INOVA ID RS: Desenvolvimento de um Sistema de Gestão de Identidade Federada Aderente ao Ecossistema de Inovação do Rio Grande do Sul

Rodrigo Cesar Lira[1], **Rui de Quadros Ribeiro**[2], **Fiterlinge Sousa**[4], **Michelle Silva Wangham**[3,4]

[1]Instituto Federal de Pernambuco (IFPE) – Paulista, PE – Brasil

[2]Universidade Federal do Rio Grande do Sul (UFRGS) – Porto Alegre, RS – Brasil

[3]Universidade do Vale do Itajaí (UNIVALI) – São José, SC – Brasil

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

rodrigo.lira@paulista.ifpe.edu.br, rui.ribeiro@cpd.ufrgs.br

fiterlinge.sousa@rnp.br, wangham@univali.br

Resumo. *O governo do estado do Rio Grande do Sul criou o programa INOVA RS com o propósito de fomentar a colaboração entre diversos atores do ecossistema de inovação gaúcho, visando impulsionar o desenvolvimento econômico e social regional. Como uma iniciativa decorrente desse programa, surgiu o projeto INOVA ID RS, que busca a construção de uma identidade digital para o ecossistema de inovação, bem como a implementação de uma federação destinada ao compartilhamento seguro de serviços digitais. Este trabalho apresenta os resultados preliminares da concepção e desenvolvimento da Federação INOVA ID RS, que está baseada nos padrões SAML e OpenId Connect.*

1. Introdução

O Rio Grande do Sul (RS) foi considerado o estado mais inovador do Brasil em 2022, segundo o ranking de competitividade do Centro de Liderança Pública[1]. Essa premiação é resultado de políticas de investimentos em programas de ciências e tecnologia, que permitiram a expansão do ecossistema de inovação gaúcho através da criação e manutenção de parques científicos e tecnológicos, e incubadoras [Secretaria de Inovação, Ciência e Tecnologia do Rio Grande do Sul 2022].

Baseando-se em iniciativas de sucesso, como o Pacto Alegre e 22@Barcelona, o governo gaúcho criou o Programa INOVA RS[2]. Esse programa surgiu como uma política pública para estimular a cooperação entre a sociedade civil organizada e os setores empresarial, acadêmico e governamental em prol do desenvolvimento econômico e social regional [Secretaria de Inovação, Ciência e Tecnologia do Rio Grande do Sul 2022].

A colaboração digital desses atores traz a tona o desafio da criação e da gestão de identidades digitais aderentes ao ecossistema de inovação. Com o propósito de aprimorar a segurança e a transparência na cooperação digital, a Rede Nacional de Ensino e

[1]https://estado.rs.gov.br/rs-primeiro-em-inovacao-no-brasil

[2]https://www.inova.rs.gov.br/programa-inovars

Pesquisa (RNP), a Feevale e a Secretaria de Inovação, Ciência e Tecnologia estabeleceram uma cooperação para desenvolver o projeto INOVA ID RS[3]. Este trabalho apresenta os resultados parciais desse projeto que visa: (i) construir uma identidade digital para o ecossistema de inovação gaúcho, (ii) desenvolver e implantar uma federação para compartilhamento de serviços digitais, baseado num modelo de gestão de identidade federada e (iii) avaliar a operação do piloto da federação, com cinco membros, por seis meses.

2. Federação INOVA ID RS

Uma federação é uma colaboração segura entre organizações que permite o intercâmbio de informações e simplifica a gestão de usuários e recursos. Os membros da federação, os parques tecnológicos e outros atores do ecossistema de inovação, registram entidades, como Provedores de Identidade (do inglês, *Identity Provider* - IDP) e Provedores de Serviço (do inglês, *Service Provider* - SP). Os IDPs autenticam usuários e compartilham seus atributos com o SP, que controla o acesso a recursos protegidos. Essa abordagem facilita a interoperabilidade e a segurança das transações entre as organizações participantes [Jensen 2011]. Compete a um operador de federação a sustentação dos componentes que constituem o núcleo da federação.

A Federação INOVA ID RS é baseada no modelo *hub and spoke with distributed login* [Dabbaghi Varnosfaderani et al. 2019], no qual um componente central, chamado de *hub*, atua como IDP quando se comunica com SP e como SP quando se comunica com IDP. O *hub* também possui um serviço de descoberta (do inglês, *Discovery Service* - DS) para redirecionar o fluxo de autenticação para o IDP da organização do usuário. Essa escolha de arquitetura foi feita devido à sua capacidade de integrar facilmente diferentes protocolos, permitindo a inclusão de SPs usando, por exemplo, o OpenID Connect.

Além do *hub* como entidade central, em cada um dos membros da federação serão implantados três componentes: (i) um IDP, (ii) um serviço de diretório e (iii) uma aplicação de gestão de identidades e acessos (do inglês, *Identity and Access Management* - IAM), seguindo a arquitetura apresentada na Figura 1. O IDP utiliza os dados do serviço de diretório para autenticação, enquanto a aplicação de gestão de identidades é responsável por inserir e atualizar os dados dos usuários no diretório.

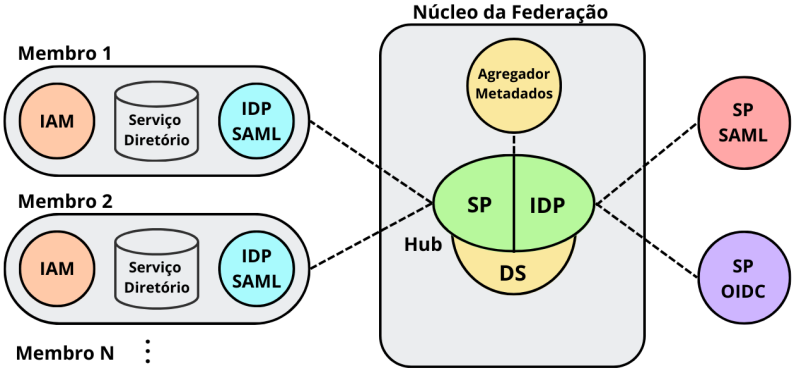

Figura 1. Diagrama da arquitetura utilizada na Federação INOVA ID RS.

Como provedor de identidade optou-se pelo uso do *Shibboleth IDP*[4], um plata-

[3] https://www.rnp.br/projetos/inovaidrs
[4] https://www.shibboleth.net

forma de autenticação baseada em Java, distribuída como software livre que incorpora o protocolo SAML2. A escolha do *Shibboleth IDP* foi baseada na comprovada estabilidade do sistema e na experiência da equipe técnica em sua implementação e operação.

O serviço de diretório, OpenLDAP[5] é utilizado como fonte de dados primários para a autenticação, com um esquema de dados personalizados contendo informações relevantes dos usuários do ecossistema gaúcho de inovação. A gestão das identidades digitais é realizada por meio de uma aplicação de IAM desenvolvida pela equipe do projeto para automatizar tarefas como criação, atualização e desativação de identidades, além de outros fluxos de trabalho.

O núcleo da federação é composto pelo *proxy* SaToSa[6] (*hub*), o serviço de descoberta *The Identity Selector Software* (*thiss.io*)[7] e o agregador de metadados pyFF[8]. O SaToSa atua como um *proxy* que permite a utilização de diversos protocolos de autenticação, enquanto o *thiss.io* é uma implementação de um DS com foco em melhorias de usabilidade. Ele segue os princípios da *SeamlessAccess*[9], sendo esse também um dos motivos de sua utilização no projeto. O pyFF, por sua vez, oferece suporte à personalização de fluxos de processamento e manipulação de metadados SAML, sendo plenamente compatível com o *thiss.io*. As escolhas desses componentes visam assegurar a eficiência e integridade das operações na Federação INOVA ID RS.

3. Resultados Preliminares

Por meio de sessões de *Design Thinking* (DT), conduzidas por analistas da RNP em cooperação com os participantes do ecossistema de inovação do Rio Grande do Sul, especificou-se os elementos da identidade digital denominada *InnovaPerson*, que representa um usuário da Federação com suas informações pessoais e vínculos institucionais. Outas sessões de DT foram conduzidas para idear a aplicação colaborativa (SP) que será implantada na fase de avaliação da Federação. Esta aplicação tem como propósito fazer a gestão e agendamento de uso de ambientes e recursos compartilhados pelos membros da federação. Por fim, atividades de cocriação foram também realizadas para definição do modelo de governança da Federação.

A aplicação IAM, denominada *GC-INOVA*, cujo desenvolvimento envolveu a utilização das tecnologias React.js (*frontend*) e Flask (*backend*) já foi concluída e testes de software foram conduzidos. *GC-INOVA* é uma aplicação voltada para a gestão do ciclo de vida das identidades digitais no contexto do ecossistema de inovação. Na fase de piloto, cada membro da Federação, implantará uma instância da aplicação *GC-INOVA*. Cada membro, contendo sua própria base de usuários, abriga uma diversidade de instituições. O papel do *GC-INOVA* reside na preservação das estruturas de dados essenciais para representar esses arranjos organizacionais e assegurar a integridade dos dados dos usuários, que serão sincronizados com o serviço de diretório utilizado.

Além de outras funcionalidades, o *GC-INOVA* possibilita o encaminhamento de convites, integração de usuários no serviço de diretório e administração dos perfis dos

[5] https://www.openldap.org
[6] https://github.com/IdentityPython/SATOSA
[7] https://thiss.io
[8] https://pyff.io
[9] https://seamlessaccess.org

usuários da federação. Para ilustrar seu funcionamento, uma demonstração da aplicação foi disponibilizada em `https://youtu.be/hfmBOFa6BeY`. Vale mencionar que a implantação da aplicação demo ocorreu na infraestrutura do GIdLab da RNP[10].

A implantação e configuração do núcleo da federação está em andamento, abrangendo a interconexão entre o SaToSa, *thiss.io* e PyFF. Os componentes do núcleo estão sendo configurados em ambientes de *containers*, visando acelerar significativamente a implantação e manutenção da federação.

No desenvolvimento do projeto foram superados desafios, dos quais se destacam: (i) a necessidade de estimular o envolvimento colaborativo dos parceiros no processo de co-criação, (ii) a disseminação efetiva dos conceitos, tecnologias e procedimentos ligados à gestão de identidade, e (iii) a tarefa de adaptação das bases de dados preexistentes das instituições integrantes da federação.

4. Considerações Finais

Neste trabalho foi apresentado o desenvolvimento do Projeto da Federação INOVA ID RS, que envolve a construção de uma identidade digital e a implantação de uma federação especializada para o ecossistema de inovação do RS.

O projeto encontra-se em desenvolvimento e tem previsão de ser concluído em maio de 2024. Como resultados preliminares, destacam-se: a definição da arquitetura da federação, o esquema de dados da identidade dos seus usuários, a modelagem da aplicação colaborativa definida pelos membros da federação (SP) em sessões de cocriação, a definição do modelo base de governança da federação e a documentação e o código-fonte da aplicação de gestão de identidade denominada *GC-INOVA*.

As próximas etapas do projeto envolvem a modelagem de negócios e sustentabilidade da federação, o desenvolvimento da aplicação colaborativa (SP), a conclusão da implantação em nuvem da arquitetura da federação e, por fim, a fase de operação do piloto da federação com quatro ambientes de inovação do Rio Grande do Sul (Zenit, Tecnopuc, Feevale TechPark, TecnoSinos e Instituto Caldeira).

Referências

Dabbaghi Varnosfaderani, S., Kasprzak, P., Pohl, C., e Yahyapour, R. (2019). A flexible and compatible model for supporting assurance level through a central proxy. In *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pages 46–52.

Jensen, J. (2011). Benefits of federated identity management - a survey from an integrated operations viewpoint. In Tjoa, A. M., Quirchmayr, G., You, I., e Xu, L., editors, *Availability, Reliability and Security for Business, Enterprise and Health Information Systems*, pages 1–12, Berlin, Heidelberg. Springer Berlin Heidelberg.

Secretaria de Inovação, Ciência e Tecnologia do Rio Grande do Sul (2022). *INOVA RS: Do desenho à implementação de uma estratégia centrada em ecossistemas regionais de inovação*. Secretaria de Inovação, Ciência e Tecnologia do Rio Grande do Sul, Porto Alegre - RS.

[10] `https://www.rnp.br/servicos/testbeds/gidlab`