

INOVA ID RS: Uma Federação de Identidade Aderente ao Ecossistema de Inovação Gaúcho

Rodrigo Cesar Lira da Silva¹, Rui de Quadros Ribeiro², Fiterlinge Martins de Sousa³,
Luciana E. Bandeira S. Ferreira⁴, Iara Machado⁵, Michelle Silva Wangham⁶

Resumo

Introdução: O Rio Grande do Sul destaca-se como um dos estados mais inovadores do Brasil, impulsionado por políticas públicas como o programa INOVA RS, que fortalecem o ecossistema de inovação local através de projetos voltados para o crescimento regional e social. Nesse contexto, o projeto INOVA ID RS, parte do INOVA RS, busca aprimorar a integração desse ecossistema. **Objetivo:** O INOVA ID RS tem como objetivo desenvolver um sistema de gestão de identidade e de acesso que se alinhe ao ecossistema de inovação gaúcho, facilitando a colaboração segura e o compartilhamento de serviços em um modelo federado de identidade. **Metodologia:** O desenvolvimento do projeto foi guiado por sessões de *Design Thinking*, onde os atores do ecossistema de inovação definiram aspectos, como a identidade digital, aplicações de interesse, governança e sustentabilidade da federação. A arquitetura *full mesh* com *proxy* foi adotada para garantir interoperabilidade entre os diferentes protocolos utilizados em provedores de serviço. Cinco ambientes de inovação do RS foram selecionados para participar da fase piloto da implantação. **Resultados:** Foi criado um esquema de dados, denominado *InovaPerson*,

¹ Mestre em Engenharia da Computação pela Universidade de Pernambuco - UPE. Professor do Instituto Federal de Pernambuco. E-mail: rodrigo.lira@paulista.ifpe.edu.br

² Bacharel em Ciências da Computação pela Universidade Luterana do Brasil - ULBRA. Analista de Tecnologia da Informação da Universidade Federal do Rio Grande do Sul. E-mail: rui.ribeiro@cpd.ufrgs.br

³ Doutor em Engenharia Elétrica pela Universidade Federal do Pará - UFPA. Analista de Sistemas na Diretoria de Pesquisa, Desenvolvimento e Inovação da Rede Nacional de Pesquisa - RNP. E-mail: fiterlinge.sousa@rnp.br

⁴ Especialista em Gestão de Projetos pela Universidade Cândido Mendes - UCAM. Coordenadora de projetos da Diretoria de Pesquisa, Desenvolvimento e Inovação da Rede Nacional de Pesquisa - RNP. E-mail: luciana.ferreira@rnp.br

⁵ Mestra em Computação Aplicada e Automação pela Universidade Federal Fluminense. Diretora de Pesquisa, Desenvolvimento e Inovação na Rede Nacional de Pesquisa - RNP. E-mail: iara.machado@rnp.br

⁶ Doutora em Engenharia Elétrica pela Universidade Federal de Santa Catarina. Gerente de Pesquisa e Desenvolvimento (P&D) em Cibersegurança da Rede Nacional de Pesquisa RNP. E-mail: michelle.wangham@rnp.br

integration among Rio Grande do Sul's innovation ecosystem members. Users can access various services without needing multiple registrations through a single federated account, which not only enhances security but also provides a more accurate view of the ecosystem.

Keywords

digital identity; identity and access management; information security; federation; innovation.

Introdução

A inovação é uma força propulsora do desenvolvimento econômico, permitindo às empresas melhorar a eficiência, criar novos produtos e responder às demandas do mercado. Nesse contexto, o Rio Grande do Sul se destaca no ambiente nacional por ser considerado um dos estados com mais empreendimentos inovadores (CENTRO DE LIDERANÇA PÚBLICA, 2023).

Esta posição é consequência de políticas de investimento em programas de ciências e tecnologia, que permitiram a expansão do ecossistema de inovação gaúcho. Complementando esse cenário, o estado tem uma ampla variedade de empresas tecnológicas, parques científicos, incubadoras de empresas, polos tecnológicos e instituições de ensino superior (IES) (SECRETARIA DE INOVAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO SUL, 2022).

Experiências anteriores demonstram que o poder público tem papel importante no desenvolvimento de políticas públicas para incentivar a inovação. Por exemplo, em Barcelona, na Espanha, uma área anteriormente considerada abandonada, tornou-se um importante centro de inovação ao ser tornada uma área de atividade econômica diversificada. Hoje, o *22@Barcelona* tornou-se um *case* de cidade inteligente e de revolução urbana (VILADECANS-MARSAL; ARAUZO-CAROD, 2012). Com base nessa e outras iniciativas semelhantes, o governo do Rio Grande do Sul criou o Programa INOVA RS⁷, uma política pública para desenvolver e incentivar a inovação no estado. Esse programa visa fortalecer os ecossistemas regionais, articulando a sociedade civil, os setores empresariais, acadêmicos e governamentais, em prol do desenvolvimento econômico e social regional. A missão dele é incluir o Rio Grande do Sul no mapa global de inovação até 2030. Nele, foram definidos projetos prioritários que respeitavam as características vocacionais de cada macrorregião do estado.

O INOVA ID RS é um projeto desenvolvido no contexto do Programa INOVA RS por meio de uma parceria formada entre a Rede Nacional de Pesquisa (RNP), Feevale e a Secretaria de Inovação, Ciência e Tecnologia do Rio Grande do Sul (SICT). Esse projeto

⁷<https://sict.rs.gov.br/programa-inovars>

visa desenvolver um sistema de gestão de identidade e de acesso aderente ao ecossistema de inovação gaúcho, que possibilite a colaboração segura e o compartilhamento de serviços em uma federação. Através da federação, a SICT poderá ter uma visão mais precisa sobre o ecossistema gaúcho como um todo.

Uma federação é um exemplo de ambiente federado que permite que organizações compartilhem recursos com base em acordos comerciais, confiança criptográfica e identificadores de usuário (AHMAD *et al.*, 2010). Do ponto de vista do usuário, ele dispõe de uma única identidade digital federada, que pode ser utilizada em diferentes provedores de serviços (do inglês, *Service Providers* - SP) implantados na federação (WANGHAM *et al.*, 2010). Isso elimina a necessidade de cada SP armazenar as credenciais dos usuários, delegando o processo de autenticação aos provedores de identidade (do inglês, *Identity Providers* - IdP) (TORROGLOSA-GARCÍA; SKARMETA-GOMEZ, 2017).

Este trabalho, portanto, apresenta os detalhes da concepção da federação INOVA ID RS, abordando as decisões tomadas durante o desenvolvimento do projeto, além de destacar os componentes e as tecnologias usadas na implantação desta federação.

Metodologia

A RNP é responsável por uma das maiores federações do mundo, a Comunidade Acadêmica Federada (CAFe)⁸. A experiência adquirida no desenvolvimento, implantação e gestão da CAFe desempenhou um papel fundamental na orientação do processo de desenvolvimento da nova federação. Contudo, é importante destacar que a federação proposta neste trabalho foi concebida com características diferentes da CAFe.

Para conceber uma federação alinhada ao ecossistema de inovação gaúcho, foi essencial realizar reuniões com os participantes desse ecossistema, nas quais eles puderam expressar suas expectativas e desafios. Inicialmente foram conduzidos *workshops* virtuais para explicar os princípios, benefícios e limitações dos sistemas de gestão de identidade e acesso (do inglês, *Identity and Access Management* - IAM). Em seguida, foram tomadas decisões importantes do projeto coletivamente por meio de sessões de *Design Thinking* conforme descrito em CUNHA *et al.* (2022).

A primeira decisão realizada utilizando a metodologia de *Design Thinking* foi a definição dos dados que seriam utilizados para representar a identidade digital federada. Em reuniões posteriores foram discutidas questões relacionadas a governança e o modelo de negócio utilizado para sustentabilidade da federação. Por fim, em um novo ciclo de ideação, os membros do ecossistema modelaram o primeiro serviço a ser implementado na federação.

⁸ <https://www.rnp.br/servicos/cafe>

Após analisar a literatura, a arquitetura *full mesh* com *proxy* foi a escolhida para a federação INOVA ID RS. Na arquitetura *full mesh*, não há a necessidade de uma entidade central, todos os componentes de identificação são distribuídos entre os membros da federação (CARRETERO *et al.*, 2018). Essa arquitetura é largamente utilizada na literatura devido a sua simplicidade e escalabilidade. O *proxy* foi um componente adicionado a arquitetura para permitir a inclusão de serviços utilizando outros protocolos, como o *OpenID Connect* (OIDC), amplamente adotado em serviços digitais de governo, como, por exemplo, o GOV.BR⁹. Em cada membro da federação foi implantado um IdP, uma instância do serviço de diretório e uma aplicação de IAM, denominada GC-INOVA.

O projeto foi desenvolvido com apoio do Serviço GidLab da RNP. O GidLab é um serviço para experimentação que oferece consultoria especializada e disponibiliza serviços e infraestrutura ligados à gestão de identidades (DALMAZO *et al.*, 2024). A infraestrutura do INOVA ID RS foi concebida para operar em um ambiente em nuvem, proporcionando economia de custos, flexibilidade e robustez na implantação.

Federação INOVA ID RS

A Figura 1 apresenta uma visão geral dos principais resultados do projeto: (i) desenvolvimento de uma identidade digital federada aderente ao ecossistema de inovação, (ii) definição de uma arquitetura que considera características dos ambientes de inovação, (iii) utilização de diferentes padrões de trocas de dados para permitir uma maior integração de serviços, (iv) implementação das relações de confiança para o funcionamento da federação, (v) implantação de fase piloto utilizando cinco membros do ecossistema de inovação, (vi) desenvolvimento de um serviço para agendamento de recursos e ambientes utilizando a autenticação federada, e por fim, (vi) um modelo de governança e sustentabilidade para a federação. Nos próximos parágrafos serão apresentados mais detalhes do desenvolvimento da federação INOVA ID RS.

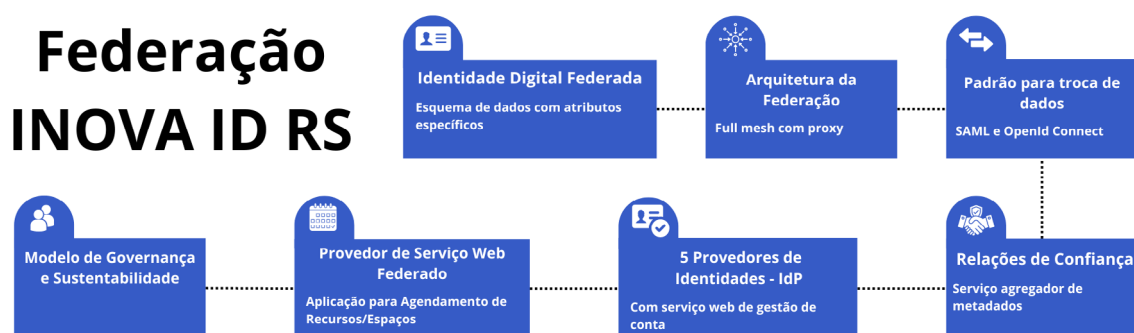


Figura 1 - Resultados principais da federação INOVA ID RS.

Fonte: Próprio autor.

⁹ <https://www.gov.br/conecta/catalogo/apis/brasil-cidadao-login-unico>

O acesso aos serviços de uma federação é feito por meio de uma identidade digital federada, fornecida pelos IdPs de cada membro da federação. O modelo do esquema de dados do serviço de diretório que armazena a identidade digital do INOVA ID RS é apresentado na Figura 2, onde são exibidos os atributos da usuária fictícia *helena*.

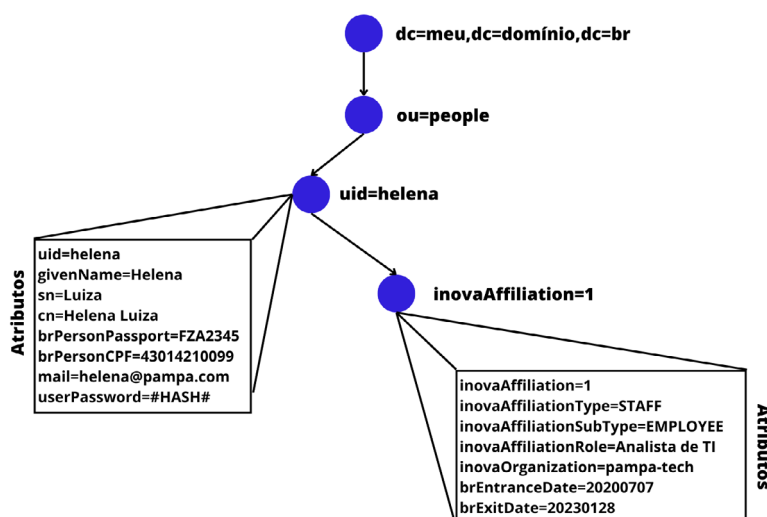


Figura 2 - Esquema de dados da identidade digital federada do INOVA ID RS.

Fonte: Próprio autor.

No esquema de dados foram indicadas informações essenciais para representar uma pessoa, como nome, sobrenome, e-mail, CPF ou passaporte, além de detalhes sobre possíveis afiliações do usuário no ecossistema de inovação. Essas afiliações são modeladas para armazenar dados como cargo, empresa, tipo e subtipo de vínculo, bem como as datas de início e término no cargo. Nas sessões de *Design Thinking* foram identificados três tipos principais de vínculos dos usuários do ecossistema de inovação. O primeiro grupo inclui indivíduos com vínculo profissional direto com o ambiente de inovação, como gestores, coordenadores de projetos e funcionários administrativos. O segundo grupo é composto por membros do ecossistema, vinculados a empresas ou startups associadas. Por fim, existem os usuários que fazem parte do ecossistema por trabalharem em parceiros institucionais, como as universidades, instituições governamentais e agências de fomento.

A Figura 3, apresenta os componentes que integram a arquitetura da federação. Na figura, o bloco '*Membro 1*' exemplifica a infraestrutura implantada para prover os recursos de um determinado ambiente de inovação. Na arquitetura adotada, os componentes são distribuídos, com cada membro implantando seu próprio IdP, conectado a um serviço de diretório local. Além desses componentes, o GC-INOVA, a aplicação de IAM desenvolvida para o projeto, também faz parte dessa estrutura. Essa configuração é particularmente interessante no contexto da regulação de proteção de dados pessoais, pois

cada ambiente de inovação é responsável (controlador) apenas pelos dados dos seus usuários.

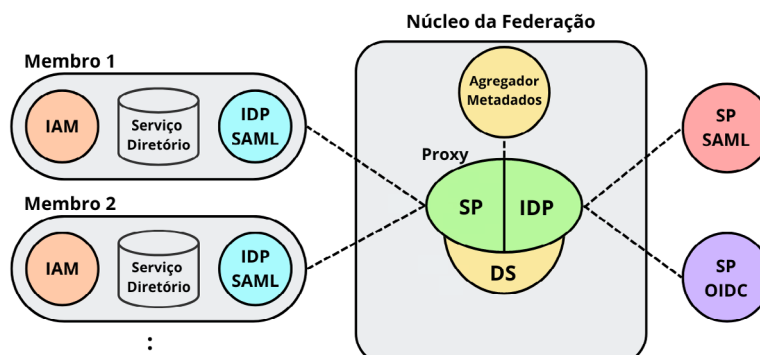


Figura 3 - Diagrama da arquitetura da federação INOVA ID RS.

Fonte: Próprio autor.

O *OpenLDAP*¹⁰ foi utilizado como serviço de diretório, servindo como a principal fonte de dados para o GC-INOVA e também fornecendo acesso ao esquema de dados da identidade digital ao IdP. Para a implantação do IdP, optou-se pelo *Shibboleth IDP*¹¹, um *framework* estável, de código aberto e amplamente utilizado em federações acadêmicas, como a CAFE.

O núcleo da federação foi construído utilizando projetos do *Identity Python*¹², uma iniciativa que integra uma variedade de ferramentas e projetos voltados para identidade digital, todos desenvolvidos em Python. Esse núcleo é composto por diversos componentes, incluindo o *proxy SaToSa*¹³, o serviço de descoberta (do inglês, *Discovery Service* - DS) conhecido como *The Identity Selector Software*¹⁴ (*thiss.io*) e o agregador de metadados *PyFF*¹⁵.

Para gerenciar o ciclo de vida das identidades digitais, foi criado a aplicação GC-Inova. Ela é composta por dois componentes: uma aplicação web desenvolvida em *ReactJS* e uma API construída em *Flask*. O GC-INOVA interage tanto com o serviço de diretório quanto com uma base de dados relacional em *MySQL*, conforme ilustrado na Figura 4.

¹⁰ <https://www.openldap.org>

¹¹ <https://www.shibboleth.net/>

¹² <https://idpy.org/>

¹³ <https://github.com/IdentityPython/SATOSA>

¹⁴ <https://thiss.io>

¹⁵ <https://pyff.io>

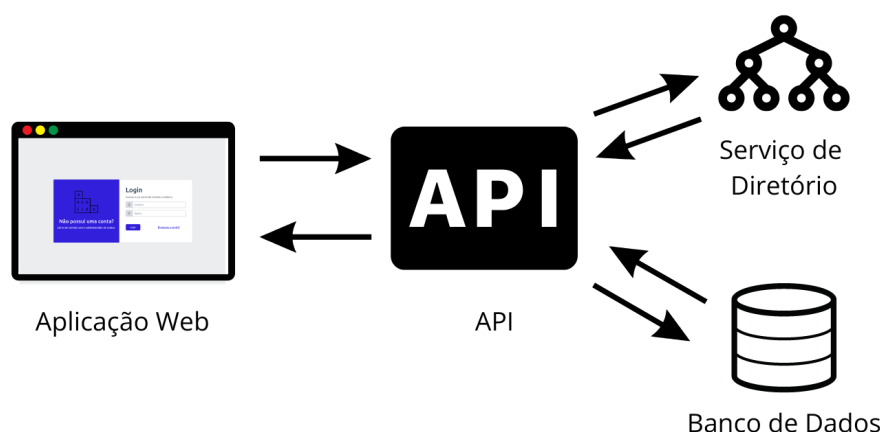
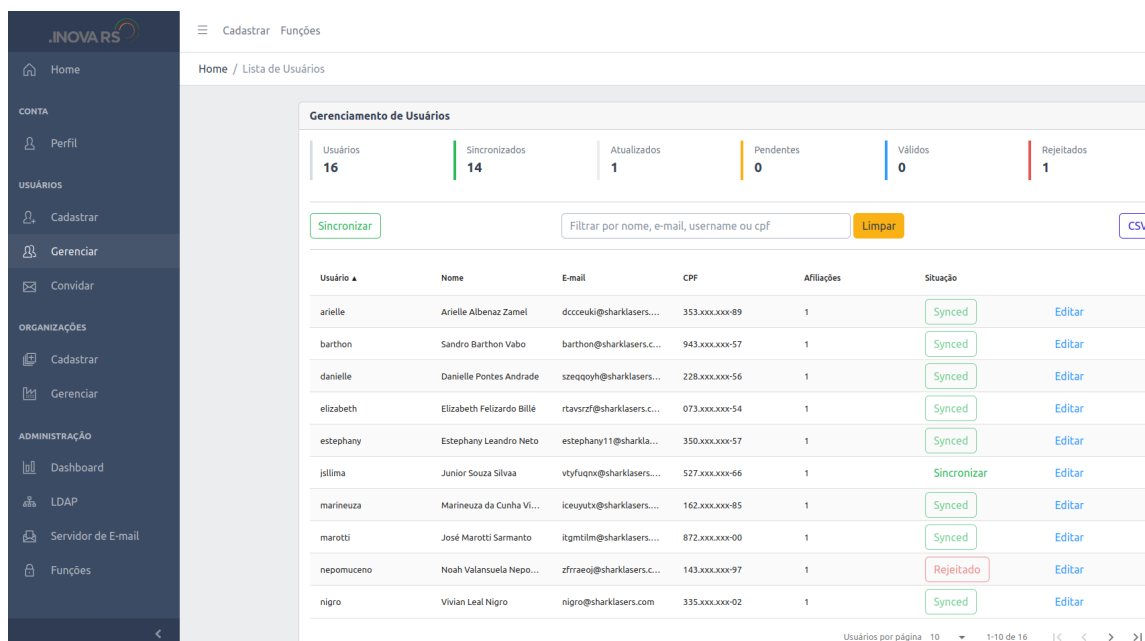


Figura 4 - Componentes da aplicação GC-INOVA, desenvolvida para gerenciar o ciclo de vida das identidades digitais.

Fonte: Próprio autor.

No GC-INOVA, o operador pode criar contas federadas diretamente na aplicação ou enviar convites de registro por e-mail. Além disso, é possível atribuir funções administrativas para usuários existentes. A Figura 5 exibe a tela onde o administrador gerencia as contas federadas do seu ambiente de inovação. O menu lateral oferece acesso a outras funcionalidades da aplicação.



| Usuário | Nome | E-mail | CPF | Afiliações | Situação |
|------------|---------------------------|---------------------------|----------------|------------|-------------|
| arielle | Arielle Albenaz Zamel | dcceuki@sharkslasers... | 353.xxx.xxx-89 | 1 | Syncced |
| barthon | Sandro Barthon Vabo | barthon@sharkslasers.c... | 943.xxx.xxx-57 | 1 | Syncced |
| danielle | Danielle Pontes Andrade | szeqoyh@sharkslasers... | 228.xxx.xxx-56 | 1 | Syncced |
| elizabeth | Elizabeth Felizardo Billé | rtavszf@sharkslasers.c... | 073.xxx.xxx-54 | 1 | Syncced |
| estephany | Estephany Leandro Neto | estephany11@sharkla... | 350.xxx.xxx-57 | 1 | Syncced |
| jsllima | Junior Souza Silvaa | vtyfuqx@sharkslasers... | 527.xxx.xxx-66 | 1 | Sincronizar |
| marineuza | Marineuza da Cunha Vi... | iceuyutx@sharkslasers... | 162.xxx.xxx-85 | 1 | Syncced |
| marotti | José Marotti Sarmanto | itgmtim@sharkslasers... | 872.xxx.xxx-00 | 1 | Syncced |
| nepomuceno | Noah Valansuela Nepo... | zfraeoj@sharkslasers.c... | 143.xxx.xxx-97 | 1 | Rejeitado |
| nigro | Vivian Leal Nigro | nigro@sharkslasers.com | 335.xxx.xxx-02 | 1 | Syncced |

Figura 5 - Funcionalidade de gerenciamento de contas federadas do GC-INOVA.

Fonte: Próprio autor.

Para validar a autenticação do INOVA ID RS e prover um primeiro serviço para a federação, foi desenvolvido um SP seguindo os requisitos definidos nas sessões de

Design Thinking. Esse serviço oferece um sistema de agendamento para a utilização de equipamentos e ambientes, facilitando o compartilhamento desses recursos entre os membros da federação com menos burocracia e maior segurança. A Figura 6 apresenta as telas da funcionalidade principal, que permite aos usuários pesquisar e agendar o uso de um equipamento ou ambiente previamente cadastrado por um membro da federação.

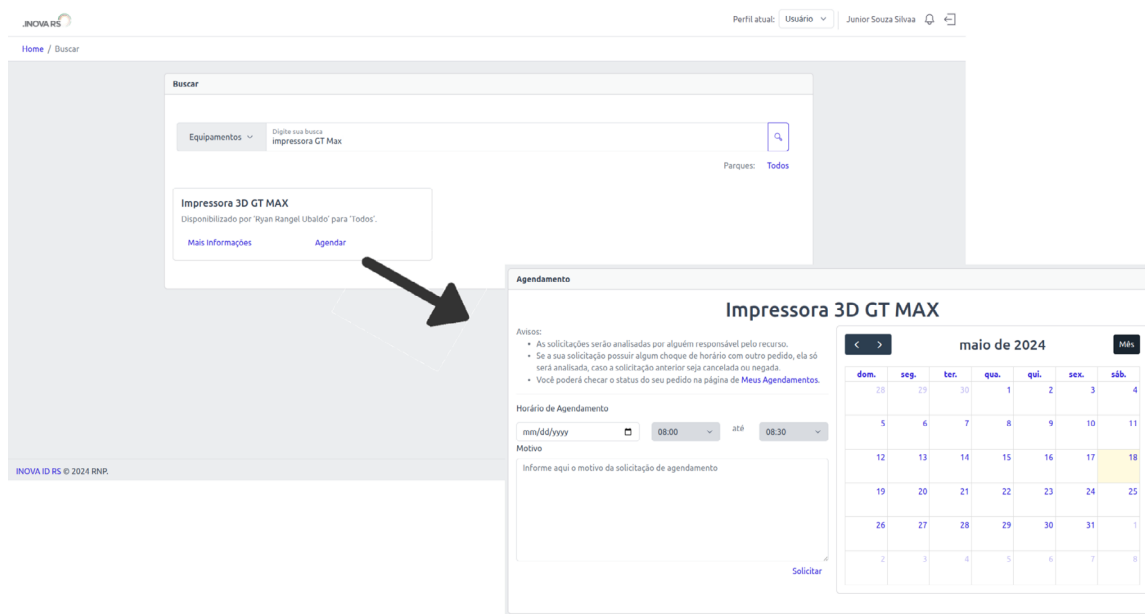


Figura 6 - Funcionalidade de solicitação de uso de um equipamento no SP desenvolvido.
Fonte: Próprio autor.

O SP desenvolvido também permite visualizar históricos, administrar pedidos de uso e gerenciar o acesso de usuários. Todas as ações geram notificações, exibidas na aplicação e enviadas ao e-mail cadastrado na conta federada. O sistema é composto por uma aplicação web desenvolvida em *ReactJS* e uma API construída em *Django*, que utiliza um banco de dados *PostgreSQL* para armazenamento de dados.

A autenticação federada é o único método de acesso ao SP, como demonstrado na Figura 7. Em (a) é apresentada a tela *login*. Clicando na imagem “INOVA RS”, o usuário é redirecionado para a tela do DS, exibida em (b). Nessa tela, o usuário deve selecionar em qual o ambiente de inovação que ele possui conta cadastrada. Em (c) é apresentada a tela do IdP do ambiente escolhido. Após indicar o usuário e senha válidos, o usuário é redirecionado para a aplicação protegida.

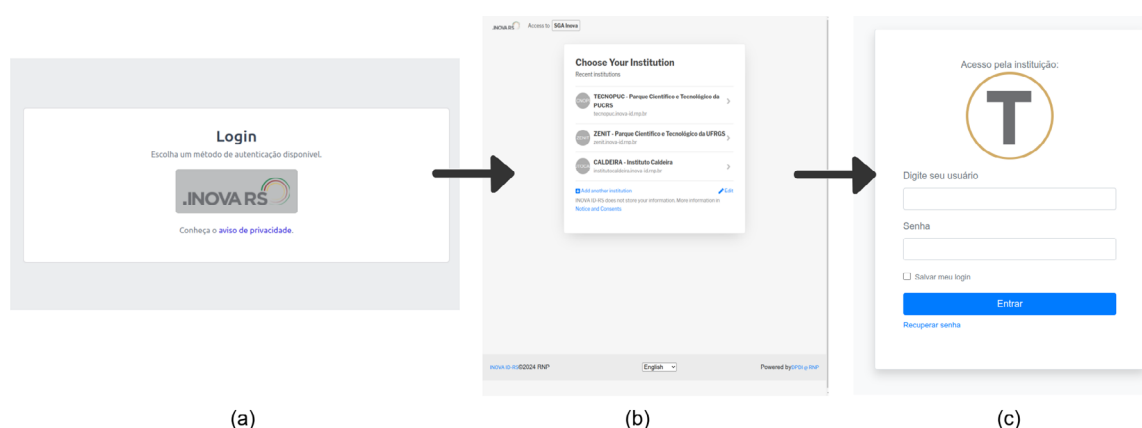


Figura 7 - Etapa de *login* no SP desenvolvido onde é utilizado a autenticação federada do INOVA ID RS.

Fonte: Próprio autor.

A fase piloto de utilização da federação INOVA ID RS foi iniciada com cinco ambientes do ecossistema de inovação do Rio Grande do Sul, sendo eles: Feevale Techpark, Tecnopuc, Tecnosinos, ZENIT e Instituto Caldeira. Durante essa fase, serão criadas contas federadas para que os primeiros usuários possam começar a utilizar a federação e o sistema de agendamento desenvolvido.

Conclusão

Neste trabalho é apresentado o desenvolvimento de um sistema de gestão de identidade federada para o ecossistema de inovação do Rio Grande do Sul. Com a identidade digital federada, será possível colaborar de forma segura e compartilhar serviços usando uma única credencial. Além disso, essa abordagem proporcionará uma visão mais abrangente e precisa do ecossistema de inovação. Essa também é uma oportunidade para que os conceitos de federação e gestão de identidade federada sejam testados no ecossistema de inovação do Rio Grande do Sul.

O projeto foi conduzido de maneira colaborativa, com os usuários definindo aspectos do desenvolvimento por meio de sessões de *Design Thinking*. A arquitetura do projeto foi idealizada para ser escalável e ampliar as possibilidades de implantação de serviços. Foram desenvolvidas duas aplicações: o GC-INOVA e o SP para agendamento de recursos. Atualmente, está em andamento uma fase piloto da federação, que envolve os ambientes de inovação Feevale Techpark, Tecnopuc, Tecnosinos, ZENIT e Instituto Caldeira.

Entre as atividades futuras, está prevista a realização de uma pesquisa de satisfação com os membros atuais da federação INOVA ID RS. Além disso, serão

integrados outros serviços existentes à federação e, finalmente, expandida para abranger todo o ecossistema de inovação.

Referências

CENTRO DE LIDERANÇA PÚBLICA. **Ranking de Competitividade dos Estados.** 2023. Disponível em:

https://clp.org.br/wp-content/uploads/2024/05/Relatorio_tecnico-Estados_2023.pdf.

Último acesso: 05 de novembro de 2024.

SECRETARIA DE INOVAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO SUL. **INOVA RS: Do desenho à implementação de uma estratégia centrada em ecossistemas regionais de inovação.** 2022. Porto Alegre - RS. Disponível em:

<https://www.sict.rs.gov.br/upload/arquivos/202212/29105439-livro-inova-rs.pdf> . Último

acesso: 05 de novembro de 2024.

CARRETERO, J.; IZQUIERDO-MORENO, G.; VASILE-CABEZAS, M.; GARCIA-BLAS, J. **Federated identity architecture of the European eID system.** 2018. IEEE Access, 6, 75302-75326.

CUNHA, Lucas do M. N.; WANGHAM, Michele S.; MACHADO, Iara. **Trust and identity: designing an identity solution for digital innovation.** 2022. Anais do XXXIII ISPIM Innovation Conference "Innovating in a Digital World".

AHMAD, Zubair; AB MANAN, Jamalul-Lail.; SULAIMAN, Sulaiman. **User requirement model for federated identities threats.** 2010. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) (Vol. 6, pp. V6-317). IEEE.

TORROGLOSA-GARCÍA, Elena; SKARMETA-GOMEZ, Antonio F.. **Towards Interoperability in Identity Federation Systems.** J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 8.2 (2017): 19-43.

DALMAZO, L. M. T.; FARIAS, J.; Ribeiro-Filho, A.; SOUSA, F.; WANGHAM, M. S.. **Serviço GidLab: Impulsionando a pesquisa experimental em Gestão de Identidade.** 2024. Anais do Computer on the Beach, 15, 290-297.

SOUZA, M., MELLO, E.; WANGHAN, M. (2014). **CAFe Expresso: Comunidade Acadêmica Federada para Experimentação usando Framework Shibboleth.** XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais-SBSeg, 405-414.

VILADECANS-MARSAL, Elisabet; ARAUZO-CAROD, Josep-Maria. **‘Can a Knowledge-based Cluster Be Created? The Case of the Barcelona 22@ District’**. Papers in Regional Science, vol. 91, no. 2, June 2012, pp. 377–401. ScienceDirect, <https://doi.org/10.1111/j.1435-5957.2011.00383.x>.

WANGHAM, M. S.; MELLO, E. R.; BÖGER, D. S., GUERIOS, M.; FRAGA, J. S. **Gerenciamento de Identidades Federadas**. 2010. Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, páginas 3–52.