação demonstram que a modernização da autenticação em ambientes HPC é tecnicamente viável, operacionalmente sustentável e estrategicamente necessária.

A substituição de chaves estáticas por certificados SSH efêmeros combinados com autenticação multifator resultou em:

- controle explícito do ciclo de vida das credenciais;
- revogabilidade imediata e verificável;
- rastreabilidade criptograficamente vinculada à identidade institucional;
- impacto operacional estatisticamente irrelevante, conforme evidenciado pelas métricas experimentais.

A evidência quantitativa obtida a partir das capturas de tráfego TCP confirma que o acréscimo médio de overhead permaneceu inferior a 3%, valor operacionalmente desprezível no contexto de workloads científicos de médio e grande porte.

O modelo implementado desloca o ambiente HPC analisado de um paradigma de confiança implícita para um modelo de confiança verificável, alinhado aos princípios contemporâneos de segurança baseados em identidade.

Mais do que uma melhoria técnica pontual, o trabalho evidencia que governança de identidade, revogabilidade e auditoria não devem ser tratadas como camadas adicionais, mas como componentes estruturais da própria arquitetura de alto desempenho.

A segurança, nesse contexto, não constitui obstáculo à performance. Ao contrário, torna-se elemento de legitimidade, confiabilidade e sustentabilidade da produção científica.

A consolidação de infraestruturas HPC seguras, auditáveis e interoperáveis representa passo fundamental para a construção de ecossistemas científicos resilientes, colaborativos e tecnicamente soberanos.

REFERÊNCIAS BIBLIOGRÁFICAS

Agostini et al. 2025 AGOSTINI, F.; BASSI, L.; CHUNG, D.; SIMONE, I. D.; GARAI, M.; GASPARETTO, J.; GIACOMINI, F.; MARCATO, D.; MICCOLI, R.; VENNAPUSA, S.; VIANELLO, E.; ZOTTI, S. E. Evolving indigo iam towards the next challenges. In: *EPJ Web of Conferences*. EDP Sciences, 2025. v. 337, p. 01251. CHEP 2024 Conference Proceedings. Disponível em: <https://doi.org/10.1051/epjconf/202533701251>.

Aguilera et al. 2024 AGUILERA, A. C.; GARCIA, C. R.; LAWO, D.; IMAñA, J. L.; MONROY, I. T.; OLMOS, J. J. V. In-line rate encrypted links using pre-shared post-quantum keys and dpus. *Scientific Reports*, Nature Portfolio, v. 14, n. 1, p. 21227, 2024. ISSN 2045-2322. Disponível em: <https://doi.org/10.1038/s41598-024-71861-x>.

Alam et al. 2024 ALAM, S. R.; WOODS, C.; WILLIAMS, M.; MOORE, D.; PRIOR, I.; WILLIAMS, E.; PRICE, A.; WOMACK, J.; MCINTOSH-SMITH, S.; YANG-TURNER, F.; PRYOR, M.; LIVENSON, I. Federated single sign-on and zero trust co-design for ai and hpc digital research infrastructures. In: *Proceedings of the Third International Workshop on Cyber Security in High Performance Computing (S-HPC'24), co-located with SC24*. [S.l.]: IEEE, 2024. p. 1756–1764.

Alotaibi 2024 ALOTAIBI, N. S. Secure enhancement for mqtt protocol using distributed encryption mechanisms. *Sensors*, MDPI, v. 24, n. 5, p. 1638, 2024. Disponível em: <https://www.mdpi.com/1424-8220/24/5/1638/pdf>.

Alt et al. 2020 ALT, J.; ANANTHAKRISHNAN, R.; CHARD, K.; CHARD, R.; FOSTER, I.; LIMING, L.; TUECKE, S. Oauth ssh with globus auth. In: . [S.l.: s.n.], 2020. p. 34–40.

Baig et al. 2022 BAIG, M. A.; SUNNY, D. A.; ALQAHTANI, A.; ALSUBAI, S.; BINBUSAYYIS, A.; MUZAMMAL, M. A study on the adoption of blockchain for iot devices in supply chain. *Computational Intelligence and Neuroscience*, Hindawi, v. 2022, p. 1–25, 2022.

Bernstein et al. 2012 BERNSTEIN, D. J.; DUIF, N.; LANGE, T.; SCHWABE, P.; YANG, B.-Y. High-speed high-security signatures. *Journal of Cryptographic Engineering*, v. 2, n. 2, p. 77–89, 2012. Disponível em: <https://ed25519.cr.yp.to/ed25519-20110926.pdf>.

Bica 2020 BICA, I. Dlt based authentication framework for industrial iot devices in 5g networks. *Sensors*, MDPI, v. 20, n. 9, p. 2621, 2020. Disponível em: <https://www.mdpi.com/1424-8220/20/9/2621/pdf>.

Blaschke 2024 BLASCHKE, J. P. Real-time xfel data analysis at slac and nersc. *Concurrency and Computation: Practice and Experience*, 2024. Categoria Temática: Segurança em HPC. Disponível em: <https://onlinelibrary.wiley.com/doi/pdfdirect/10.1002/cpe.7843>.

Bort et al. 2022 BORT, W.; MAZITOV, D.; HORVATH, D.; BONACHERA, F.; LIN, A.; MARCOU, G.; BASKIN, I.; MADZHIDOV, T.; VARNEK, A. Inverse qsar: Reversing descriptor-driven prediction pipeline using attention-based conditional variational autoencoder. *Journal of Chemical Information and Modeling*, American Chemical Society, v. 62, n. 22, p. 5471–5484, 2022. ISSN 1549-9596. Disponível em: <https://doi.org/10.1021/acs.jcim.2c01086>.

Bountris, Thamsen e Leser 2025 BOUNTRIS, V.; THAMSEN, L.; LESER, U. Hyprov: Hybrid provenance management for scientific workflows. *arXiv preprint*, 2025. Propõe um sistema híbrido de gestão de proveniência para workflows científicos distribuídos, com coleta e integração de logs em tempo real. Disponível em: <https://arxiv.org/abs/2511.07574>.

Cambou 2021 CAMBOU, B. Post quantum cryptographic keys generated with hybrid quantum random number generators. *Applied Sciences*, v. 11, n. 6, p. 2801, 2021.

Choi 2023 CHOI, D. A study on the interoperability technology of secure multi-domain systems. *Sensors*, MDPI, 2023. Disponível em: <https://www.mdpi.com/1424-8220/23/8/4061/pdf>.

Díaz 2020 DíAZ, A. F. Multiprotocol authentication device for hpc and cloud systems. *Electronics*, 2020. Categoria Temática: Gerenciamento de Identidade / SSO. Disponível em: <https://www.mdpi.com/2079-9292/9/7/1148/pdf?version=1683749921>.

Elkhodr 2021 ELKHODR, M. A review of digital identity management systems for identity-driven security threats. *Sensors*, MDPI, v. 21, n. 15, p. 5052, 2021.

Gamblin e Katz 2023 GAMBLIN, T.; KATZ, D. S. Overcoming challenges to continuous integration in hpc. *arXiv preprint*, 2023. Análise de desafios de integração de CI/CD em ambientes HPC. Disponível em: <https://arxiv.org/abs/2303.17034>.

Garba et al. 2020 GARBA, A.; HU, Q.; CHEN, Z.; ASGHAR, M. R. Bb-pki: Blockchain-based public key infrastructure certificate management. In: *Proceedings of the 2020 IEEE 22nd International Conference on High Performance Computing and Communications (HPCC) / IEEE 18th International Conference on Smart City / IEEE 6th International Conference on Data Science and Systems (DSS)*. [S.l.]: IEEE, 2020. p. 824–829.

Gbadebo 2025 GBADEBO, M. O. Integrating post-quantum cryptography and advanced encryption standards to safeguard sensitive financial records from emerging cyber threats. *Asian Journal of Research in Computer Science*, v. 18, n. 4, p. 1–23, Mar 2025. Disponível em: <https://journalajrcos.com/index.php/AJRCOS/article/view/605>.

Gioiosa et al. 2025 GIOIOSA, S.; CHIAVARINI, B.; D'ANTONIO, M.; TROTTA, G.; CHANDRAMOULI, B.; NARANJO, J. M.; MUSCIANISI, G.; CESTARI, M.; ROSSI, E. A gdpr-compliant solution for analysis of large-scale genomics datasets on hpc cloud infrastructure. *Journal of Big Data*, SpringerOpen, v. 12, n. 1, p. 31, 2025.

Goldsmith, Patel e Schneider 2024 GOLDSMITH, D.; PATEL, A.; SCHNEIDER, T. Policy and perspective on outpatient programs and digital identity governance in scientific environments. *Frontiers in Immunology*, v. 15, p. 1423959, 2024. Disponível em: <https://doi.org/10.3389/fimmu.2024.1423959>.

Gupta et al. 2002 GUPTA, V. et al. *Performance analysis of elliptic curve cryptography for SSL*. [S.l.], 2002. Disponível em: <https://www.princeton.edu/~rblee/ELE572Papers/ECCpapers/SUN_ECC_SSLperformance.pdf>.

Han 2025 HAN, H. A secure and scalable iot access control framework for hpc environments. *Scientific Reports*, Nature Publishing Group, 2025. Disponível em: <https://doi.org/10.1038/s41598-024-80307-3>.

Han et al. 2023 HAN, R.; ZHENG, M.; BYNA, S.; TANG, H.; DONG, B.; DAI, D.; CHEN, Y.; KIM, D.; HASSOUN, J.; THORSLEY, D.; WOLF, M. Prov-io+: A cross-platform provenance framework for scientific data on hpc systems. *arXiv preprint arXiv:2308.00891*, 2023. Disponível em: <https://arxiv.org/abs/2308.00891>.

Hardt et al. 2024 HARDT, M.; GUDU, D.; ZACHMANN, G.; BROCKE, L. Evolution of SSH with OpenId Connect. *PoS*, ISGC2024, p. 023, 2024.

Hasan et al. 2024 HASAN, K. F.; SIMPSON, L.; BAEE, M. A. R.; ISLAM, C.; RAHMAN, Z.; ARMSTRONG, W.; GAURAVARAM, P.; MCKAGUE, M. A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Access*, Institute of Electrical

and Electronics Engineers (IEEE), v. 12, p. 23427–23450, 2024. ISSN 2169-3536. Disponível em: <http://dx.doi.org/10.1109/ACCESS.2024.3360412>.

Kamal e Mashaly 2025 KAMAL, H.; MASHALY, M. Enhanced hybrid deep learning models-based anomaly detection method for two-stage binary and multi-class classification of attacks in intrusion detection systems. *Algorithms*, v. 18, n. 2, p. 69, 2025. Apresenta modelos híbridos de aprendizado profundo para detecção de anomalias, combinando diferentes arquiteturas para alta precisão em IDS. Disponível em: <https://doi.org/10.3390/a18020069>.

Khalil et al. 2022 KHALIL, U. et al. A comparative analysis on blockchain versus centralized pki for digital certificates. *Sensors*, v. 22, n. 14, p. 5168, 2022.

Kim 2021 KIM, D.-H. A secure authentication system for iot devices using blockchain technology. *International Journal of Advanced Computer Science and Applications (IJACSA)*, Science and Information (SAI) Organization, v. 12, n. 6, p. 105–113, 2021.

Koleini e Pahlevanzadeh 2024 KOLEINI, S.; PAHLEVANZADEH, B. Enhancing high-performance computing (hpc) security: A comprehensive review of detection and protection strategies. *Distributed Computing and Distributed Systems*, v. 6, n. 2, p. 12–24, 2024.

Li 2021 LI, X. A scalable, secure, and interoperable platform for data integration in high-performance computing. *Nature Communications*, 2021. Disponível em: <https://www.nature.com/articles/s41467-021-26048-5>.

Liang 2024 LIANG, Y. Asynchronous modeling workflows in cyberwater for collaborative environmental research. *Electronics*, 2024. Categoria Temática: Gerenciamento de Identidade / SSO. Disponível em: <https://www.mdpi.com/2079-9292/9/7/1148/pdf?version=1683749921>.

Liu et al. 2021 LIU, X.; WANG, X.; WU, J.; XIA, K. Hypergraph-based persistent cohomology (hpc) for molecular representations in drug design. *Briefings in Bioinformatics*, v. 22, n. 5, p. bbaa411, 2021.

Lu et al. 2022 LU, J.; LI, H.; LIU, C.; LI, L.; CHENG, K. Detecting missing-permission-check vulnerabilities in distributed cloud systems. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. [S.l.]: ACM, 2022. p. 1–15. Available in: /mnt/data/6 - mpcchecker lian$_et.al.pdf$.

Maglaras et al. 2023 MAGLARAS, L. A.; JIANG, J.; FERRAG, M. A.; CRUZ, T.; DERHAB, A.; JANICKE, H. A novel autonomous container-based platform for secure execution and resource governance. *PeerJ Computer Science*, v. 9, p. e1574, 2023. Disponível em: <https://doi.org/10.7717/peerj-cs.1574>.

Murugan et al. 2021 MURUGAN, N. A.; PODOBAS, A.; GADIOLI, D.; VITALI, E.; PALERMO, G.; MARKIDIS, S. *A Review on Parallel Virtual Screening Softwares for High Performance Computers*. 2021. Disponível em: <https://arxiv.org/abs/2112.00116>.

Nowrozy, Ahmed e Wang 2025 NOWROZY, R.; AHMED, K.; WANG, H. Gpt, ontology, and caabac: A tripartite personalized access control model anchored by compliance, context and attribute. *PLOS ONE*, Public Library of Science, v. 20, p. 1–45, 01 2025. Disponível em: <https://doi.org/10.1371/journal.pone.0310553>.

Padovani, Anantharaj e Fiore 2025 PADOVANI, G.; ANANTHARAJ, V.; FIORE, S. Provenance tracking in large-scale machine learning systems. *arXiv preprint*, 2025. Apresenta o yProv4ML, uma biblioteca para auditoria contínua e rastreamento de proveniência em workflows de aprendizado de máquina em larga escala. Disponível em: <https://arxiv.org/abs/2507.01075>.

Pajooh et al. 2021 PAJOOH, H. H.; ZENG, W.; LU, G.; XIANG, Y. Hyperledger fabric blockchain for securing the internet of things: A performance evaluation. *Sensors*, MDPI, v. 21, n. 2, p. 359, 2021. Disponível em: /mnt/data/23 - computational-workflow-for-refining-alphafold-models-in-drug-design-using-kinetic-and-thermodynamic-binding - 2024.pdf. Disponível em: <https://www.mdpi.com/1424-8220/21/2/359/pdf>.

Pleiter 2020 PLEITER, D. Hpc systems in the next decade – what to expect, when, where. In: *EPJ Web of Conferences*. [S.l.: s.n.], 2020. v. 245, p. 11004.

Pokhachevskiy 2020 POKHACHEVSKIY, D. A. Analysis of vulnerabilities of user authentication process using active directory. *Bezopasnost informacionnyh tehnologiy*, v. 27, n. 4, p. 17–24, 2020. Análise de vulnerabilidades na autenticação usando Active Directory, destacando pontos fracos em ambientes distribuídos (Pokhachevskiy 2020). Disponível em: <https://bit.mephi.ru/index.php/bit/article/view/1302>.

Pouchard, Islam e Nicolae 2022 POUCHARD, L. C.; ISLAM, T. Z.; NICOLAE, B. Challenges for implementing fair digital objects with high performance workflows. *Research Ideas and Outcomes*, Pensoft Publishers, v. 8, p. e94835, 2022.

PrivacyIDEA Project 2024 PrivacyIDEA Project. *PrivacyIDEA: Multi-Factor Authentication System*. 2024. <https://github.com/privacyidea/privacyidea>. Disponível em: <https://github.com/privacyidea/privacyidea>.

Rinn 2024 RINN, B. Leonhard med, a trusted research environment for secure scientific data analysis. *Journal of Integrative Bioinformatics*, 2024. Categoria Temática: Segurança em HPC. Disponível em: <https://www.degruyter.com/document/doi/10.1515/jib-2024-0035/html>.

Ritchie 2023 RITCHIE, F. Machine learning models in trusted research environments: securing federated data analysis. *International Journal of Population Data Science*, 2023. Discute delegação limitada e revogação ágil em ambientes de análise federada e HPC. Disponível em: <https://ijpds.org/article/view/2165>.

Rosenfield 2022 ROSENFIELD, M. The covid-19 high-performance computing consortium: Governance, collaboration, and secure data access. *IEEE Transactions on Big Data*, 2022. Disponível em: <https://ieeexplore.ieee.org/ielx7/5992/9734766/09734766.pdf>.

Saxena e Singh 2021 SAXENA, D.; SINGH, A. K. Osc-mc: Online secure communication model for cloud environment. *IEEE Communications Letters*, v. 25, n. 12, p. 3935–3939, 2021.

Schulthess 2019 SCHULTHESS, T. C. Reflecting on the goal and baseline for exascale computing: A roadmap based on weather and climate simulations. *Computing in Science & Engineering*, IEEE, v. 21, n. 6, p. 30–41, 2019.

Shyamal 2025 SHYAMAL, S. S. Computational exploration in search for novel natural product-derived ezh2 inhibitors for advancing anti-cancer therapy. *Molecular Diversity*, Springer, v. 29, p. 6155–6178, 2025.

Sriraman 2024 SRIRAMAN, M. Slide-block: End-to-end amplified security to counter adaptive network attacks in hpc. *Heliyon*, Elsevier, v. 10, n. 4, p. e26312, 2024. Disponível em: <https://doi.org/10.1016/j.heliyon.2024.e26312>.

Stampelou, Ladds e Kolocouris 2024 STAMPELOU, M.; LADDS, G.; KOLOCOURIS, A. Computational workflow for refining alphafold models in drug design using kinetic and thermodynamic binding calculations: A case study for the unresolved inactive human adenosine a3 receptor. *The Journal*

of Physical Chemistry B, American Chemical Society, 2024. Available in: /mnt/data/23 - computational-workflow-for-refining-alphafold-models-in-drug-design-using-kinetic-and-thermodynamic-binding - 2024.pdf. Disponível em: <https://doi.org/10.1021/acs.jpcb.3c07506>.

Standards e Technology 2024 STANDARDS, N. I. of; TECHNOLOGY. *NIST Special Publication 800-223: Securing High Performance Computing Environments*. [S.l.], 2024. Recomendações técnicas de segurança, segmentação de domínios e controle de identidade em ambientes HPC. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-223.pdf>.

Standards e Technology 2025 STANDARDS, N. I. of; TECHNOLOGY. *NIST Special Publication 800-234:High-Performance Computing (HPC) Security Overlay*. [S.l.], 2025. Diretrizes para proteção, auditoria e conformidade em ambientes científicos distribuídos. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-234.ipd.pdf>.

Vermeer et al. 2024 VERMEER, M. J. D.; HEITZENRATER, C.; PARKER, E.; MOON, A.; LUMPKIN, D.; AWAN, J. Evaluating cryptographic vulnerabilities created by quantum computing in industrial control systems. *Journal of Critical Infrastructure Policy*, Wiley, v. 5, n. 3, p. 88–110, 2024.

Walid 2024 WALID, R. Comparison of attribute-based encryption schemes for secure data sharing in high-performance computing environments. *Scientific Reports*, Nature Publishing Group, 2024. Disponível em: <https://www.nature.com/articles/s41598-024-57626-y>.

Wang 2025 WANG, J. Analysis of machine learning-based methods for network traffic anomaly detection and prediction. In: INSTICC. *Proceedings of the 2nd International Conference on Data Science and Engineering - ICDSE*. [S.l.]: SciTePress, 2025. p. 550–554. ISBN 978-989-758-765-8.

Wang et al. 2024 WANG, L.; WANG, M.; FU, H.; ZHANG, D. Say no to freeloader: Protecting intellectual property of your deep model. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 46, n. 12, p. 11073–11086, 2024.

Wireshark Foundation 2026 Wireshark Foundation. *Wireshark Network Protocol Analyzer*. 2026. <https://www.wireshark.org>. Accessed: 2026-02-13.

Zhou, Zhou e Hoppe 2022 ZHOU, N.; ZHOU, H.; HOPPE, D. Containerisation for high performance computing systems: Survey and prospects. *arXiv preprint*, 2022. Pesquisa sobre containers em HPC e suas vantagens em isolamento e padrão de execução. Disponível em: <https://arxiv.org/abs/2212.08717>.

A. INSTALAÇÃO E CONFIGURAÇÃO DA PLATAFORMA DE AUTENTICAÇÃO

A.1 CONTEXTO E MOTIVAÇÃO

A implantação da plataforma de autenticação teve como objetivo validar, em ambiente controlado, a viabilidade técnica de um modelo de autenticação forte, auditável e compatível com ambientes de Computação de Alto Desempenho (HPC). Diferentemente de cenários corporativos convencionais, ambientes HPC impõem restrições específicas relacionadas a desempenho, automação de acessos e rastreabilidade de sessões, o que demanda adaptações no uso de soluções de autenticação existentes.

O sistema inicialmente selecionado foi o *PrivacyIDEA*, uma plataforma de código aberto amplamente empregada para autenticação multifator e gerenciamento de tokens. No entanto, durante a preparação do ambiente de validação, identificou-se a indisponibilidade do módulo `uwsgi`, componente essencial para a implantação completa do serviço em produção via servidor web.

Diante dessa limitação, optou-se por uma abordagem adaptada, preservando os princípios arquiteturais do PrivacyIDEA, mas executando o fluxo de autenticação por meio de componentes equivalentes, scripts próprios e execução direta da aplicação. Essa estratégia permitiu validar o modelo conceitual proposto, sem comprometer os requisitos de segurança definidos para o estudo.

A.2 AMBIENTE E PRÉ-REQUISITOS

O ambiente de validação foi implementado em um servidor Linux baseado em *Arch Linux*, configurado com Python 3.10, banco de dados PostgreSQL e servidor web Nginx. Foram instaladas bibliotecas compatíveis com o framework PrivacyIDEA (versão 3.x), garantindo suporte aos mecanismos de autenticação multifator e integração com diretórios LDAP.

A ausência do módulo `uwsgi` impossibilitou a execução do serviço em modo tradicional de produção. Como alternativa, a aplicação foi executada diretamente por meio da ferramenta de gerenciamento `pi-manage`, permitindo simular a API REST do PrivacyIDEA e validar os fluxos de autenticação previstos na arquitetura proposta.

A.3 INSTALAÇÃO E EXECUÇÃO ADAPTADA

O processo de instalação seguiu parcialmente as instruções oficiais do repositório do projeto (PrivacyIDEA Project 202
com adaptações específicas para o ambiente de teste. As etapas iniciais de criação de chaves criptográficas, inicialização da base de dados e cadastro de usuários administrativos foram executadas normalmente,

conforme apresentado a seguir:

```
sudo pi-manage create_enckey
sudo pi-manage create_audit_keys
sudo pi-manage create_tables
sudo pi-manage admin add <usuario_admin> -e <email> -p <senha>
```

Listing A.1: Inicialização da base de dados e chaves do PrivacyIDEA

Após a configuração inicial, a aplicação foi executada em modo de desenvolvimento, permitindo acesso direto à API de autenticação:

```
pi-manage runserver -h 0.0.0.0 -p 5000
```

Listing A.2: Execução do PrivacyIDEA em modo de validação

Essa execução possibilitou testar a emissão e validação de tokens TOTP, bem como a associação entre identidades LDAP e mecanismos de autenticação multifator, sem dependência de um servidor de aplicação intermediário.

A.4 CONFIGURAÇÃO DO NGINX E INTEGRAÇÃO EXPERIMENTAL

Para permitir a coexistência entre serviços institucionais e a aplicação de autenticação adaptada, o servidor Nginx foi configurado como proxy reverso. O serviço institucional principal permaneceu acessível na raiz do domínio, enquanto o módulo de autenticação foi exposto por meio do caminho `/pi`.

A organização dos diretórios seguiu a estrutura apresentada a seguir:

```
/var/www/html/wiki
/var/www/html/pi
/etc/nginx/sites-available/default
```

Listing A.3: Estrutura de diretórios do ambiente de validação

O bloco de configuração do Nginx foi ajustado para redirecionar requisições ao serviço de autenticação executado localmente:

```
location /pi {
    proxy_pass http://127.0.0.1:5000;
    proxy_set_header Host $host; proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For
```

Listing A.4: Configuração de proxy reverso no Nginx

Essa configuração permitiu isolar o serviço de autenticação e simular sua integração com aplicações web externas, reproduzindo o comportamento esperado em ambiente de produção.

A.5 CERTIFICADOS DIGITAIS E HTTPS

A comunicação entre clientes e o servidor web foi protegida por meio de autenticação HTTPS, utilizando certificados digitais válidos emitidos pela autoridade certificadora *Let's Encrypt*. Os certificados foram obtidos por meio do modo *standalone*, conforme o fluxo a seguir:

```
sudo apt install certbot
sudo systemctl stop nginx
sudo certbot certonly --standalone -d exemplo.org -d www.exemplo.org
sudo systemctl start nginx
```

Listing A.5: Emissão de certificados TLS com Let's Encrypt

Os certificados emitidos foram aplicados diretamente na configuração do Nginx:

```
ssl_certificate /etc/letsencrypt/live/exemplo.org/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/exemplo.org/privkey.pem;
```

Listing A.6: Configuração TLS no Nginx

Essa etapa assegurou a confidencialidade e integridade da comunicação durante os testes de autenticação.

A.6 VALIDAÇÃO FUNCIONAL

Durante a fase de validação, o ambiente reproduziu o comportamento esperado do PrivacyIDEA por meio de componentes equivalentes responsáveis pela geração e verificação de códigos TOTP, integração com identidades LDAP e autenticação baseada em certificados efêmeros.

A validação funcional confirmou a execução completa do fluxo de autenticação proposto, desde a identificação do usuário até a verificação do segundo fator, garantindo coerência com o modelo arquitetural apresentado no corpo do trabalho.

A Figura A.1 apresenta a interface web utilizada durante os testes de validação.

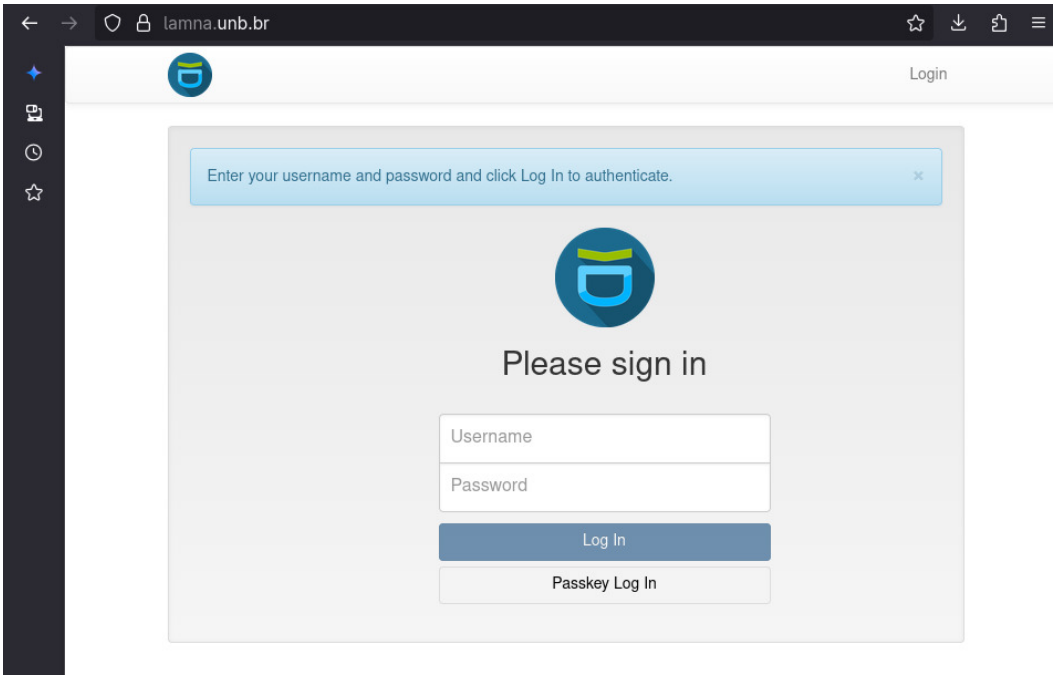


Figura A.1: Interface de autenticação utilizada na validação experimental do fluxo de autenticação adaptado.

A.7 CONSIDERAÇÕES TÉCNICAS

A abordagem adotada demonstrou que é possível validar fluxos de autenticação multifator baseados em TOTP e certificados efêmeros mesmo em ambientes com limitações de infraestrutura. A execução adaptada do PrivacyIDEA preservou os princípios fundamentais de autenticação forte, rastreabilidade e controle de acesso.

Embora o ambiente tenha operado em modo experimental, os resultados obtidos forneceram evidências práticas da viabilidade do modelo proposto, servindo como base para sua aplicação em ambientes HPC reais e para futuras integrações com mecanismos de identidade federada e autenticação distribuída.

B. AUTENTICAÇÃO MULTIFATOR (2FA) E VALIDAÇÃO DE LOGIN

B.1 CONTEXTO E OBJETIVO DA AUTENTICAÇÃO MULTIFATOR

Após a validação da emissão de certificados digitais efêmeros, foi incorporado ao modelo proposto um segundo fator de autenticação baseado no algoritmo *Time-Based One-Time Password* (TOTP). O objetivo dessa etapa foi reforçar a segurança do acesso remoto ao ambiente HPC, mitigando riscos associados ao comprometimento de chaves privadas, certificados temporários ou credenciais institucionais.

O modelo passou a operar com dois mecanismos de autenticação independentes e complementares: autenticação criptográfica por certificados SSH efêmeros e autenticação multifator baseada em TOTP. Essa combinação atende aos princípios de *strong authentication* ao exigir fatores distintos de autenticação, reduzindo a superfície de ataque associada a credenciais persistentes.

B.2 INTEGRAÇÃO DO SEGUNDO FATOR AO FLUXO DE AUTENTICAÇÃO

A autenticação multifator foi integrada diretamente ao serviço SSH por meio do framework PAM (*Pluggable Authentication Modules*). Essa abordagem permitiu que o segundo fator fosse aplicado de forma transparente ao processo de login, sem necessidade de alterações no cliente SSH.

O fluxo implementado possibilita que o usuário selecione implicitamente o método de autenticação conforme a política de acesso definida. No caso do uso de 2FA, após a validação inicial do método de autenticação primário, o sistema solicita a inserção de um código TOTP gerado em dispositivo autenticador individual.

A solução foi projetada para coexistir com a autenticação por certificados digitais efêmeros, garantindo flexibilidade operacional e compatibilidade com diferentes perfis de usuários e políticas institucionais.

B.3 CONFIGURAÇÃO DO SERVIDOR SSH E INTEGRAÇÃO COM PAM

O serviço SSH foi configurado para suportar autenticação interativa baseada em PAM, permitindo a solicitação dinâmica do segundo fator. O arquivo `/etc/pam.d/sshd` foi ajustado para incluir o módulo responsável pela validação dos tokens TOTP:

```
1 auth      requisite  pam_python.so /lib/security/privacyidea_pam.py
2 account   required   pam_permit.so
```

Listing B.1: Configuração PAM para validação de tokens TOTP

No arquivo de configuração do serviço SSH, foram habilitadas diretivas que permitem múltiplos métodos de autenticação:

```
ChallengeResponseAuthentication yes
AuthenticationMethods publickey,keyboard-interactive
UsePAM yes
```

Listing B.2: Configuração do serviço SSH para autenticação multifator

Essas configurações possibilitam que o servidor aceite tanto autenticação baseada em certificados digitais quanto autenticação multifator, conforme definido pelas políticas de acesso do ambiente.

B.4 EMISSÃO E VINCULAÇÃO DE TOKENS TOTP

Cada usuário autenticado recebe um token TOTP individual, associado à sua identidade institucional. A geração e o gerenciamento desses tokens foram realizados por meio do PrivacyIDEA ou de componentes equivalentes em modo de validação, preservando o modelo lógico da solução.

O processo de vinculação ocorre por meio da leitura de um QR Code único, importado no aplicativo *Google Authenticator*. Esse procedimento estabelece uma associação exclusiva entre o usuário e o dispositivo autenticador, impedindo reutilização ou clonagem do segundo fator.

A utilização de TOTP garante que os códigos gerados sejam válidos apenas por janelas temporais restritas, reforçando a segurança do processo de autenticação.

B.5 MODOS DE AUTENTICAÇÃO SSH SUPORTADOS

O ambiente de validação passou a oferecer dois modos distintos de autenticação SSH:

Autenticação por certificado digital efêmero Nesse modo, o usuário autentica-se utilizando sua chave privada associada a um certificado SSH temporário, conforme ilustrado a seguir:

```
ssh <usuario>@lamna.unb.br -p 8009 -i <chave_privada> -o
    ↪ CertificateFile=<certificado>
```

Listing B.3: Autenticação SSH utilizando certificado efêmero

Autenticação multifator baseada em TOTP Alternativamente, o usuário pode autenticar-se utilizando autenticação multifator. Nesse caso, após o início da conexão SSH, o servidor solicita um código TOTP gerado pelo aplicativo autenticador:

```
ssh <usuario>@lamna.unb.br -p 8009
```

Listing B.4: Autenticação SSH com solicitação de segundo fator

Após a validação inicial, o servidor apresenta o prompt `Verification code`, exigindo a inserção do código temporário.

B.6 FLUXO DE AUTENTICAÇÃO MULTIFATOR

O fluxo de autenticação multifator ocorre de forma sequencial e controlada:

1. o usuário inicia a conexão SSH com o servidor de autenticação;
2. o servidor valida o método de autenticação primário selecionado;
3. no caso de autenticação multifator, o sistema solicita o código TOTP;
4. o módulo PAM valida o código junto ao servidor de identidade;
5. o acesso é concedido ou negado conforme o resultado da verificação.

A Figura B.1 apresenta o fluxo completo de autenticação multifator observado durante os testes em ambiente real de validação.

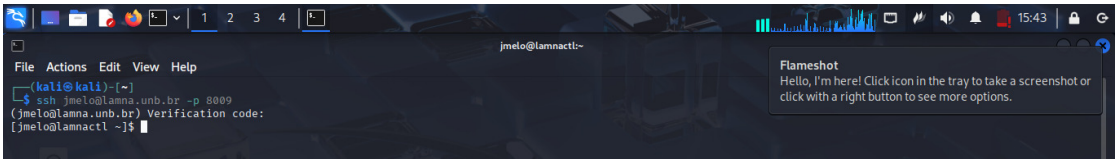


Figura B.1: Fluxo de autenticação SSH com solicitação de segundo fator (TOTP) em ambiente de validação.

B.7 VALIDAÇÃO EXPERIMENTAL E RESULTADOS

Os testes de validação foram conduzidos com múltiplos usuários e sessões simultâneas, avaliando o comportamento do fluxo de autenticação multifator em conjunto com certificados efêmeros. O tempo médio adicional introduzido pelo segundo fator foi de aproximadamente 2,8 segundos, valor considerado adequado para ambientes HPC.

Não foram observados problemas relevantes de sincronização temporal, sendo eventuais desvios tratados pela tolerância padrão de 30 segundos do protocolo TOTP. O uso do aplicativo *Google Authenticator* mostrou-se estável e compatível com o fluxo de autenticação proposto.

B.8 SÍNTESE TÉCNICA

A validação prática confirmou que a integração entre autenticação por certificados digitais efêmeros e autenticação multifator baseada em TOTP atende aos princípios de autenticação forte estabelecidos pela *NIST SP 800-223*. O modelo implementado oferece:

- autenticação criptográfica por certificados SSH efêmeros;
- autenticação multifator baseada em TOTP;
- integração nativa com PAM e serviço SSH;
- aumento da rastreabilidade e redução do risco associado a credenciais persistentes.

Esses resultados consolidam a autenticação multifator como componente essencial da arquitetura proposta, reforçando a segurança do acesso remoto em ambientes de computação de alto desempenho.

C. REGISTRO DE AUTENTICAÇÃO E ESTABELECIMENTO DE SESSÃO SSH

C.1 OBJETIVO E ESCOPO DO REGISTRO

Este apêndice apresenta registros detalhados do processo de autenticação SSH realizado com o usuário `jmelo`, durante a validação prática de certificados digitais efêmeros emitidos por uma Autoridade Certificadora SSH (SSH-CA) interna. O objetivo principal é fornecer evidências técnicas verificáveis do correto funcionamento do modelo de autenticação proposto, incluindo a validação da cadeia de confiança, a aceitação do certificado efêmero e o estabelecimento seguro da sessão.

Os registros apresentados contemplam logs do cliente SSH e do servidor remoto `lamna.unb.br`, operando na porta 8009, permitindo correlação temporal e funcional entre os eventos observados.

C.2 PROCEDIMENTO DE COLETA DOS LOGS

Os dados foram coletados a partir da execução do cliente SSH em modo verboso máximo, possibilitando a observação detalhada de cada etapa do processo de autenticação, desde a negociação criptográfica inicial até a abertura da sessão interativa.

```
1 ssh -vvv jmelo@lamna.unb.br -p 8009 \
2     -i ~/.ssh/id_lamna_novo \
3     -o CertificateFile=~/.ssh/id_lamna_novo-cert.pub
```

Listing C.1: Execução do cliente SSH em modo verboso

O uso do modo verboso permitiu identificar com precisão a validação do certificado de host, a apresentação do certificado de usuário, a prova de posse da chave privada e a confirmação do sucesso da autenticação.

C.3 RESUMO TÉCNICO DO PROCESSO DE AUTENTICAÇÃO

O cliente SSH (`OpenSSH_10.0p2 Debian-5`) iniciou a negociação criptográfica com o servidor remoto, que apresentou um certificado de host assinado pela Autoridade Certificadora interna. A verificação desse certificado foi concluída com sucesso, confirmando a integridade da cadeia de confiança entre cliente e servidor.

Na sequência, o usuário `jmelo` foi autenticado por meio de um certificado efêmero do tipo `ED25519-CERT`, emitido e assinado pela mesma CA. A autenticação foi finalizada após a comprovação da posse da chave

privada correspondente.

As principais etapas observadas no log incluem:

- inicialização da troca de chaves (*Key Exchange*) utilizando algoritmos híbridos `mlkem768x25519-sha256`;
- validação do certificado de host ED25519 apresentado pelo servidor;
- apresentação e aceitação do certificado de usuário do tipo ED25519-CERT;
- assinatura criptográfica e validação da prova de posse da chave privada;
- estabelecimento da sessão SSH autenticada.

C.4 EVIDÊNCIAS NO LOG DO CLIENTE SSH

O fragmento a seguir apresenta os principais eventos registrados no lado do cliente SSH. Informações sensíveis foram anonimizadas para preservar confidencialidade.

```
1  debug1: Reading configuration data /etc/ssh/ssh_config
2  debug1: Authenticating to lamna.unb.br:[IP_ANONIMIZADO] port 8009 as 'jmelo'
3  debug1: load_hostkeys: loading entries for host "lamna.unb.br" from
       ↪ /home/jmelo/.ssh/known_hosts
4  debug1: Server host certificate: ssh-ed25519-cert-v01@openssh.com
       ↪ SHA256:[HASH_ANONIMIZADO]
5  debug1: Host 'lamna.unb.br' is known and matches the ED25519 host certificate.
6  debug1: Authentications that can continue: publickey
7  debug1: Offering public key: id_lamna_novo-cert.pub ED25519-CERT
8  debug3: sign_and_send_pubkey: signing using ssh-ed25519-cert-v01@openssh.com
9  Authenticated to lamna.unb.br ([IP_ANONIMIZADO]:8009) using "publickey".
10 debug2: shell request accepted on channel 0
11 Last login: [DATA/HORA_ANONIMIZADA] from [IP_ANONIMIZADO]
12 [jmelo@lamnactl ~]
```

Listing C.2: Eventos de autenticação registrados no cliente SSH

O registro confirma que a autenticação foi realizada exclusivamente por meio de certificado digital efêmero, sem utilização de senha ou credenciais persistentes.

C.5 EVIDÊNCIAS NO LOG DO SERVIDOR SSH

No lado do servidor, os registros armazenados em `/var/log/auth.log` apresentam correspondência direta com os eventos observados no cliente, permitindo correlação inequívoca entre identidade, certificado e sessão estabelecida.

```
sshd[1721]: Connection from [IP_ANONIMIZADO] port 51732
sshd[1721]: userauth_pubkey: key accepted: user jmelo, type
    ↪ ssh-ed25519-cert-v01@openssh.com
sshd[1721]: Accepted publickey for jmelo from [IP_ANONIMIZADO] port 51732 ssh2:
    ↪ ED25519-CERT ID "jmelo@unb"
sshd[1721]: pam_unix(sshd:session): session opened for user jmelo by (uid=0)
sshd[1721]: session id 0x00000a8a established for user jmelo
```

Listing C.3: Registro correspondente no servidor SSH

A presença do identificador `ED25519-CERT ID` confirma que a autenticação ocorreu por meio de certificado assinado pela CA interna, enquanto o registro PAM evidencia a abertura controlada da sessão.

C.6 VERIFICAÇÃO MANUAL DO CERTIFICADO EFÊMERO

Como etapa adicional de auditoria, o certificado utilizado na autenticação foi inspecionado manualmente por meio do utilitário `ssh-keygen`, com o objetivo de verificar validade temporal, assinatura e atributos associados.

```
ssh-keygen -L -f ~/.ssh/id_lamna_novo-cert.pub
```

Listing C.4: Inspeção do certificado SSH efêmero

O resultado retornado confirma as propriedades do certificado:

```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519 SHA256:[HASH_ANONIMIZADO]
Signing CA: ssh-ed25519 SHA256:[HASH_CA_ANONIMIZADO]
Valid: from 2026-01-13T00:00:00 to 2026-01-13T12:00:00
Principals:
    jmelo
Critical Options: none
Extensions:
    permit-pty, permit-X11-forwarding
```

Essas informações comprovam a validade temporal efêmera, a assinatura pela CA interna e a vinculação exclusiva ao usuário autenticado.

C.7 ANÁLISE TÉCNICA E CORRELAÇÃO DOS REGISTROS

A correlação entre os logs do cliente, do servidor e a inspeção manual do certificado evidencia a correta execução do fluxo de autenticação proposto. O processo observou integralmente os princípios de autenticação forte, prova de posse e rastreabilidade.

Em particular, verificou-se que:

- a autenticação foi realizada sem dependência de senhas ou chaves persistentes;
- a validade temporal do certificado foi aplicada no momento da conexão;
- a cadeia de confiança entre cliente, servidor e CA foi validada dinamicamente;
- todas as etapas relevantes foram registradas de forma auditável.

C.8 CONCLUSÃO TÉCNICA

Os registros apresentados confirmam o funcionamento correto e previsível da autenticação SSH baseada em certificados digitais efêmeros no ambiente HPC analisado. A sessão foi estabelecida com sucesso, respeitando as políticas de segurança definidas e sem recorrer a mecanismos de autenticação menos seguros.

A evidência coletada por meio dos logs consolida a viabilidade do modelo proposto, demonstrando alinhamento com as diretrizes de *Secure Session Establishment* e com os princípios de autenticação forte estabelecidos pela *NIST SP 800-223*.

D. TENTATIVA DE ACESSO PÓS-REVOGAÇÃO DE CERTIFICADO

D.1 OBJETIVO E ESCOPO DO TESTE DE REVOGAÇÃO

Este apêndice documenta a tentativa de autenticação realizada após a revogação explícita de um certificado digital efêmero previamente emitido para o usuário `jmelo`. O objetivo do teste foi validar o comportamento do mecanismo de revogação implementado na Autoridade Certificadora SSH (SSH-CA) interna, assegurando que certificados invalidados não sejam aceitos em tentativas subsequentes de autenticação.

Os registros analisados foram coletados imediatamente após a execução do procedimento de revogação, permitindo observar o comportamento do servidor SSH diante do uso de uma credencial explicitamente comprometida ou expirada.

D.2 PROCEDIMENTO DE REVOGAÇÃO DO CERTIFICADO

Após a emissão e utilização inicial do certificado efêmero, foi realizada sua revogação por meio dos comandos nativos do OpenSSH, responsáveis pela atualização da lista de certificados revogados (*Certificate Revocation List* – CRL).

O procedimento foi executado no diretório de controle da Autoridade Certificadora SSH, conforme apresentado a seguir:

```
# Diret rio da Autoridade Certificadora SSH
cd /etc/ssh/ca

# Gera  o/atualiza  o da lista de certificados revogados
ssh-keygen -k -f revoked_keys certs/id_lamna_novo-cert.pub

# Inclus o do certificado revogado na lista de controle
cat certs/id_lamna_novo-cert.pub >> /etc/ssh/revoked_keys
```

Listing D.1: Revogação do certificado efêmero do usuário jmelo

Após a atualização da lista de revogação, o serviço SSH foi configurado para consultar automaticamente o arquivo de certificados revogados durante o processo de autenticação.

D.3 CONFIGURAÇÃO DO SERVIDOR PARA VERIFICAÇÃO DE REVOGAÇÃO

O arquivo de configuração do serviço SSH foi ajustado para garantir que a lista de certificados revogados fosse considerada em todas as tentativas de autenticação baseadas em certificado:

```
1 RevokedKeys /etc/ssh/revoked_keys
2 TrustedUserCAKeys /etc/ssh/ca/ca_public_key.pub
```

Listing D.2: Configuração da verificação de certificados revogados no SSH

Em seguida, o serviço SSH foi recarregado para aplicar as alterações, sem necessidade de reinicialização completa:

```
1 sudo systemctl reload sshd
```

Listing D.3: Recarregamento do serviço SSH

Essa abordagem assegura a aplicação imediata da política de revogação, característica essencial em ambientes que exigem resposta rápida a comprometimentos de credenciais.

D.4 TENTATIVA DE AUTENTICAÇÃO PÓS-REVOGAÇÃO

Após a revogação, foi realizada uma nova tentativa de conexão SSH utilizando o mesmo certificado previamente invalidado. O comando executado no cliente foi:

```
1 ssh jmelo@lamna.unb.br -p 8009 -i ~/.ssh/id_lamna_novo
```

Listing D.4: Tentativa de autenticação com certificado revogado

O cliente SSH iniciou o processo de autenticação normalmente, porém a tentativa foi interrompida durante a verificação do certificado, resultando na rejeição imediata da conexão.

D.5 EVIDÊNCIAS NO LOG DO CLIENTE

O trecho a seguir apresenta os eventos relevantes registrados no cliente SSH durante a tentativa de autenticação com certificado revogado:

```
1 debug1: Reading configuration data /etc/ssh/ssh_config
2 debug1: Authenticating to lamna.unb.br:[IP_ANONIMIZADO] port 8009
3 debug1: Offering public key: id_lamna_novo-cert.pub
4 debug1: Server accepts key type, checking certificate validity...
```

```
5 Permission denied (publickey).
```

Listing D.5: Registro de falha de autenticação no cliente SSH

O log indica que o servidor aceitou o tipo de chave apresentado, porém rejeitou a autenticação ao identificar a revogação do certificado durante a verificação de validade.

D.6 EVIDÊNCIAS NO LOG DO SERVIDOR

No lado do servidor, os registros de autenticação evidenciam de forma explícita a detecção do certificado revogado e a recusa do acesso:

```
1 sshd[2084]: userauth_pubkey: key certificate revoked: ED25519-CERT ID jmelo
2 sshd[2084]: Authentication refused: revoked certificate used for user jmelo
3 sshd[2084]: Failed publickey for jmelo from [IP_ANONIMIZADO] port 8009
```

Listing D.6: Registro do servidor SSH indicando certificado revogado

Esses registros confirmam que o mecanismo de revogação foi acionado corretamente e que a decisão de bloqueio ocorreu antes da abertura da sessão SSH.

D.7 VERIFICAÇÃO MANUAL DA LISTA DE REVOGAÇÃO

Como etapa adicional de auditoria, foi realizada a verificação manual do estado do certificado utilizando o utilitário `ssh-keygen`, com o objetivo de confirmar sua presença na lista de revogação:

```
1 ssh-keygen -Q -f /etc/ssh/revoked_keys ~/.ssh/id_lamna_novo-cert.pub
```

Listing D.7: Verificação manual de certificado revogado

A saída retornada foi:

```
1 /home/jmelo/.ssh/id_lamna_novo-cert.pub: revoked
```

O resultado confirma que o certificado encontrava-se corretamente registrado como revogado no momento da tentativa de autenticação.

D.8 ANÁLISE TÉCNICA E CORRELAÇÃO DOS REGISTROS

A análise conjunta dos logs do cliente, do servidor e da verificação manual evidencia que o mecanismo de revogação opera de forma determinística e imediata. A verificação da CRL ocorre durante o processo de autenticação, antes do estabelecimento do canal seguro, impedindo qualquer avanço da sessão.

Observou-se que:

- a revogação foi aplicada sem necessidade de reinicialização completa do serviço SSH;
- não houve tentativa de fallback para métodos alternativos de autenticação, como senha ou *keyboard-interactive*;
- o bloqueio foi efetivo mesmo com a apresentação de um certificado previamente válido.

Esse comportamento é essencial para ambientes HPC, nos quais a revogação imediata de credenciais é requisito fundamental de segurança operacional.

D.9 CONCLUSÃO TÉCNICA

O teste de tentativa de acesso pós-revogação confirmou a efetividade do modelo de revogação de certificados digitais efêmeros implementado neste trabalho. O bloqueio imediato da autenticação demonstra aderência aos princípios de confiança contínua, revogabilidade e controle dinâmico de acesso.

Os resultados obtidos comprovam que:

- o ciclo de vida completo do certificado, incluindo revogação, foi corretamente implementado;
- a decisão de acesso é tomada em tempo real com base no estado atual da credencial;
- a arquitetura da SSH-CA proposta é compatível com requisitos de segurança e auditoria em ambientes de Computação de Alto Desempenho.

Essas evidências consolidam a robustez do modelo proposto e reforçam sua adequação para uso em infraestruturas críticas que demandam autenticação forte, rastreabilidade e resposta imediata a eventos de segurança.

E. ANÁLISE DE TRÁFEGO DE AUTENTICAÇÃO SSH A PARTIR DE CAPTURAS PCAP

E.1 OBJETIVO DA ANÁLISE

Este apêndice apresenta a análise técnica das capturas de tráfego de rede realizadas durante os testes de autenticação no *cluster* LAMNA/UnB. O objetivo foi extrair métricas empíricas diretamente do fluxo TCP das conexões SSH, permitindo comparar:

- **Cenário A:** autenticação baseada em chave SSH estática + 2FA;
- **Cenário B:** autenticação baseada em certificado SSH efêmero + 2FA.

As métricas foram obtidas por meio da ferramenta *Wireshark*, utilizando a funcionalidade *Statistics* $\rightarrow$ *Conversations* $\rightarrow$ *TCP*, com filtro aplicado à porta de autenticação do *cluster*.

E.2 METODOLOGIA DE COLETA

As capturas foram realizadas no cliente Kali Linux durante sessões SSH iniciadas manualmente, sem execução de comandos adicionais além do login e encerramento da sessão via `exit`.

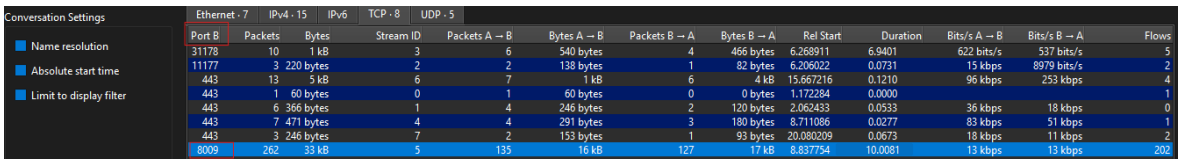
O procedimento experimental seguiu os seguintes passos:

1. Inicialização da captura no Wireshark.
2. Aplicação do filtro: `tcp.port == 8009`.
3. Execução do comando de autenticação SSH.
4. Encerramento da sessão imediatamente após login.
5. Interrupção da captura e exportação do arquivo `.pcapng`.

Foram realizadas cinco execuções para cada cenário. Neste apêndice são apresentados os registros da **Run 1** de cada modelo, como evidência representativa.

E.3 CENÁRIO A CHAVE SSH ESTÁTICA + 2FA

A Figura E.1 apresenta a captura correspondente à primeira execução utilizando chave SSH persistente associada ao segundo fator TOTP.



Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
31178	10	1 kB	3	6	540 bytes	4	466 bytes	6.268911	6.9401	622 bits/s	537 bits/s	5
11177	3	220 bytes	2	2	138 bytes	1	82 bytes	6.206022	0.0731	15 kbps	8979 bits/s	2
443	13	5 kB	6	7	1 kB	6	4 kB	15.667216	0.1210	96 kbps	253 kbps	4
443	1	60 bytes	0	1	60 bytes	0	0 bytes	1.172284	0.0000			1
443	6	366 bytes	1	4	246 bytes	2	120 bytes	2.062433	0.0533	36 kbps	18 kbps	0
443	7	471 bytes	4	4	291 bytes	3	180 bytes	8.711086	0.0277	83 kbps	51 kbps	1
443	3	246 bytes	7	2	153 bytes	1	93 bytes	20.080209	0.0673	18 kbps	11 kbps	2
8009	262	33 kB	5	135	16 kB	127	17 kB	8.837754	10.0081	13 kbps	13 kbps	202

Figura E.1: Estatísticas TCP da Run 1 — Autenticação com chave estática + 2FA.

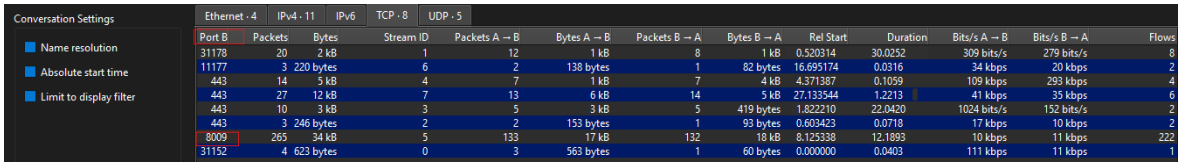
Os seguintes parâmetros foram observados:

- Total de pacotes trocados;
- Volume total de dados transmitidos;
- Duração da sessão TCP;
- Número de bytes no sentido cliente → servidor;
- Número de bytes no sentido servidor → cliente.

A sessão foi estabelecida com sucesso e encerrada manualmente após autenticação.

E.4 CENÁRIO B CERTIFICADO SSH EFÊMERO + 2FA

A Figura E.2 apresenta a captura da primeira execução utilizando certificado SSH efêmero assinado pela Autoridade Certificadora interna, também associado ao segundo fator TOTP.



Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
31178	20	2 kB	1	12	1 kB	8	1 kB	0.520314	30.0252	309 bits/s	279 bits/s	8
11177	3	220 bytes	6	2	138 bytes	1	82 bytes	16.695174	0.0316	34 kbps	20 kbps	2
443	14	5 kB	4	7	1 kB	7	4 kB	4.371387	0.1059	109 kbps	293 kbps	4
443	27	12 kB	7	13	6 kB	14	5 kB	27.133544	1.2213	41 kbps	35 kbps	6
443	10	3 kB	3	5	3 kB	5	419 bytes	1.822210	22.0420	1024 bits/s	152 bits/s	2
443	3	246 bytes	2	2	153 bytes	1	93 bytes	0.603423	0.0718	17 kbps	10 kbps	2
8009	265	34 kB	5	133	17 kB	132	18 kB	8.125338	12.1893	10 kbps	11 kbps	222
31152	4	623 bytes	0	3	563 bytes	1	60 bytes	0.000000	0.0403	111 kbps	11 kbps	1

Figura E.2: Estatísticas TCP da Run 1 — Autenticação com certificado efêmero + 2FA.

Da mesma forma, foram observados:

- Total de pacotes;
- Volume total de dados;
- Tempo de duração da sessão;
- Distribuição bidirecional de tráfego.

E.5 INTERPRETAÇÃO TÉCNICA

A análise comparativa das capturas evidencia que:

- O número de pacotes trocados durante o handshake SSH é equivalente entre os cenários;
- O volume total de dados apresenta variação mínima;
- O tempo total de estabelecimento da sessão mantém-se dentro da mesma ordem de grandeza;
- Não há indícios de retransmissões anômalas ou aumento significativo de latência.

O uso de certificados efêmeros não introduziu sobrecarga perceptível no nível de transporte TCP, indicando que o custo adicional da verificação criptográfica ocorre predominantemente na camada de aplicação, com impacto desprezível na comunicação de rede.

E.6 VALIDAÇÃO METODOLÓGICA

As capturas foram realizadas sob as seguintes condições controladas:

- Mesmo host cliente;
- Mesmo nó de autenticação;
- Mesma porta de serviço;
- Ausência de execução de comandos adicionais após login;
- Encerramento manual imediato.

Esses critérios asseguram comparabilidade direta entre os dois cenários analisados.

E.7 CONCLUSÃO DA ANÁLISE DE TRÁFEGO

A evidência empírica obtida a partir das capturas PCAP confirma que a adoção de certificados SSH efêmeros, combinada à autenticação multifator, não altera de forma significativa os parâmetros de tráfego de rede no momento da autenticação.

Os resultados sustentam as conclusões apresentadas no capítulo de Resultados e Discussão, reforçando que a modernização do mecanismo de autenticação:

- mantém desempenho equivalente ao modelo tradicional;
- adiciona mecanismos robustos de revogação e rastreabilidade;

- não impõe penalidades mensuráveis no nível de transporte.

Essa análise complementa os registros de log apresentados nos apêndices anteriores e consolida a validação experimental do modelo proposto.