Serviço GIdLab: Impulsionando a pesquisa experimental em Gestão de Identidade

Luan Matheus Trindade Dalmazo
luantrindade@ufpr.br
Universidade Federal do Paraná (UFPR)

Jorge Farias
jsfj@cin.ufpe.br
Universidade Federal de Pernambuco (UFPE)

Airton Ribeiro Filho
airton.r.filho@ufv.br
Universidade Federal de Viçosa (UFV)

Fiterlinge Sousa
fiterlinge.sousa@rnp.br
Rede Nacional de Ensino e Pesquisa (RNP)

Michelle Silva Wangham
wangham@univali.br
Universidade do Vale do Itajaí (UNIVALI)

ABSTRACT

An available infrastructure for testing authentication and authorization flows is often necessary in the Identity Management (IdM) field. Creating virtual environments for this purpose can result in high costs in terms of time, effort, and resources required for building and maintaining these setups. Thus, GIdLab emerges as a laboratory dedicated to experimentation, provided by the Brazilian National Education and Research Network (RNP). GIdLab offers specialized consultancy in IdM with a tailor-made experimentation lab that provides a set of authorization and authentication infrastructures and an eduroam environment ready to be used by researchers and software developers. This article aims to describe GIdLab service, its infrastructure, the associated federations, the use of proxies, related projects, identity decentralized testbed, and, finally, the results obtained over ten years of supporting experimentation.

PALAVRAS-CHAVE

Experimentação, Gestão de Identidades, Federação Shibboleth, Federação SimpleSAMLphp, SATOSA

1 INTRODUÇÃO

A Gestão de Identidade (GId) ou ainda Gestão de Identidade e de Acesso engloba um conjunto de processos, políticas e tecnologias usado para garantir a identidade de uma entidade e assegurar a consistência de informações de uma identidade (identificadores, atributos e credenciais) para prover procedimentos de autenticação, autorização e auditoria em ambientes online [1].

Frente à rápida transformação digital e à redefinição dos perímetros de segurança da informação nas instituições, a relevância da área de GId se destaca. O aumento da sofisticação dos ataques e as crescentes demandas por segurança, proteção de dados pessoais e usabilidade colocam a GId como uma questão crucial, despertando interesse tanto na academia quanto nas empresas e no governo [2]. A importância da área pode ser visualizada em [3], no qual é evidenciado que 71% dos ataques cibernéticos foram devidos a credenciais comprometidas.

Desenvolver pesquisa aplicada na área de GId exige que os experimentos sejam conduzidos em um ambiente distribuído, no qual os pesquisadores frequentemente dedicam uma quantidade significativa de tempo para estabelecer a infraestrutura de GId para conduzir seus experimentos, apenas para descartá-la uma vez que a pesquisa é concluída. Configurar uma infraestrutura adequada para experimentação pode ser mais desafiador e demorado do que a própria investigação da pesquisa. A complexidade para montar tal ambiente depende da solução tecnológica escolhida [4]. É crucial destacar que os pesquisadores devem evitar o uso de serviços de GId em produção para conduzir suas pesquisas experimentais. Além disso, o desenvolvimento deste tipo pesquisa requer um ambiente escalável, distribuído, controlado e confiável.

A Rede Nacional de Ensino e Pesquisa (RNP) oferece às suas instituições usuárias três serviços na área de GId: a Infraestrutura de Chaves Públicas para ensino e pesquisa (ICPedu[1]), a Comunidade Acadêmica Federada (CAFe[2]) e o serviço de autenticação em redes sem fio (eduroam[3]). Com o objetivo de apoiar e realizar prospecção tecnológica na área de GId, em 2010, a RNP criou o Comitê Técnico de Gestão de Identidades (CT-GID). Em 2012, com o apoio do CT-GID, foi lançada a primeira edição do Programa de Gestão de Identidades (PGID), uma iniciativa que financia projetos de curto prazo de Pesquisa, Desenvolvimento e Inovação (PD&I), que tem como objetivos fomentar uma interação contínua da comunidade acadêmica com o CT-GId e fornecer insumos, tanto conceituais como práticos, para a evolução dos serviços oferecidos pela RNP, tanto novos quanto futuros e para investimentos futuros em PD&I.

Os serviços de GId oferecidos pela RNP não permitem em suas políticas de uso que pesquisadores os utilizem para realizar seus experimentos práticos. Diante da demanda por infraestruturas de autenticação e autorização para conduzir os projetos de pesquisa e desenvolvimento do PGID, o CT-GID inicia o projeto GIdLab.

Este artigo apresenta o GIdLab[4], um serviço para experimentação em Gestão de Identidade, ofertado por meio de uma consultoria especializada, que tem por objetivo disponibilizar aos pesquisadores um ambiente controlado de testes para que estes possam conduzir experimentos com Infraestruturas de Autenticação e de Autorização (IAAs). O serviço é customizado para a execução de experimentos e pode ser configurável, por possuir infraestrutura aberta para a implantação de novas tecnologias e/ou soluções. O projeto GIdLab foi iniciado em fevereiro de 2013 e, desde 2017 é ofertado pela RNP como um serviço para experimentação tendo como público alvo

[1] https://pessoal.icpedu.rnp.br/home
[2] https://www.rnp.br/servicos/cafe
[3] https://www.rnp.br/servicos/eduroam
[4] https://www.rnp.br/servicos/testbeds/gidlab

pesquisadores e desenvolvedores brasileiros, principalmente, os participantes do PGID, dos Grupos de Trabalho (GTs) e colaboradores da RNP envolvidos no desenvolvimento de novos serviços e soluções. Apenas em 2023, foram conduzidos 23 atendimentos associados a projetos de experimentos no GIdLab .

O GIdLab disponibiliza uma série de tecnologias e serviços de gestão de identidade, a saber:

- Uma federação SAML, baseada no framework Shibboleth, conhecida como CAFe Expresso, com IdPs e SPs prontos para uso e construída aos moldes da Comunidade Acadêmica Federada (CAFe);
- Oferece um serviço de proxy, utilizando SATOSA e a plataforma COManage pronta para o gerenciamento de VO (*Virtual Organization)*;
- Uma federação SAML que utiliza o framework SimpleSAMLphp (SSP), incluindo um proxy SAML SSP.
- Um ambiente OpenID Connect que utiliza o Keycloak e o OpenID Connect playground;
- Um ambiente para experimentos de gestão de identidades descentralizadas (IDD);
- Um ambiente de testes Eduroam;
- Um repositório com um conjunto de máquinas virtuais (VMs) e contêineres Docker para implantar provedores de federação;
- Um serviço de atendimento ao cliente de primeiro nível (Service Desk), além de um serviço técnico especializado para auxiliar pesquisadores e desenvolvedores.

Este artigo discute na Seção 2 os trabalhos relacionados; na Seção 3 apresenta os serviços e tecnologias oferecidas; na Seção 4 são apresentados os resultados alcançados; na Seção 5 são sugeridas pesquisas exploratórias que podem utilizar esse serviço; e, por fim, na Seção 6, são apresentadas as conclusões e as indicações de trabalhos futuros.

2 TRABALHOS RELACIONADOS

Os trabalhos relacionados descritos nessa seção foram selecionados por meio da execução de um protocolo de revisão da literatura, considerando as bases *IEEE Xplore, ACM Digital Library, Springer Link e Science Direct*. Os doze trabalhos identificados passaram por um análise para determinar sua relevância para o escopo do serviço GIdLab. A inclusão dos trabalhos seguiu os seguintes critérios: trata de gestão de identidades federadas, envolvimento com ambientes para experimentação, ou ambos. Por outro lado, os critérios de exclusão englobaram trabalhos que não tratavam da gestão de identidades ou aqueles aos quais não foi possível ter acesso.

O ***GÉANT World Testbed Facility***, Farina et al. [5] utiliza uma infraestrutura distribuída com autenticação federada, autorização e controle de acesso para prover instalações de teste distribuídas em grande escala que sejam semelhantes aos ambientes do mundo real, tipicamente multidomínios, a fim de garantir a adaptação ágil de novos conceitos, arquiteturas, tecnologias e protocolos, desde a prototipagem, passando pelos testes, até a produção.

O trabalho intitulado ***Credential translations in Future Internet testbeds federation***, F. Silva et al.[6] apresenta o design e a implementação de um módulo para tradução de credenciais que permite ao usuário de uma federação de autenticação e autorização acadêmica (A&A), como a CAFe (Comunidade Acadêmica Federada Brasileira), acessar a federação de *testbed* FI (*Future Internet*). Isso se tornou necessário a partir do problema de gerenciamento de identidades em um ambiente distribuído globalmente criado com os avanços na implantação de *testbeds* para internet do futuro.

O *OpenStack* é um projeto de computação em nuvem de código aberto, e o trabalho: ***Adding Federated Identity Management to OpenStack***, W. Chadwick et al.[7] tem como objetivo adicionar um gerenciamento de identidade federada independente de protocolo aos serviços *OpenStack*. Embora muitas implantações de nuvem possam ser autônomas, são necessárias nuvens comunitárias federadas seguras e, portanto, deve haver métodos para gerenciamento de identidade federada.

Embora a visão do 5G seja acomodar milhares de milhões de dispositivos e aplicações IoT (*Internet of Things*), o seu sucesso depende muito da sua capacidade de fornecer segurança melhorada e acessível. O artigo ***Identity Federation for Cellular Internet of Things***, Santos et al. [8] apresenta uma solução de Federação de Identidades que reutiliza a autenticação SIM para dispositivos IoT celulares, permitindo login único.

Rapid Connect [9], uma forma fácil de conectar serviços a pesquisadores e educação superior australiana. O serviço AAF (*Australian Access Federation*) *Rapid Connect* permite que a AAF traduz asserções SAML que são verificadas por um Shibboleth SP padrão em *JSON Web Token* (JWT), que é mais adequado para uso por serviços com ambientes ou serviços restritos, sem necessidade de acessar algumas das partes mais avançadas da oferta da AAF.

Tabela 1: Comparação entre os Serviços Oferecidos no GIdLab e nos Trabalhos Relacionados.

Serviços Oferecidos	GIdLab	*GÉANT World Testbed Facility*	*Credential translations*	*OpenStack*	*Cellular Internet of Things*	*Rapid Connect*
Autenticação Federada	X	X	X	X	X	X
Ambiente de Testes	X	X	X			
Suporte à Identidade Descentralizada	X					
Suporte a IOT					X	
Eduroam	X					
Conteneirização	X					
OpenID e Oauth	X					
Proxies de Integração	X					

De modo a facilitar a comparação dos trabalhos relacionados com o Serviço GidLab descrito neste artigo, a Tabela 1 apresenta um resumo comparativo dos serviços oferecidos em cada um dos trabalhos. Todos os trabalhos citados são sobre gestão de identidades, e mais especificamente sobre autenticação federada. Porém, apenas o *Gêant World Testbed*[5] e o *Credential Translation* [6] tratam de ambientes de testes como o Gidlab. Outros serviços como o suporte a identidade descentralizada, eduroam, OpenId, Oauth, *proxies* de integração e conteneirização não são encontrados nos trabalhos relacionados. E o único serviço oferecido pelos trabalhos relacionados que não é oferecido pelo Gidlab é o suporte a IoT. O ponto principal da comparação é que apesar de trabalhos oferecerem alguns serviços o Gidlab concentra todos eles em um ambiente.

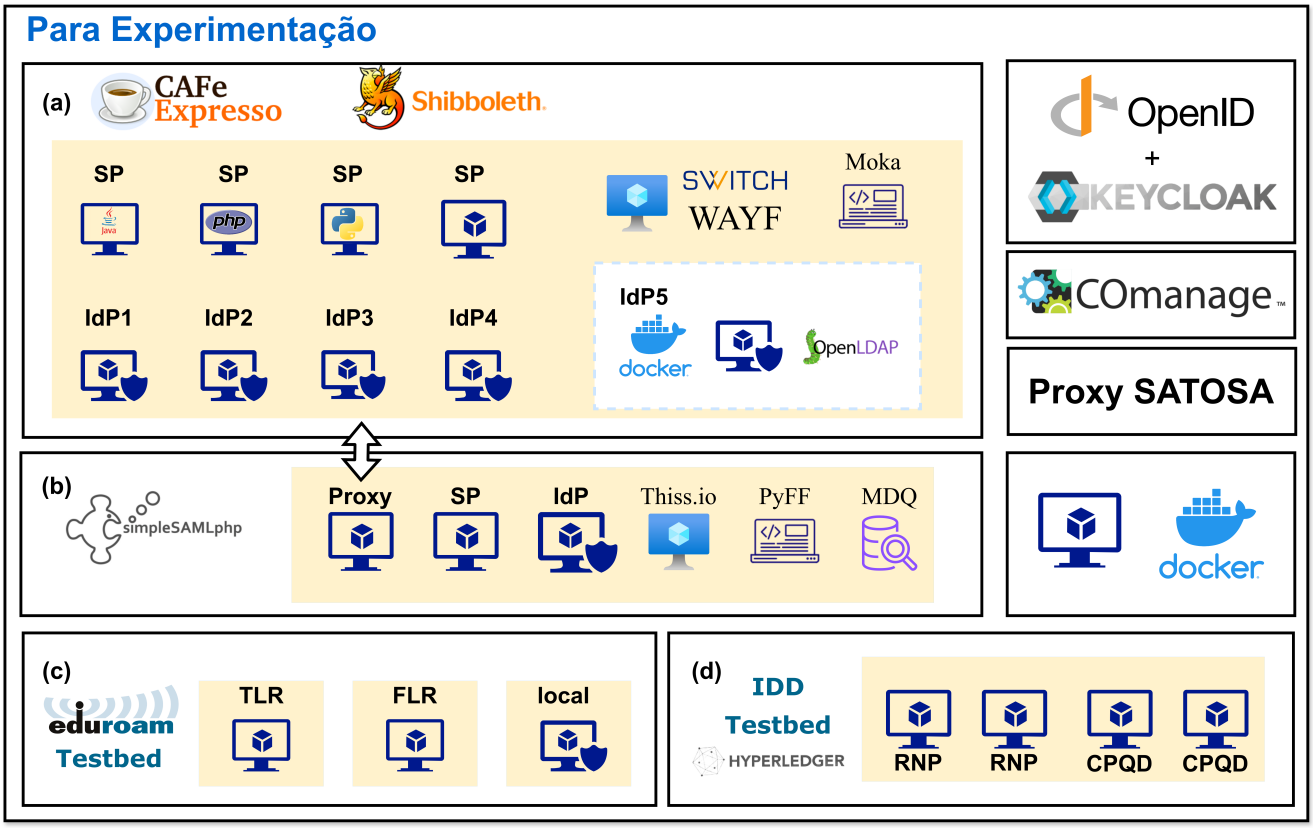

Figura 1: Projetos associados ao GIdLab. (a) Remete a Federação CAFe Expresso, (b) Federação SimpleSAMLphp, (c) Testbed eduroam e (d) ao Testbed de Identidade Descentralizada.

3 SERVIÇOS E TECNOLOGIAS OFERECIDAS

Os serviços e tecnologias que fazem parte do GIdLab podem ser visualizados na Figura 1. A ilustração demonstra a presença de duas federações: CAFe Expresso e SimpleSAMLphp, um ambiente de experimentação eduroam, e projetos individuais como OpenID Connect (OIDC) com *Kleycloak*, COmanage, *Proxy* SATOSA e uso da tecnologia de container para casos específicos. Nas próximas seções, serão apresentados alguns dos protocolos utilizados, os serviços ofertados serão descritos em profundidade, e ao fim, os recursos computacionais ofertados serão detalhados.

3.1 Protocolos

Os protocolos desempenham um papel essencial na comunicação e na segurança das informações em ambientes digitais. Além disso, os protocolos são fundamentais para assegurar a interoperabilidade entre diferentes plataformas e serviços. No GIdLab, os principais protocolos utilizados são RADIUS, SAML, OAuth e o OIDC.

Dentre os diversos protocolos utilizados, alguns se destacam por suas contribuições específicas. O RADIUS, por exemplo, é essencial em ambientes de redes, permitindo a autenticação remota de usuários e o controle de acesso a recursos [10]. Já o OAuth 2.0 se destaca ao viabilizar a delegação segura de acesso a recursos entre aplicações, sem a necessidade de compartilhamento de senhas [11]. Complementando o OAuth 2.0, o OIDC oferece uma camada adicional de identificação de usuários, fortalecendo a segurança em sistemas distribuídos [12]. Por fim, o SAML desempenha um papel crucial em ambientes que requerem autenticação única, possibilitando a troca segura de informações de autenticação e autorização entre diferentes partes [13]. Esses protocolos, cada um em sua área de atuação, desempenham um papel crucial na construção de sistemas seguros e interoperáveis.

3.2 Federações

Em GId, comumente o uso de federações, entidades capazes de realizarem a troca de informações de forma segura [14], é amplamente utilizado. Em tais entidades, normalmente encontra-se presente um provedor de identidades (IdP) e um provedor de serviços (SP), o primeiro é responsável pelo gerenciamento e armazenamento de credenciais, enquanto o segundo oferece serviços para usuários autorizados [15]. É comum ainda que as federações contenham vários IdPs, para tal cenário, o uso de um serviço de descoberta é encorajado, para que o usuário no fluxo de acesso ao SP, possa escolher o provedor de identidades a ser utilizado. Ainda, cada SP e IdP possui um arquivo XML (*Extensible Markup Language*) contendo seus metadados, com descritores que representam aspectos de suas configurações, portanto, o uso de um agregador de metadados é

necessário no contexto federativo, para que esta tecnologia possa gerenciar e monitorar o metadado de seus constituintes. Nos próximos tópicos, serão abordadas as federações presentes no GIdLab, de forma a detalhar as tecnologias presentes e evidenciar seus usos.

3.2.1 CAFe Expresso. É uma federação Shibboleth, composta por IdPs, sendo esses populados com dados de usuários fictícios com diferentes perfis e atributos, SPs e um serviço WAYF (*Where Are You From*), nos moldes das entidades presentes na federação CAFe. Os SPs permitem ao pesquisador hospedar aplicações desenvolvidas em Java, PHP, Python ou um SP padrão shibboleth. É ofertado também um IdP MFA (*Multi-factor authentication*) e também um IdP em container, que oferece a capacidade de empacotar e executar o IdP em um ambiente isolado. O *framework* Shibboleth é utilizado por federações acadêmicas de diversos países, incluindo a Comunidade Acadêmica Federada (CAFe) do Brasil. A especificação Shibboleth define um protocolo para descoberta de serviços, o Serviço de Descoberta (Discovery Service - DS), que possibilita a descoberta de provedores de serviços e de identidades. Na CAFe Expresso, é possível fazer uso de dois serviços de descoberta: WAYF ou EDS (*Embbeded Discovery Service*). O funcionamento de ambos é semelhante: apresentar para o usuário uma lista com os IdPs da federação e, uma vez que o usuário escolhe um IdP, redirecioná-lo para a página do IdP escolhido. Os SPs e IDPs provém metadados utilizados para estabelecer uma relação de confiança entre as entidades, para agregar esses metadados é utilizado o agregador de metadados Moka. Essa ferramenta é uma versão utilizada na federação CAFe que permite além de agregar metadados fazer uma verificação da sua integridade. Na Figura 1 (a), são apresentadas todas as entidades presentes no ambiente CAFe Expresso.

O Shibboleth oferece um módulo para o servidor Apache HTTP para entrega de forma transparente de asserções SAML [16]. As aplicações Python web são disponibilizadas por meio de dois servidores, sendo um deles um servidor HTTP que atua como proxy. O trabalho [16] mostra uma forma de composição de contêineres baseados na arquitetura de microsserviços para ofertar uma aplicação web Python como um SP Shibboleth.

3.2.2 Federação SimpleSAMLphp. O SimpleSAMLphp (SSP) é um framework desenvolvido em PHP [17], a aplicação é versátil quanto ao uso, a qual pode ser configurada como IdP, SP ou *proxy*, é também possível fazer uso de módulos externos como *cronn* e *metarefresh* para tornar a tecnologia ainda mais robusta.

No contexto dessa federação no GIdLab, o serviço de descoberta utilizado é o Thiss, oferecido pela *Coalition for Seamless Access* [18], a implementação oferece a possibilidade de armazenamento do último IdP utilizado, opção para personalização de idiomas, estilização e pesquisa inteligente dentre os metadados da federação. Quanto ao gerenciamento dos metadados dos constituintes da federação SimpleSAMLphp, faz-se uso do PyFF, tecnologia agregadora de metadados, com monitoramento e gerenciamento dos arquivos XMLs dos membros da federação [19].

A federação conta ainda com um *proxy*, configurado também com o framework SimpleSAMLphp, capaz de expandir o acesso da federação atual para as demais que utilizem de outro framework (a exemplo do Shibboleth). Em resumo, a federação como um todo pode ser visualizada na Figura 1 (b).

3.3 Eduroam

Eduroam (Education Roaming) é uma rede serviços internacional para acesso sem fio (roaming) para comunicação de usuários em pesquisa e educação [20]. O serviço oferece conectividade à internet através de conexão sem fio (Wi-Fi) para estudantes, pesquisadores e funcionários de instituições de ensino e pesquisa e ao visitar instituições parceiras. As instituições não precisam fornecer nomes de usuários e senhas temporárias ou compartilhadas de maneira insegura. Por meio do eduroam, as NRENs (National Research Network) oferecem um serviço altamente visível e valorizado que auxilia diretamente suas instituições clientes e seus usuários.

O eduroam permite que qualquer usuário de uma instituição participante tenha acesso à rede de qualquer outra instituição conectada no eduroam. As credenciais dos usuários são fornecidas pela instituição de origem e ao se conectar em um ponto de acesso de outra instituição que esteja visitando, seus dados não são armazenados, sendo enviados a instituição de origem para verificação e validação do acesso.

O serviço eduroam utiliza hierarquia de servidores RADIUS e pontos de acesso sem fio IEEE802.11, que estão distribuídos pelas instituições de ensino participantes. A infraestrutura do testbed eduroam está distribuída nos PoPs da RNP e é reprensentada na Figura 1 (c). A configuração do testbed eduroam possui três níveis de servidores RADIUS: local, nacional (federação) e top-level da confederação. No nível local, tem-se 2 servidores que representam instituições. No nível da federação, tem-se 1 servidor *proxy*. No nível da confederação, 1 servidor top-level pronto para ser configurado com outras federações. Todas as tecnologias utilizadas para implementação do testbed são de código livre.

3.4 *Proxies* de Integração

Os proxies desempenham um papel crucial em ambientes de autenticação e autorização federadas, oferecendo diversas possibilidades de uso. Por exemplo, podem ser utilizados para consolidar múltiplos serviços digitais sob o controle de uma única organização, permitindo que apareçam como um único SP para um IdP externo ou para a Federação [21]. Isso simplifica o processo de registro, pois apenas o proxy precisa ser registrado como SP. Outro exemplo, os *proxies* podem atuar como pontes, recuperando recursos de servidores e repassando por meio de protocolos diferentes como SAML, OAuth2 e OpenID Connect. Esses casos de uso exemplificam como os *proxies* facilitam a interoperabilidade entre diferentes sistemas, superando barreiras de protocolos e formatos de troca de dados. A seguir, serão detalhados os *proxies* de integração presentes no Serviço GIdLab.

Para possibilitar a tradução entre diferentes protocolos de comunicação e utilizar bases de logins sociais, o GIdLab utiliza um *proxy* chamado SATOSA[5]. O SATOSA também é utilizado quando o SP possui alguma limitação para ingressar em federações. Isso assegura uma maior capacidade de integração entre diferentes ferramentas. A tecnologia é implementada em Python, é modular com o uso de *plugins*, e tem como principal objetivo simplificar e tornar mais eficiente a implementação de autenticação federada em diversos contextos, reduzindo a complexidade e os desafios técnicos envolvidos nesse processo. Na Figura 2 temos a arquitetura do

[5] https://github.com/IdentityPython/SATOSA

SATOSA mostrando alguns dos seus componentes. Os *plugins* de *backend* são estruturas que funcionam como SP e essas estruturas conectam em IdPs que estão fora da infraestrutura do SATOSA. Os *plugins* de *frontend* permitem configurar IdPs para habilitar SPs que estarão sob o domínio do SATOSA. Já os *plugins* de microsserviços dão suporte desde mapeamentos de atributos até roteamento das requisições de entradas e saída.

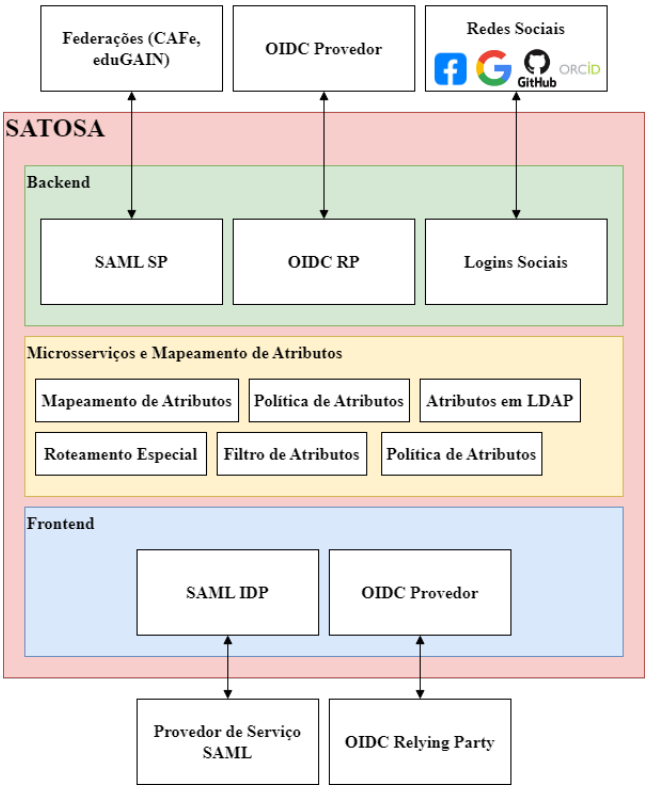

Figura 2: Arquitetura SATOSA.

Para a comunicação entre a Federação SimpleSAMLphp e a CAFe Expresso, é utilizado o *proxy* SSP[6]. O SSP fornece suporte para SAML 2.0 tanto para SPs quanto para IdPs. No entanto, ele também suporta outros protocolos e estruturas de identidade, como CAS, OpenID Connect, WS-Federation e OAuth. A importância desse *proxy* reside na capacidade de possibilitar a comunicação entre diferentes federações. Dessa forma, um SP localizado na Federação SimpleSAMLphp pode facilmente se comunicar com um IdP presente na CAFe Expresso.

Outra forma de utilização de *proxy* é habilitando *SAML Proxy* no *framework* Shibboleth IdP.Dessa forma, o Shibboleth IdP funciona como um intermediário entre os provedores de identidade e os provedores de serviços, facilitando a troca de informações de autenticação por meio do protocolo SAML. O Shibboleth IdP é uma solução confiável, bem estabelecida e está em uso em todas as instituições que aderiram a CAFe. Ao usar o *SAML Proxy*, o Shibboleth IdP amplia a sua capacidade de integração com uma ampla variedade de sistemas e aplicativos, tornando-o adequado para ambientes complexos e heterogêneos. O Shibboleth IdP oferece suporte a padrões de segurança rigorosos, garantindo a proteção dos dados durante todo o processo de autenticação e essas garantias são mantidas ao utilizá-lo como *proxy*.

[6]https://simplesamlphp.org/

3.5 Solução para Gestão de Times (Organizações Virtuais)

As universidades ou departamentos de pesquisa podem formar coletivamente uma Organização Virtual (OV) [22]. Estas OVs podem pertencer a federações distintas, e para a administração eficiente das identidades organizacionais, opta-se pelo modelo de gestão de identidades federado.

Para esse objetivo, o COmanage (*Collaborative Organization Management*) surge como uma solução promissora para o gerenciamento e controle de membros das organizações, enquanto simultaneamente viabiliza mecanismos de acesso federado. O projeto fundamenta-se em dois componentes principais: um *registry* destinado à administração da colaboração e do ciclo de vida dos membros; e APIs projetadas para integrar aplicações federadas aos atributos e informações essenciais para o controle de acesso.

3.6 *Testbed* de Identidade Descentralizada

A sociedade está organizada em sistemas políticos que possuem estruturas governamentais com papéis bem definidos e cabe somente a estas a soberania para identificação de seus cidadãos. Desta forma, o conceito de Identidade Digital Descentralizada (IDD), também chamada de Identidade Autossoberana, do inglês *Self Sovereign Identity* (SSI) propõe-se em dar ao usuário a soberania para administrar suas identidades digitais e não em criá-las [23].

No modelo descentralizado, o próprio usuário é o responsável por manter suas identidades digitais, por exemplo, em um aplicativo de carteira digital em seu telefone inteligente, cujos atributos são atestados criptograficamente por seus emissores (e.g. Secretaria de Segurança Pública) e poderão ter sua integridade e autenticidade verificada pelos provedores de serviço [14].

A crescente demanda por aplicações de IDD que interagem com redes *blockchain* impulsionou a pesquisa e o desenvolvimento de um ambiente de experimentação dedicado. Essa iniciativa expandiu a infraestrutura do GidLab, atendendo às necessidades dessa nova área de pesquisa[24]. O ambiente desenvolvido é baseado na plataforma *Hyperledge Indy* [25]. No protótipo de *testbed*, tem-se a execução do *ledger* base, no qual é possível criar aplicações e provas de conceito utilizando essa base. O protótipo se constitui em uma rede formada por nós de duas instituições envolvidas no projeto (RNP e CPQD), onde cada instituição possui dois nós, como ilustrado na Figura 1 (d).

3.7 Recursos disponíveis

O GIdLab, serviço para experimentação dedicado à gestão de identidade, possui uma infraestrutura composta por 46 máquinas virtuais. Destas, 20 formam o núcleo do serviço, abrigando os componentes fundamentais do ambiente de experimentação. Essas máquinas centrais são estrategicamente configuradas com 4 IdPs, incluindo uma implementação do pacote MFA (Multifator de autenticação) da federação CAFe. Além disso, apresentam 4 SPs, 2 serviços de

descoberta, 2 agregadores de metadados distintos, um conjunto de 4 VMs para um testbed completo da Eduroam, uma instância do Keycloak, uma instância do proxy SATOSA, entre outras. As bases LDAP utilizadas nos 4 IdPs possuem um conjunto de usuários fictícios previamente configurados para possibilitar a realização do fluxo completo de autenticação.

As demais VMs, fora do núcleo, desempenham papéis cruciais no suporte à pesquisa e desenvolvimento no GIdLab. Elas servem como ambientes flexíveis para experimentação, oferecendo aos pesquisadores a capacidade de explorar projetos específicos relacionados à gestão de identidade. Entre os projetos em andamento, destacam-se experimentos com Shibboleth integrado ao Azure AD, implementação de Eduroam em redes 5G, utilização do OAuth2 (FileSender), autenticação FIDO passkeys, implementação do CoManage, exploração do Eduroam com suporte a wifi 6 e desenvolvimento de Service Provider utilizando .NET.

Atualmente, as máquinas virtuais que compõem o núcleo do GIdLab são monitoradas através da ferramenta Centreon. Esse monitoramento vai além dos recursos de hardware, abrangendo também os serviços específicos de cada VM, tais como Jetty, Apache2, Nginx, Tomcat, Mysql, entre outros. No Centreon, são configuradas visualizações personalizadas para proporcionar uma melhor compreensão do estado das VMs. Além disso, alertas são emitidos pelo Centreon para um grupo criado no Microsoft Teams sempre que uma VM entra em estado crítico.

O GIdLab surge, portanto, como um ecossistema de GId dinâmico, onde a pesquisa e o desenvolvimento tecnológico convergem para impulsionar a inovação em tecnologias de GId. Sua infraestrutura diversificada reflete um compromisso com a exploração contínua de soluções avançadas no campo da identidade digital.

4 RESULTADOS

Ao longo dos dez anos de atividade do serviço para experimentação, foram atendidos um total de 126 projetos experimentais. A Figura 3 ilustra a distribuição anual dos projetos, especificando aqueles categorizados como externos e os projetos diretamente associados à RNP. Torna-se evidente uma tendência nos dois últimos anos (2022 e 2023) de atendimentos a instituições fora da Rede Nacional de Ensino e Pesquisa, com o intuito de fornecer meios e tecnologias para diversas instituições do país.

Além disso, é possível observar um aumento no número de chamados, conforme evidenciado pela Figura 3. Esse crescimento, especialmente nos últimos dois anos, reflete a crescente demanda por tecnologias associadas a GId, destacando um terreno fértil para exploração e experimentação na área.

A Figura 4 ilustra a distribuição geográfica desses atendimentos, considerando o mapa do Brasil, é necessário pontuar que nessa ilustração foram excluídos os apoios realizados a projetos internos da RNP, e duplos atendimentos de uma mesma instituição. O Serviço GidLab atuou nas cinco regiões do país e, no total, ofereceu suporte a mais de 38 instituições.

Em 2023, totalizam-se 23 atendimentos, sendo que 15 deles já foram finalizados. Dentre esses projetos, uma parte considerável está associada diretamente à Federação CAFe Expresso, em especial ao desenvolvimento de aplicações web federadas (SPs).

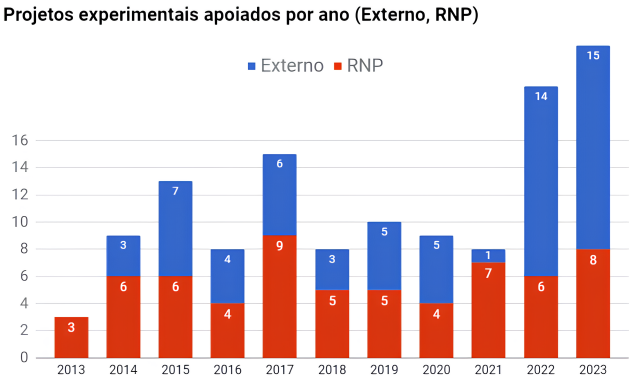

Figura 3: Número de projetos atendidos do GIdLab.

Figura 4: Distribuição geográfica das instituições atendidas.

4.1 Estudo de caso

O GIdLab obteve sucesso em várias experimentações com a infraestrutura oferecida. Alguns projetos usaram mais de uma ferramenta para alcançar seus objetivos como, por exemplo, no atendimento do Laboratório Interinstitucional de e-Astronomia (LIneA[7]). O LIneA é uma plataforma cujo intuito é a participação brasileira em projetos de astronomia, com uma infraestrutura de *hardware* e *software* para processamento, armazenamento e distribuição de dados da área. O LIneA planejava estruturar seus usuários através de perfis categorizados, levando em consideração seus interesses e o estágio em suas carreiras científicas. Com a definição dos perfis dos usuários, o LIneA queria segmentar o acesso aos recursos do laboratório. Por exemplo, qualquer usuário registrado poderia navegar por todas as páginas marcadas como públicas, usar as ferramentes de visualização e catálogos. Para os estudantes e pesquisadores, eles definiram

[7] https://www2.linea.org.br/

três perfis de acesso delimitando recursos computacionais como quantidade de processamento e memória.

No atendimento do LIneA foi utilizado o COmanage (software de gerenciamento organizacional colaborativo) para definir e avaliar os perfis de acesso e para realizar o gerenciamento do ciclo de vida dos membros participantes. Foi usado também o proxy SATOSA para realizar a integração com diferentes fontes de identidade. A arquitetura utilizada no projeto pode ser visualizada na Figura 5, do lado esquerdo do diagrama estão os Logins Sociais e a Federação CAFe que são as fontes de identidades registradas no proxy SATOSA do LIneA, do lado direito do diagrama estão os serviços ofertados como *JupyterHUB* e *Science Portal*. O COmanage foi utilizado para criar o que eles denominaram como "Identidade LIneA", que são os dados de alguma das fontes de identidade com novas credenciais e atributos extras para organizar os recursos disponíveis em cada perfil de usuário.

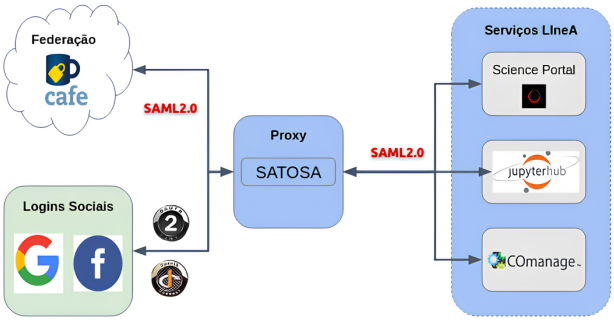

Figura 5: Arquitetura utilizada no LIneA.

4.2 Lições aprendidas

Os anos de operação do Serviço GIdLab trouxeram consigo uma série de aprendizados. O primeiro deles refere-se à importância da transferência de tecnologia sobre GId. Observa-se em muitos atendimentos de projetos de experimentos que os pesquisadores desconhecem os conceitos fundamentais, como os de identidade federadas. Devido a isto, já na primeira reunião com os pesquisadores que solicitam o uso do Serviço GidLab, a equipe técnica especializada conduz uma apresentação teórica sobre os principais conceitos e tecnologias. Para facilitar a compreensão de conceitos e do funcionamento de aplicações já implementadas no laboratório, são oferecidas demonstrações e roteiros para que os pesquisadores possam degustar, entender o fluxo de informação e avaliar seu uso.

Entende-se que o compartilhamento de conhecimento deve ser realizado de maneira externa e interna ao GIdLab. A cima foi detalhado a divulgação externa, mas, ainda há a formação interna dos integrantes. Assim, o projeto disponibiliza aos bolsistas a oportunidade de participar de cursos oferecidos pela Escola Superior de Redes (ESR). A ESR oferece cursos avançados em tecnologias de rede, proporcionando formação teórica e prática para profissionais de TI e engenheiros de redes. A seleção dos cursos é cuidadosamente realizada, visando atender às demandas específicas dos futuros atendimentos. Prioriza-se a escolha de cursos que não só abordem as tecnologias já estabelecidas, mas também aquelas emergentes, preparando a equipe para os desafios presentes e futuros do cenário da tecnologia da informação. Por exemplo, a equipe já realizou cursos como Gestão de containers com *Docker*, orquestração de containers com *Kubernetes* e Eduroam. Este investimento em educação continuada não apenas qualifica, mas também prepara para os possíveis novos desafios.

Outro fator aprendido ao longo dos anos de projeto é a importância do acompanhamento das novas demandas em GId. Isso envolve acompanhar relatórios de segurança, novas implementações de tecnologias e a oferta de novas soluções. Diante dessas necessidades, a RNP coordena o Comitê Técnico de Gestão de Identidade (CT-GId), responsável por apresentar demandas emergentes e sugestões tecnológicas. Ainda, os eventos promovidos pela REFEDS[8] e pela Internet2[9] são palcos para debates e exposições de perspectivas em GId. Por fim, o Workshop de Gestão de Identidades Digitais (WGID) é um evento no qual são apresentados conteúdos fundamentais para ampliar as visões quanto a área de Gestão de Identidade. Através dessas abordagens, é possível manter os serviços modernizados, de modo que possíveis necessidades possam ser antecipadas e atendimentos sejam realizados de maneira ainda mais rápida.

5 SUGESTÕES DE PESQUISAS EM GID

A Gestão de Identidade tornou-se um elemento central no panorama digital contemporâneo, à medida que organizações e serviços online buscam equilibrar a facilidade de acesso com a segurança robusta. Nesse contexto, a implementação eficaz de infraestruturas de autenticação e de autorização desempenha um papel fundamental. O GIdLab não se limita às infraestruturas atualmente em uso e está sempre aberto ao estudo e à implementação de novas tecnologias. Projetos que exploram a gestão de identidades podem se beneficiar significativamente do ambiente disponível no GIdLab. Esta seção apresenta as principais tendências relacionadas a GId para os próximos anos descritas no relatório de visão de futuro do Comitê Técnico de Gestão de Identidade da RNP (CT-GID).

O relatório de visão de futuro divide as principais tendências em GId em três horizontes. O primeiro horizonte apresenta as tendências para o próximo biênio, o segundo horizonte aborda as tendências que podem resultar em novos produtos ou serviços exploráveis em 2 a 3 anos, e o terceiro horizonte apresenta hipóteses que necessitam de validação, semeando iniciativas para futuros negócios que possam ser explorados em 5 anos ou mais [26].

No primeiro horizonte, as tendências em gestão de identidade estão concentradas na adoção de mecanismos inovadores para reforçar a segurança e simplificar os processos de autenticação. Prioridades incluem a implementação de autenticação sem senha, como o FIDO *Passkeys*, e a arquitetura de confiança zero integrada em soluções de nuvem. Além disso, a criação de um ecossistema para identidade descentralizada e o uso de certificados de assinatura única visam assegurar maior controle e privacidade dos usuários. Por fim, o suporte ao *Hotspot 2.0/Passpoint* e a integração ao *OpenRoaming* estão sendo investigados pela comunidade Eduroam, o que permitirá a ampliação da abrangência da cobertura do serviço e benefícios aos usuários [26].

As tendências citadas no segundo horizonte, são a gestão de identidade integrada com automação e inteligência artificial, visando

[8] https://refeds.org/
[9] https://internet2.edu/

otimizar processos e fortalecer a detecção de ameaças. A integração da eduroam com redes 5G que além de ampliar a cobertura, traz desafios ao propor cooperação entre a academia e a indústria de telecomunicações, enquanto a atribuição de identidades de software e o suporte a algoritmos pós-quânticos reforçam a segurança dos sistemas e aplicativos. Além disso, a implementação de um modelo de confiança para credenciais verificáveis busca promover a confiabilidade das identidades digitais em ambientes cada vez mais complexos e dinâmicos [26].

Já no terceiro horizonte, as tendências se voltam para a exploração de novos paradigmas, como a identidade baseada em consentimento. Nesse cenário, os usuários terão maior controle sobre o uso de suas informações, podendo definir regras e restrições para o compartilhamento de dados. A atribuição de identidades de software baseada em SLSA (*Supply Chain Levels for Software Artifacts*) e a investigação da viabilidade de dispositivos decidirem o compartilhamento de informações representam um avanço rumo a uma gestão de identidade mais autônoma e transparente, onde a privacidade e a segurança dos dados dos usuários são prioridades [26].

O GIdLab pode ainda ser utilizado para realizar pesquisas experimentais de avaliação de desempenho e escalabilidade dos serviços que utilizam protocolos de autenticação e autorização (SAML, OIDC, etc.), visando otimizar e garantir eficiência operacional. Também pode realizar experimentos com identidade descentralizada, utilizando protocolos como OAuth 2.0 e OIDC para explorar soluções que reforcem a privacidade e a segurança na gestão de identidades.

6 CONCLUSÃO

O GIdLab surgiu de uma necessidade da comunidade de pesquisadores brasileiros para apoiar suas pesquisas, cujos resultados possam ser usados nos serviços da RNP e em universidades. Sendo assim, a escolha inicial dos serviços oferecidos no GIdLab estavam fortemente ligados com os serviços oferecidos na RNP. Em um segundo momento do projeto, novas tecnologias e federações foram disponibilizadas e, atualmente, o esforço está em integrar diversas federações, adequá-las a diferentes contextos de pesquisa e avançar para o conceito de identidade descentralizada.

O amplo uso da CAFe Expresso como um ambiente de experimentação evidenciou a importância de um ambiente como este para o auxílio e o fomento de pesquisas na área de gestão de identidades federadas. A disponibilização de máquinas virtuais pré-configuradas e containers Dockers prontos para o uso, permitiram que os pesquisadores acelerassem a execução de seus experimentos.

Como trabalhos futuros, pretende-se disponibilizar aos pesquisadores um novo serviço de monitoramento da infraestrutura com novas funcionalidades e desenvolver uma aplicação para configuração de experimentos baseada em containers. Outra intenção da equipe técnica é ampliar o atendimento de projetos de experimentos, incluindo projetos internacionais.

Por fim, sugere-se ainda, o desenvolvimento de objetos de aprendizagens que usem as federações para promover o ensino de conceitos, técnicas e tecnologias envolvidos com GId.

AGRADECIMENTOS

Os autores agradecem o apoio financeiro e as bolsas concedidas pela Rede Nacional de Ensino e e Pesquisa (RNP).

REFERÊNCIAS

[1] ITU. Ngn identity management framework. Recommendation Y.2720, ITU, 2009.
[2] Emerson Ribeiro de Mello, Shirlei Aparecida de Chaves, Carlos Da Silva, Michelle Silva Wangham, Andrey Brito, and Marco Aurélio Amaral Henriques Henriques. Autenticação e autorização: antigas demandas, no-vos desafios e tecnologias emergentes. 2022.
[3] IBM. IBM X-Force Threat Intelligence Index 2024. https://www.ibm.com/reports/threat-intelligence, 2024.
[4] M. S. Wangham, E. R. Mello, M. C. Souza, and H. Coelho. GidLab: Laboratório de experimentação em Gestão de Identidades. In *Workshop de Gestão de Identidades Digitais (WGID) do SBSeg 2013*, pages 481–486, Porto Alegre, 2013. SBC.
[5] Fabio Farina, Peter Szegedi, and Jerry Sobieski. GÉant world testbed facility: Federated and distributed testbeds as a service facility of gÉant. In *2014 26th International Teletraffic Congress (ITC)*, pages 1–6, 2014.
[6] Edelberto F. Silva, Natalia C. Fernandes, Noemi Rodriguez, and Débora C. Muchaluat-Saade. Credential translations in future internet testbeds federation. In *2014 IEEE Network Operations and Management Symposium (NOMS)*, pages 1–6, 2014.
[7] David W. Chadwick, Kristy Siu, Craig Lee, Yann Fouillat, and Damien Germonville. Adding federated identity management to openstack. *Journal of Grid Computing*, 12(1):3–27, 2013.
[8] Bernardo Santos, Van Thuan Do, Boning Feng, and Thanh van Do. Identity federation for cellular internet of things. In *Proceedings of the 2018 7th International Conference on Software and Computer Applications*, ICSCA '18, page 223–228, New York, NY, USA, 2018. Association for Computing Machinery.
[9] Rapid connect. https://manager.aaf.edu.au/rapid_connect/.
[10] Joshua Hill. An analysis of the radius authentication protocol, 2001.
[11] Dick Hardt. The oauth 2.0 authorization framework. Technical report, 2012.
[12] Natsuhiko Sakimura, John Bradley, Mike Jones, Breno De Medeiros, and Chuck Mortimore. Openid connect core 1.0. *The OpenID Foundation*, page S3, 2014.
[13] John Hughes and Eve Maler. Security assertion markup language (saml) v2. 0 technical overview. *OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08*, 13:12, 2005.
[14] Michelle S Wangham, Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios, and Joni da Silva Fraga. Gerenciamento de identidades federadas. In *Minicurso – SBSeg 2010*, 2010.
[15] Emerson Ribeiro de Mello, Shirlei Aparecida de Chaves, Carlos Eduardo da Silva, Michelle Silva Wangham, Andrey Brito, and Marco Aurélio Amaral Henriques. Autenticação e autorização: antigas demandas, novos desafios e tecnologias emergentes. In *Minicursos do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. 2022.
[16] Felipe Cardoso, Allex Andrade, Emerson Mello, Carolina Felicissimo, and Michelle Wangham. Como ofertar aplicações web python como um provedor de serviço shibboleth usando microsserviços. In *Anais Estendidos do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 88–95, Porto Alegre, RS, Brasil, 2020. SBC.
[17] The Commons Conservancy. Simplesamlphp. https://simplesamlphp.org/, 2023. Acessado em: 2 de agosto de 2023.
[18] Leif Johansson. The identity selector software (thiss.io). https://thiss.io/, 2019. Acessado em: 8 de agosto de 2023.
[19] Leif Johansson. *pyFF Documentation*, 2012. Release 2.0.0.
[20] Allex Magno Andrade, Jucélio Jair Silva, Edelberto F Silva, Luciano F da Rocha, and Michelle Wangham. Pesquisas exploratórias no testbed eduroam do gidlab. In *Anais Estendidos do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 126–129. SBC, 2018.
[21] Angelo Furfaro and Giuseppe De Marco. Mixing heterogeneous authentication and authorization infrastructures through proxies. In *ICEIS (1)*, pages 124–131, 2020.
[22] Maykon Chagas de Souza. Um mecanismo de controle e gerência de segurança para ambientes de e-science. Master's thesis, Universidade do Vale do Itajaí, Itajaí, SC, Brasil, Julho 2016. Dissertação de Mestrado, Programa de Mestrado Acadêmico em Computação Aplicada, Orientadora: Michelle Silva Wangham, Dra.
[23] Marcos Allende López. Self-sovereign identity: The future of identity: Self-sovereignity, digital wallets, and blockchain. 2020.
[24] E. C., Ismael Ávila, Jeffson Celeiro, Fiterlinge Sousa, and Michelle Wangham. Relato de experiência do processo de implantação do testbed para gestão de identidades digitais descentralizadas. In *Anais do II Workshop de Testbeds*, pages 25–37, Porto Alegre, RS, Brasil, 2023. SBC.
[25] Hyperledger Foundation. Indy, Oct 2023.
[26] Emerson Mello, Andrey Brito, Antônio Gomes, Frederico Schardong, Marco Henriques, Michelle Wangham, Shirlei Chaves, and Edelberto Silva. Relatóriode visãode futuro, 5 2023.