Provedores de Identidade Gerenciados na CAFe: Soberania e Inclusão para Organizações sem Equipe Técnica

Frederico Schardong[1], Eduardo Dani Perottoni[1], Brendon Vicente Rocha Silva[1], Laerte F. Belotto[2], Reinaldo Matushima[2], Jean C. Faustino[2]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)

[2]Rede Nacional de Ensino e Pesquisa (RNP)

Resumo. *A Comunidade Acadêmica Federada (CAFe), operada pela Rede Nacional de Ensino e Pesquisa (RNP), pressupõe que cada instituição participante opere seu próprio Provedor de Identidade (IdP). Essa premissa exclui organizações de ensino e pesquisa sem capacidade técnica, como sociedades científicas, fundações de apoio e escolas técnicas. Diante dessa barreira, elas tendem a permanecer fora da federação ou delegar a Gestão de Identidade (GId) a provedores comerciais internacionais. Este artigo argumenta que a soberania de GId é inalcançável individualmente por organizações sem equipe técnica e propõe a oferta de um IdP gerenciado como serviço por um operador nacional como solução.*

1. Introdução

A identidade federada permite acessar serviços externos com credenciais institucionais. No Brasil, a Comunidade Acadêmica Federada (CAFe), operada pela Rede Nacional de Ensino e Pesquisa (RNP), reúne centenas de instituições sobre o protocolo *Security Assertion Markup Language* (SAML) [OASIS 2005]. A adesão à CAFe exige que cada instituição opere um Provedor de Identidade (IdP) [Moreira et al. 2014].

Esse requisito é administrável por universidades que dispõem de equipes de Tecnologia da Informação (TI). Entretanto, ele não é aplicável a um amplo conjunto de organizações sem corpo técnico de TI adequado, como sociedades científicas, fundações de apoio e escolas técnicas. Dentre estas, muitas sequer possuem IdP institucional e autenticam usuários de cada serviço com bases de usuários, credenciais e políticas de segurança próprias. Sem capacidade técnica, essas organizações permanecem sem IdP e fora da federação ou contratam IdPs comerciais, como o Microsoft Entra, que oferecem autenticação, MFA e gestão de usuários. Essa opção resolve o problema imediato, mas entrega a identidade dos usuários a ecossistemas internacionais, abdicando da soberania nacional sobre dados pessoais sujeitos à legislação nacional e, geralmente, não se integra a CAFe.

Este artigo argumenta que GId nessas organizações só é viável de forma coletiva, mediada por um operador nacional. A proposta consiste em um *IdP gerenciado*, ofertado como serviço e integrado à CAFe. A Seção 2 detalha a barreira operacional e o dilema de soberania que dela decorre; a Seção 3 descreve a proposta; e a Seção 4 conclui o artigo.

2. A Barreira Operacional e o Dilema da Soberania

Participar da CAFe exige sustentar um IdP: atualizar o *Shibboleth*, manter diretório de identidades, administrar certificados, chaves, atributos e a publicação periódica de me-

tadados, gerenciar políticas de MFA, garantir disponibilidade e segurança e conduzir a homologação [RNP 2026]. Essas tarefas são administráveis por universidades com equipe capacitada, mas desproporcionais para sociedades científicas com direção voluntária ou escolas sem setor de TI. Constituir essa capacidade, mesmo por terceirização, requer operação permanente e pessoal especializado em servidores, federação e segurança. Ainda que ferramentas e documentação da RNP apoiem a instalação inicial, a sustentação permanece um custo fixo e recorrente. Assim, a soberania de GId da operação própria é em grande medida ilusória, pois depende de uma competência que essas organizações não possuem e que não se justifica internalizar.

A baixa portabilidade e interoperabilidade entre provedores proprietários eleva o custo de migração e favorece o aprisionamento tecnológico [Opara-Martins et al. 2016], enquanto a cobrança recorrente por usuário ativo pode ser incompatível com instituições públicas de ensino e pesquisa. Esse deslocamento tem implicações diretas para a proteção de dados. A Lei Geral de Proteção de Dados (LGPD) [Brasil 2018] atribui à organização, na condição de controladora, responsabilidades sobre a base de dados de seus membros, como finalidade, minimização, transparência e prestação de contas, que não se extinguem ao delegar a autenticação. O desafio é simultaneamente de soberania e de governança de dados: como oferecer identidade forte e federada a organizações com pouco ou nenhum pessoal capacitado em GId.

3. Provedor de Identidade Gerenciado como Porta de Entrada

A solução proposta desacopla a participação na CAFe da operação da infraestrutura. Em vez de cada organização manter seu próprio IdP, e/ou sua própria integração de IdP à CAFe, propõe-se que um operador nacional, como a própria RNP ou entidade a ela vinculada, ofereça IdPs gerenciados como serviço. Cada organização recebe um IdP gerenciado com sua identidade visual, exemplificado na Figura 1, isolado logicamente dos demais, sem precisar manter infraestrutura ou equipe local. Cabe à organização administrar apenas usuários e grupos, enquanto a operadora do serviço configura aplicações, metadados, protocolos, homologação, alta disponibilidade e segurança. Em termos da LGPD, a organização atuará como controladora dos dados de seus membros, e a operadora como operador, processando-os estritamente para autenticação, autorização e federação. Ademais, o Marco Civil da Internet [Brasil 2014] estabelece garantias de privacidade, sigilo e proteção dos dados tratados no território nacional. Nesse contexto, a escolha de um operador nacional é uma decisão de governança que favorece controle contratual, auditoria e prestação de contas sob a legislação brasileira.

Propõe-se um IdP nativo em OpenID Connect (OIDC) [Sakimura et al. 2014], padrão *de facto* da *web*. Este IdP proverá identidade para os sistemas internos, permitindo que aplicações da organização autentiquem usuários via OIDC. A escolha também está alinhada com a proposta de criação da CAFe 2.0, reconcepção da federação acadêmica sobre o *OpenID Federation* [OpenID Foundation 2026][1].

Duas implementações são viáveis para o IdP gerenciado. O *Shibboleth* IdP[2] é a tecnologia usada pela CAFe, conta com extensão para OIDC e há trabalho em curso para

[1]https://web.archive.org/web/20260618000240/https://gt-baita.ifrs.edu.br/
[2]https://shibboleth.net/

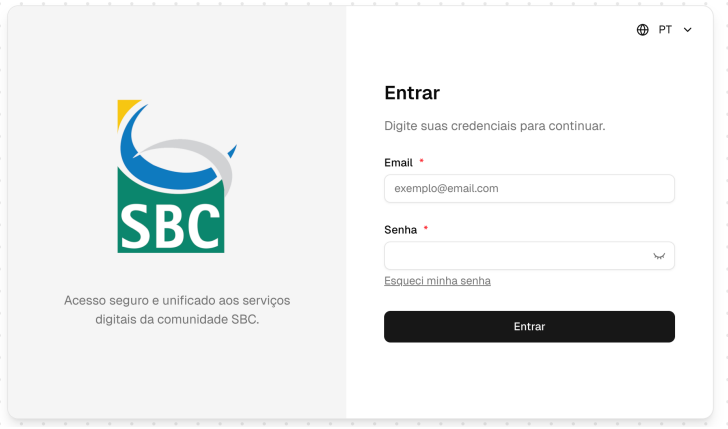

Figura 1. Proposta de tela de autenticação do IdP. SBC usada como exemplo.

OpenID Federation. Opta-se pelo *Keycloak*[3], que oferece características relevantes a uma oferta gerenciada: (i) isolamento lógico de inquilinos (chamados *realms*); (ii) console administrativo para gestão intuitiva dos *realms*; e (iii) autorização e controle de acesso. O item (i) é decisivo para a escalabilidade da oferta do serviço. Com o *Shibboleth*, atender centenas de organizações exigiria gerenciar e manter uma instalação *Shibboleth* por instituição. O item (ii) responde à carência de equipe nas organizações. Em contrapartida, o *Keycloak* não consome metadados de federação SAML, o que torna a mediação por um *proxy* um requisito arquitetural. Para isso, o serviço proposto inclui uma ponte OIDC/SAML, para a organização participar da CAFe sem absorver a complexidade da tradução entre protocolos.

O serviço deve contemplar autenticação por senha, *Time-based One-Time Password* (TOTP) por *e-mail* e *offline*, bem como chaves de segurança *passkey*, e outros. O portador da identidade deve poder gerenciar seus fatores de autenticação, encerrar sessões ativas e inspecionar quais aplicações ele autorizou acessar seus atributos. Esse controle operacionaliza, na interface do IdP, princípios da LGPD como finalidade, consentimento e prestação de contas. A Figura 2 ilustra a arquitetura proposta. Nela, o IdP gerenciado separa a gestão de usuários da operação da infraestrutura.

Há *trade-offs* de segurança e conectividade relacionados ao IdP gerenciado. Em um IdP local, um comprometimento tende a ter menor alcance, mas limitações na equipe podem prejudicar ações corretivas. No IdP gerenciado, a operação especializada pode elevar esses controles, porém falhas podem afetar múltiplas organizações. Assim, práticas de mitigação de vulnerabilidades devem ser adotadas. O IdP gerenciado depende da conectividade e são necessários redundância, monitoramento e alta disponibilidade.

4. Conclusão

A proposta de um IdP ofertado como serviço por um operador nacional confiável, busca preencher simultaneamente as lacunas de centralizar a GId de organizações que hoje não adotam boas práticas de GId e conectá-las a CAFe. Trata-se de um IdP nativo em OIDC e compatível com a CAFe, que separe a administração de usuários de configurações técnicas, ofereça autenticação forte e transparência alinhada à LGPD.

[3]https://www.keycloak.org/

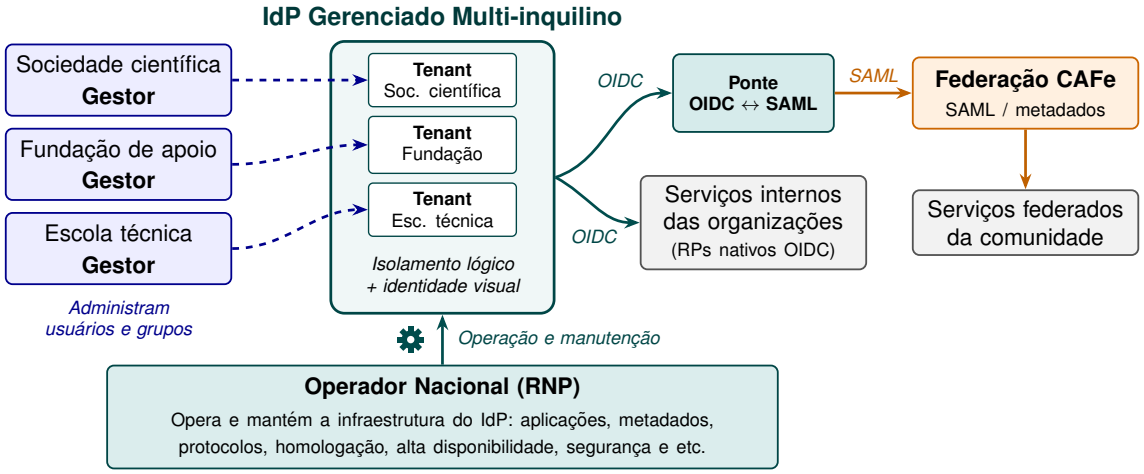

Figura 2. Arquitetura proposta.

Mais do que resolver os desafios de GId dessas organizações, a abordagem proposta as convertem em participantes efetivas da federação e amplia a CAFe. A questão que se coloca à RNP, e à comunidade de gestão de identidade, deixa de ser apenas técnica e torna-se estratégica. Trata-se de oferecer às organizações brasileiras de ensino e pesquisa uma rota nacional, federada e soberana de identidade, antes que esse espaço seja ocupado, de forma duradoura, por ecossistemas internacionais. Aprimorar e validar a proposta em organizações reais, por meio de um piloto, constituem os trabalhos futuros.

Referências

Brasil (2014). Lei n. 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União.

Brasil (2018). Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União.

Moreira, E. Q., Foscarini, D., Silva Junior, G. C. d., Alixandrina, L. A. O., Vieira Neto, L. P., and Rossetto, S. (2014). *Federação CAFe: Implantação do Provedor de Identidade*. Escola Superior de Redes (RNP), Rio de Janeiro.

OASIS (2005). Assertions and protocols for the OASIS security assertion markup language (SAML) v2.0. OASIS Standard.

Opara-Martins, J., Sahandi, R., and Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration. *Journal of Cloud Computing*.

OpenID Foundation (2026). Openid federation 1.0. `https://openid.net/specs/openid-federation-1_0.html`. Acesso em: jun. 2026.

RNP (2026). CAFe — requisitos de uso. `https://ajuda.rnp.br/cafe/idp-cafe`. Acesso em: jun. 2026.

Sakimura, N., Bradley, J., Jones, M. B., de Medeiros, B., and Mortimore, C. (2014). Openid connect core 1.0 incorporating errata set 1. OpenID Foundation.