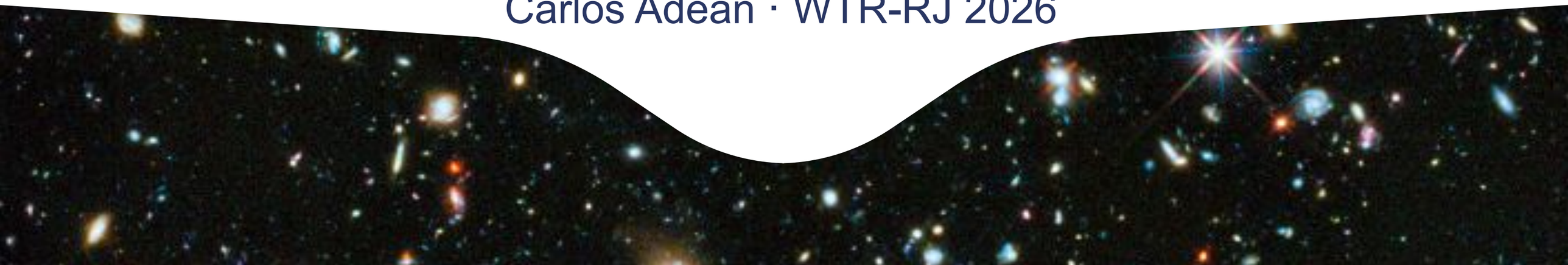
LIneA

Laboratório Interinstitucional de e-Astronomia

Maturidade de Segurança nas ICTs - Caso de Uso do LIneA

Gestão de Acesso Federado e a Adoção do Framework SIRTFI

Carlos Adean · WTR-RJ 2026



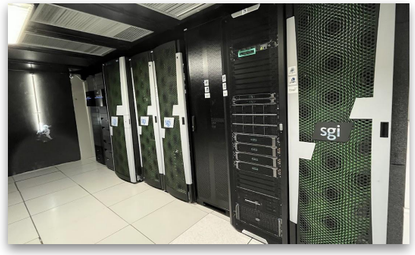
Agenda

1. **Contexto e motivação:** o LIneA, o ambiente multi-colaboração e os requisitos do Rubin Observatory.
2. **Gestão de identidades e confiança federada:** a evolução do acesso federado e a adoção do SIRTFI.
3. **Construção da segurança no LIneA:** governança, apoio institucional e evolução dos controles.
4. **Experiências e aprendizados:** resposta a incidentes, resultados, lacunas e lições aprendidas

Múltiplas colaborações

SDSS DES DESI TON LSST

LIneA





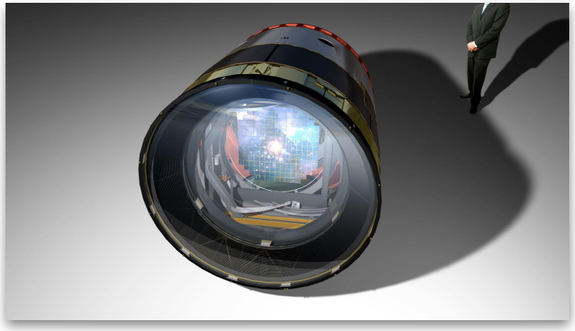


Rubin Observatory - LSST

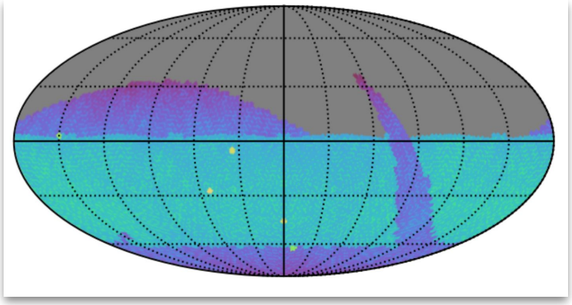






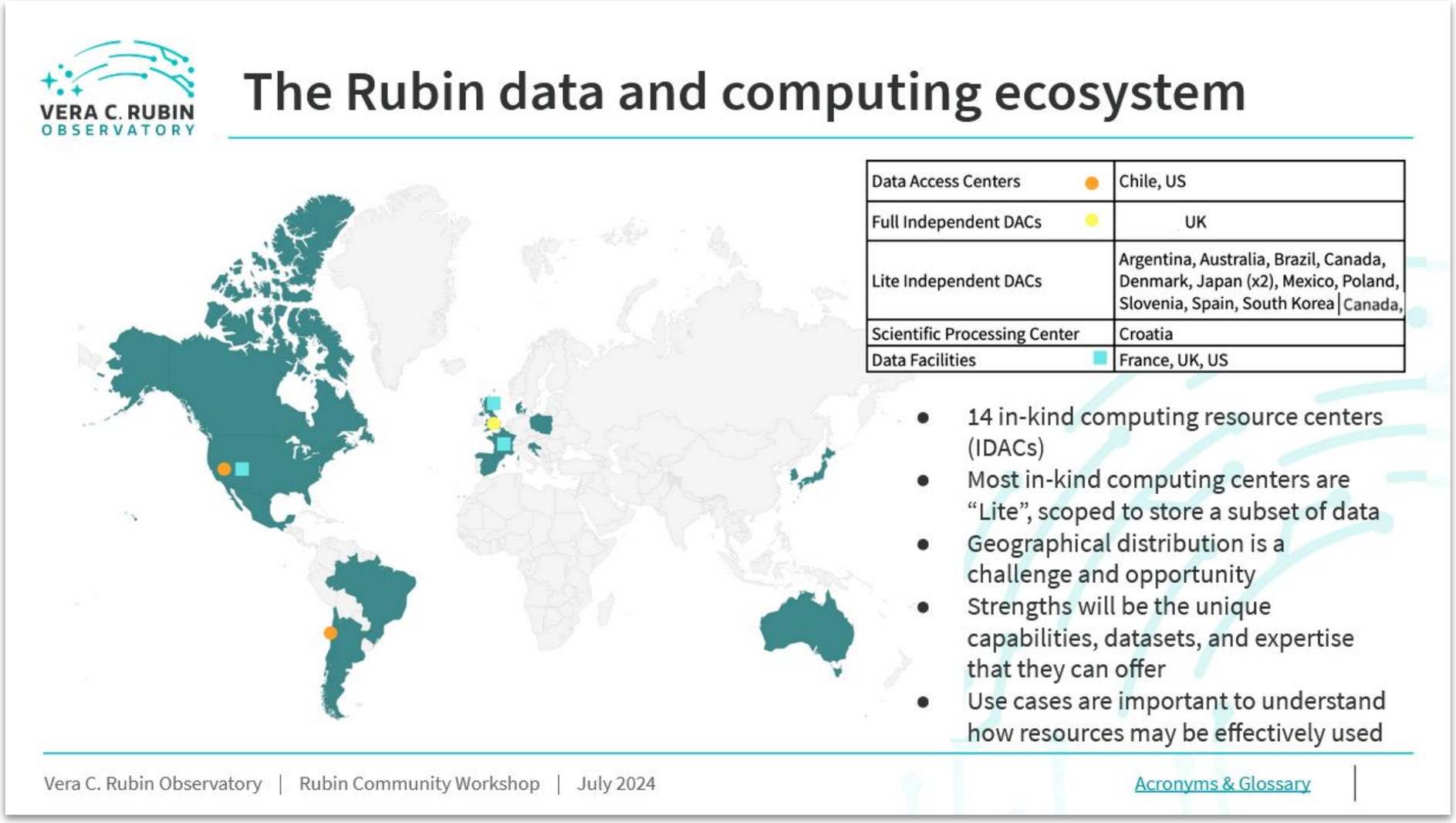


LSSTCam
3.2 Gigapixels



Independent Data Access Center Brazil - IDAC-BR

IDAC BRASIL
LSST



https://www.lsst.org/scientists/in-kind-program/computing-resources

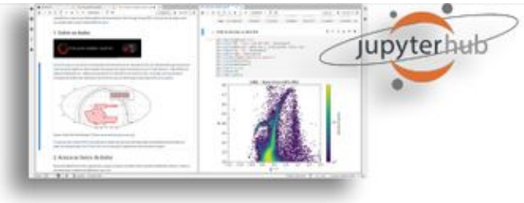
créditos slide: Knut Olsen - LSST RCW 2024

LIneA Science Platform - Ecossistema do IDAC-BR



User Query Tool

SQL/ADQL/MyDB/TAP Service



JupyterHub over K8S



Occultation Prediction Database

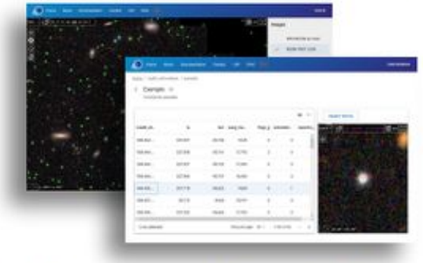
com serviço de subscrição



PZ Server

LSST members only

in-kind cont.



Sky Viewer and Target Viewer

Image visualization and catalog overlay

IDAC BRASIL

LSST



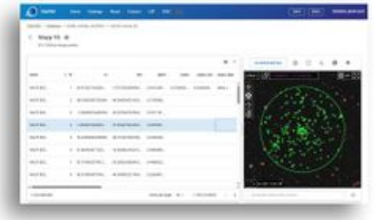
Cutout Service (Int)



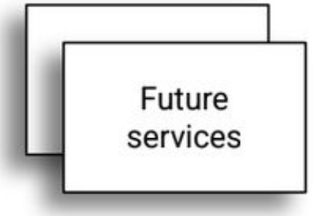
interactive app JupyterLab over HPC



LSDB @LIneA



Canvas (Int)



VAC OnDemand, X-matching

Em desenvolvimento

scienceplatform.linea.org.br

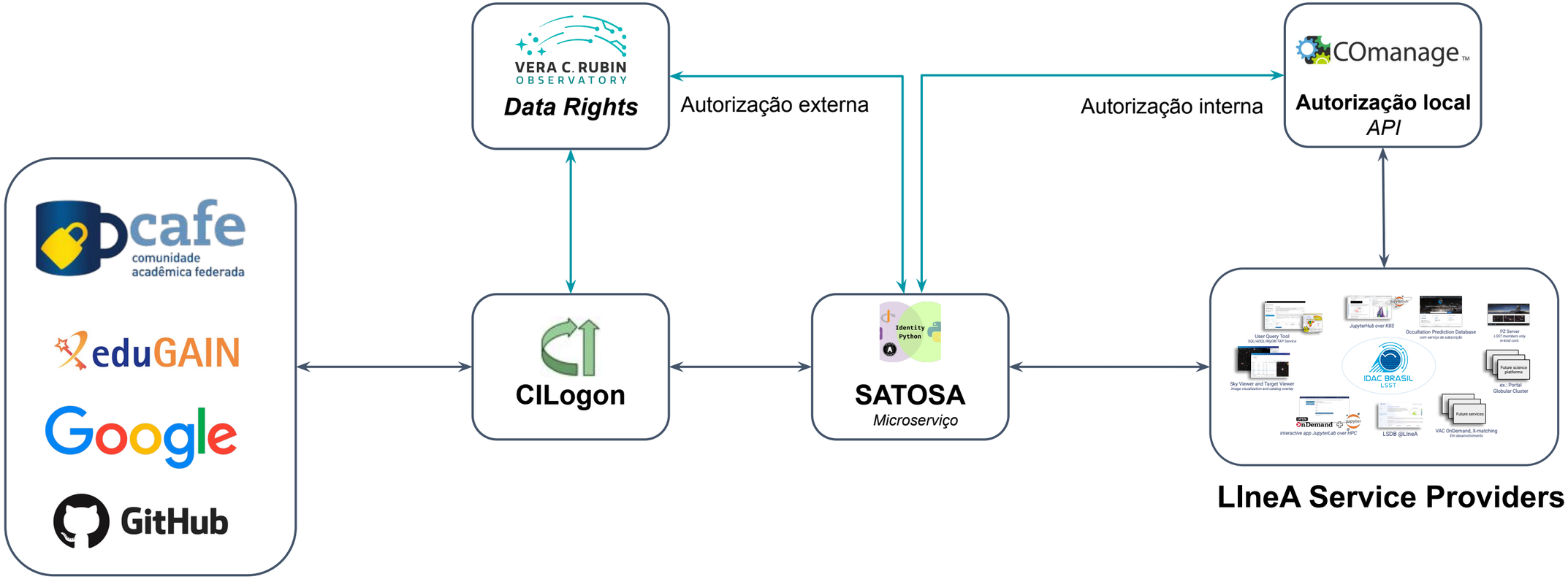
Requisitos Técnicos e Institucionais

Sistema de autenticação e autorização alinhados com o Rubin Observatory Access System

1. Todos os membros da colaboração devem poder autenticar-se em qualquer IDAC.
2. O acesso aos dados deve respeitar os direitos definidos para cada membro individualmente.

Integração com o Rubin Observatory Access System

Separar quem tem Rubin Data Rights de quem não tem



Adoção do SIRTFI na adesão ao CILogon

PGSI

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

NORMAS E PADRÕES

- Norma de Gestão e Armazenamento de Logs
- Norma de Gestão de Vulnerabilidades
- Norma de Gestão de Identidades
- Política de Uso Aceitável do Provedor de Identidades

PROCEDIMENTOS E ORIENTAÇÕES

- Análise e Resolução de Incidentes de Segurança
- Aplicação de Patches de Segurança
- Atualização de Responsáveis pelo IDP
- Triagem de Incidentes de Segurança
- Armazenamento e análise de logs
- Provisionamento de contas
- Desprovisionamento de contas

SIRTFI
Security Incident Response Trust Framework for Federated Identity

EM AMARELO OS DOCUMENTOS PARA CONFORMIDADE COM O SIRTFI

Um time pequeno, orçamento limitado e apoio externo

O LIneA tem 10 pessoas, das quais 8 integram as equipes de desenvolvimento e infraestrutura, além de enfrentar limitações orçamentárias.

Dois apoios importantes ao longo dessa jornada

- **GidLab - desde 2019**
  - Apoio na evolução da gestão de identidades e acessos.
  - + 30 reuniões
- **CAIS/RNP - desde 2021**
  - Modelos, orientação sobre o escopo necessário para o SIRTFI, revisão dos documentos, avaliação de riscos
  - +30 reuniões

SIRTFI

Security Incident Response Trust Framework for Federated Identity

Evolução da governança de segurança

1. **2021 - Estruturação inicial**

   Política geral, quatro normas auxiliares e procedimentos operacionais
2. **2023 - 1a Revisão da PGSI**

   Primeira revisão da política geral
3. **Abril de 2024 - Proteção de dados**

   Política de cópia de segurança, com referências à ISO 27001 e 27002.
4. **Outubro de 2025 - Uso do HPC**

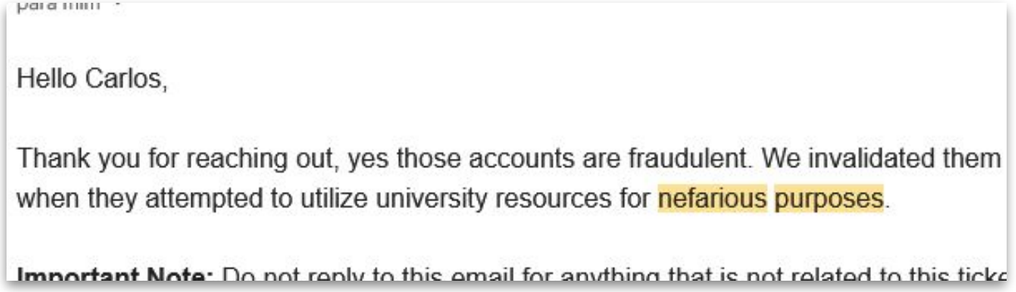
   Norma específica de utilização do ambiente de HPC
5. **Abril de 2026 - 2a Revisão da PGSI e Atualização da Norma de Gestão de Identidades**

   Atualização da norma de gestão de identidades, contemplando provedores externos.

Um caso real: uso indevido de recursos

Da identificação ao tratamento

- Três solicitações de registro utilizando identidades institucionais externas.
- Utilização de uma das contas para mineração de criptomoedas.
- Detecção pelo monitoramento e início dos procedimentos internos.
- Contato com a instituição de origem, que confirmou a natureza fraudulenta das contas.



Hello Carlos,

Thank you for reaching out, yes those accounts are fraudulent. We invalidated them when they attempted to utilize university resources for nefarious purposes.

Confirmação da natureza fraudulenta das contas pela instituição de origem.

Resultados e lacunas

O que avançou

- Política Geral de Segurança da Informação.
- Normas específicas e procedimentos operacionais.
- Comitê Gestor de Segurança.
- Autodeclaração SIRTFI registrada na CAFe.
- Procedimentos utilizados na resposta a incidentes.
- Revisão e ampliação contínua da documentação.

O que ainda precisamos melhorar

- Plano de continuidade e recuperação dos serviços.
- Gestão de dependências e riscos dos serviços.
- Maior disseminação das responsabilidades de segurança.

Lições aprendidas

1) **Comece:** não esperar ter todos os recursos ou uma estrutura perfeita.
2) **Estabeleça prioridades:** implementar aquilo que a instituição consegue sustentar.
3) **Busque apoio:** aproveitar a experiência de instituições e grupos que já percorreram esse caminho.
4) **Trabalhe a cultura:** tecnologia e documentação são importantes, mas a mudança de mentalidade é o maior desafio.

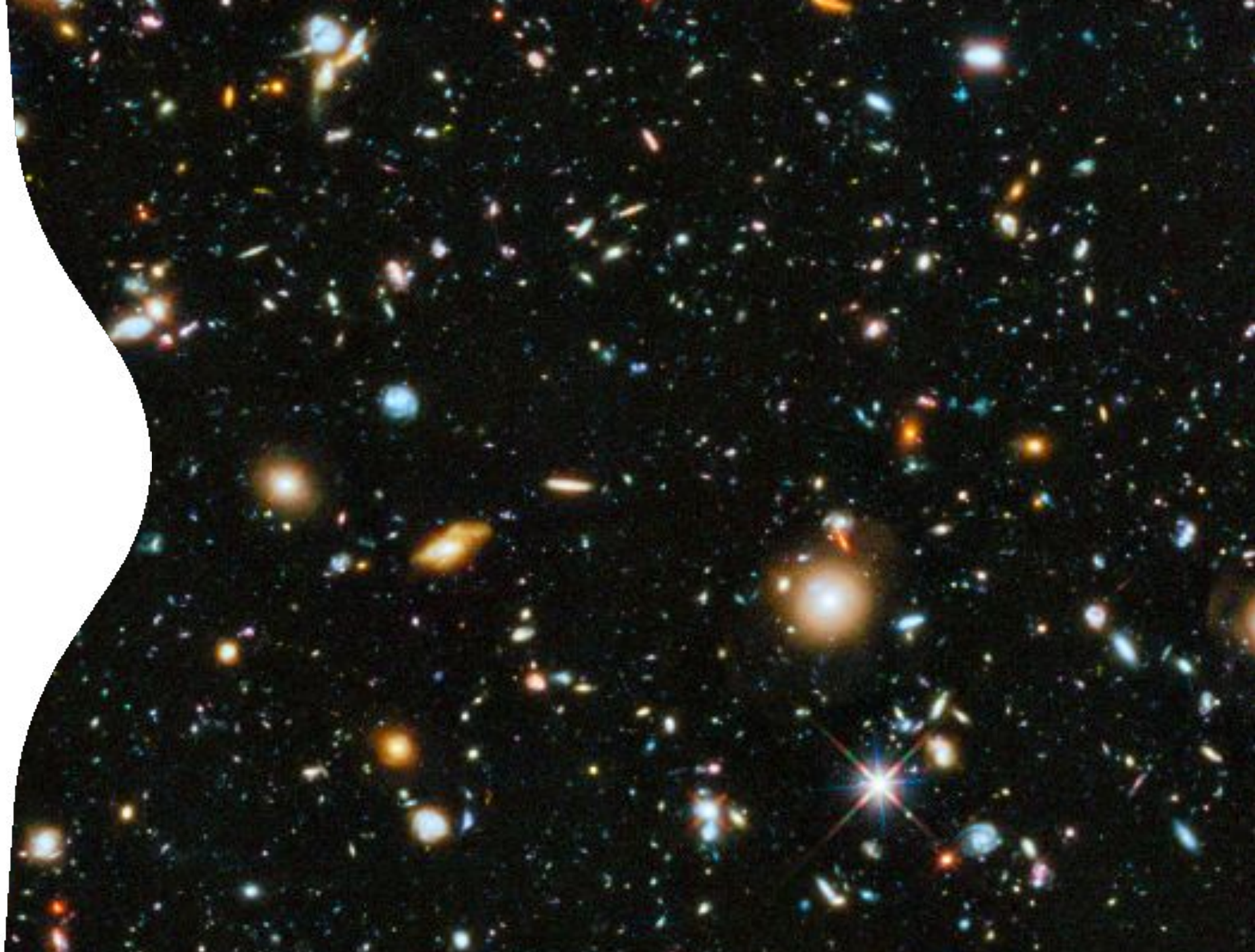
Sugestão à RNP: simulação da aplicação do framework SIRTFI envolvendo instituições clientes da RNP (sugestão inspirada no SIRTFI Exercise Working Group).



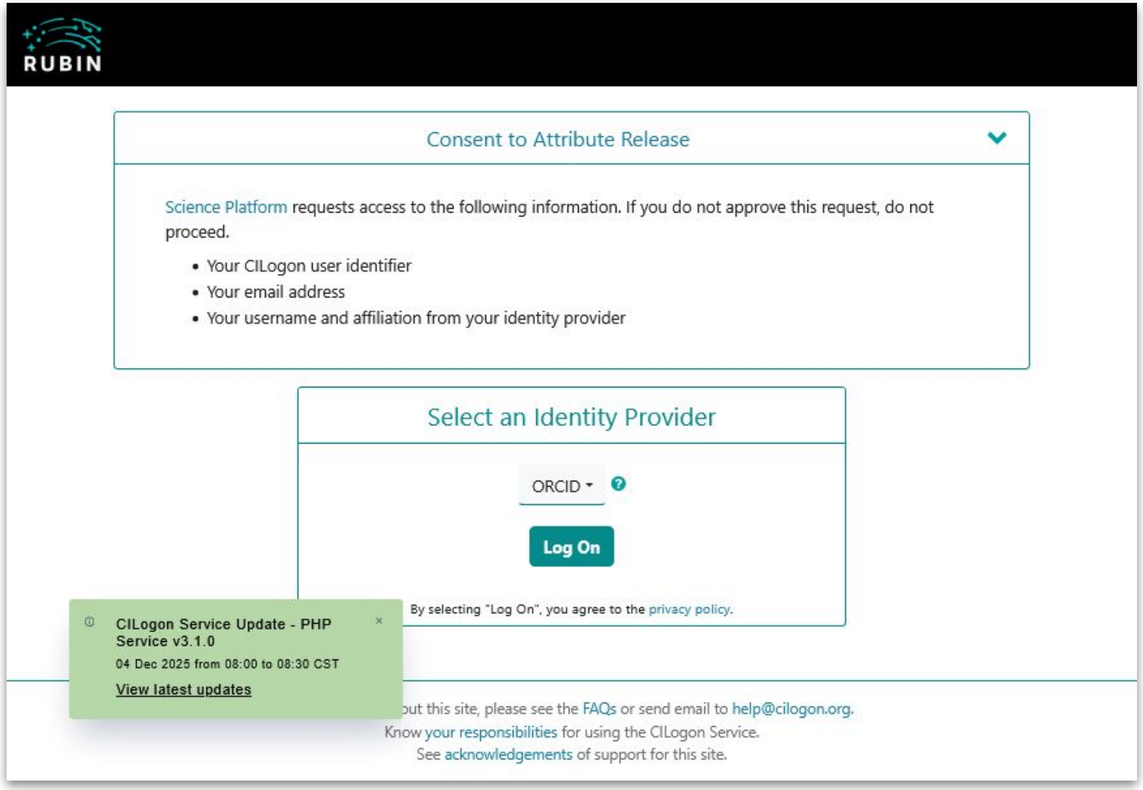
Obrigado!

carlosadean@linea.org.br

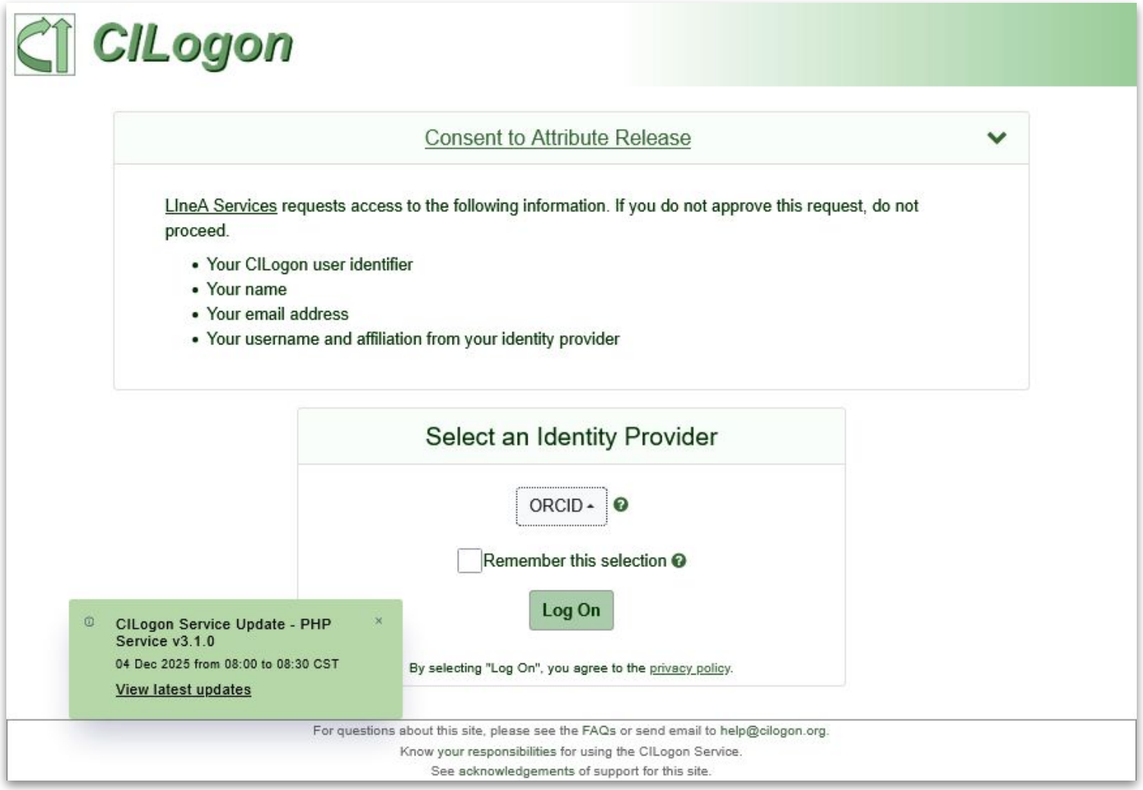
Extras



Telas do CILogon - Perfil Rubin e Público Geral



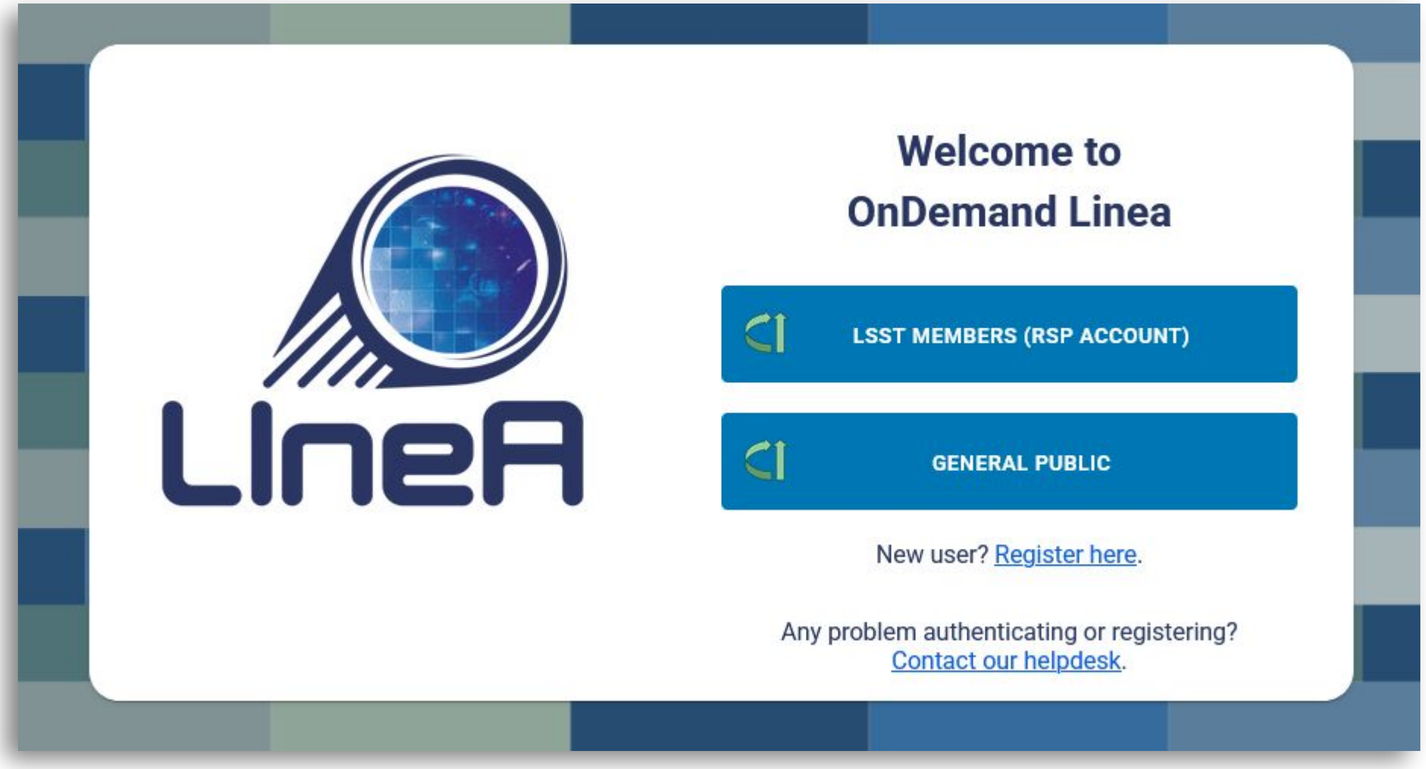
Versão customizada para o Rubin Access System



Versão padrão no plano Basic Authentication do LIneA

Exemplo de tela de login nas plataformas do IDAC-BR

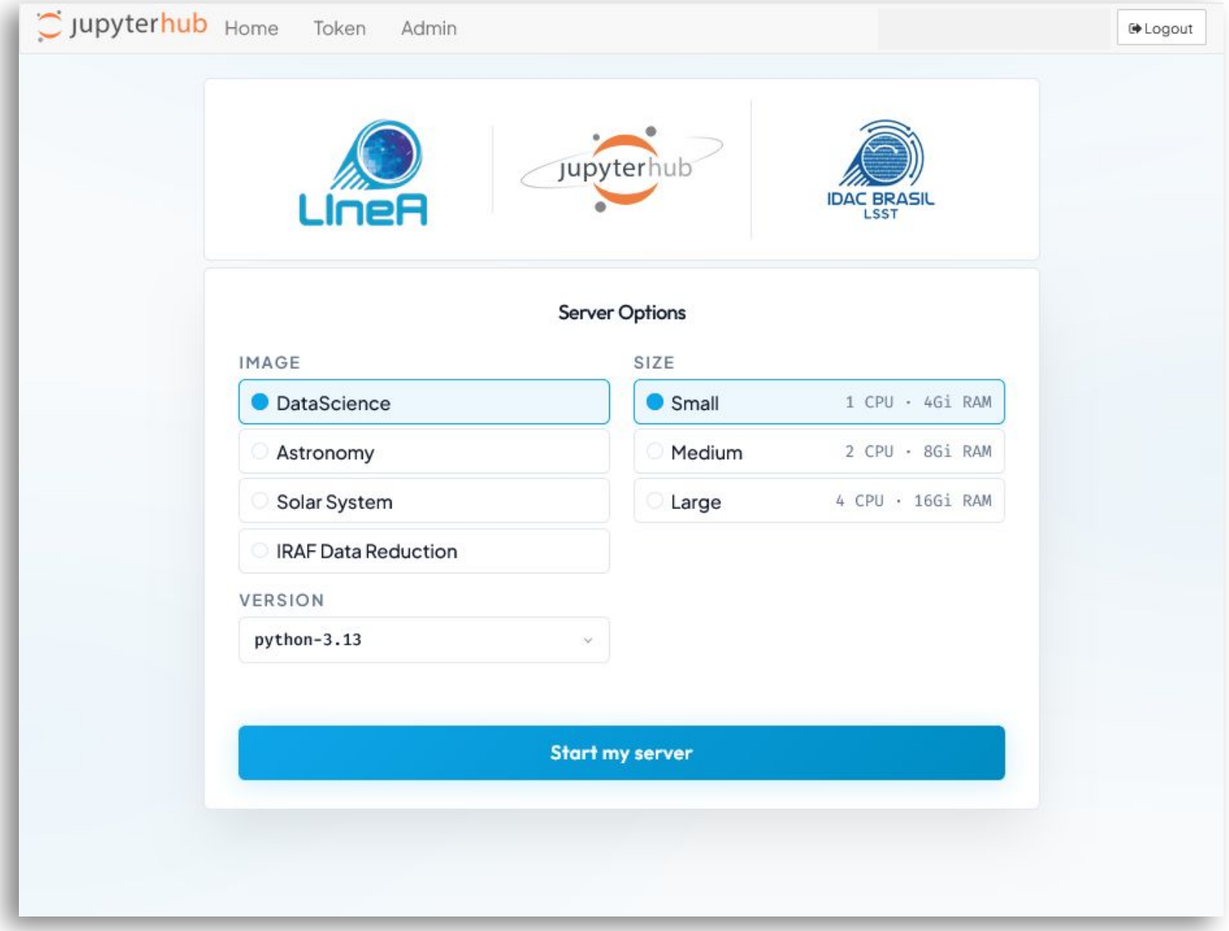
A&A com CILogon e Rubin Auth. API



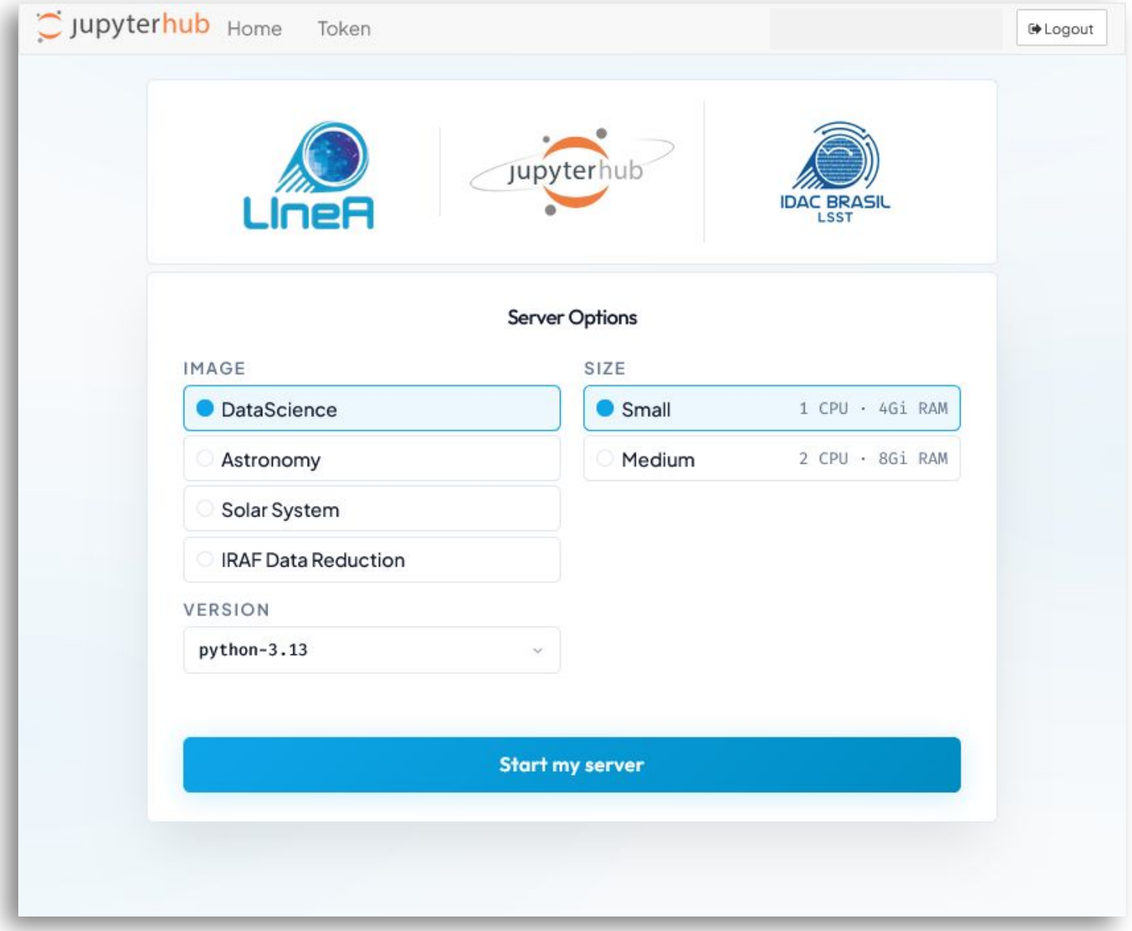
Como a aplicação se comporta para o usuário

Jupyter Hub

https://scienceplatform.linea.org.br



Perfil Colaboração

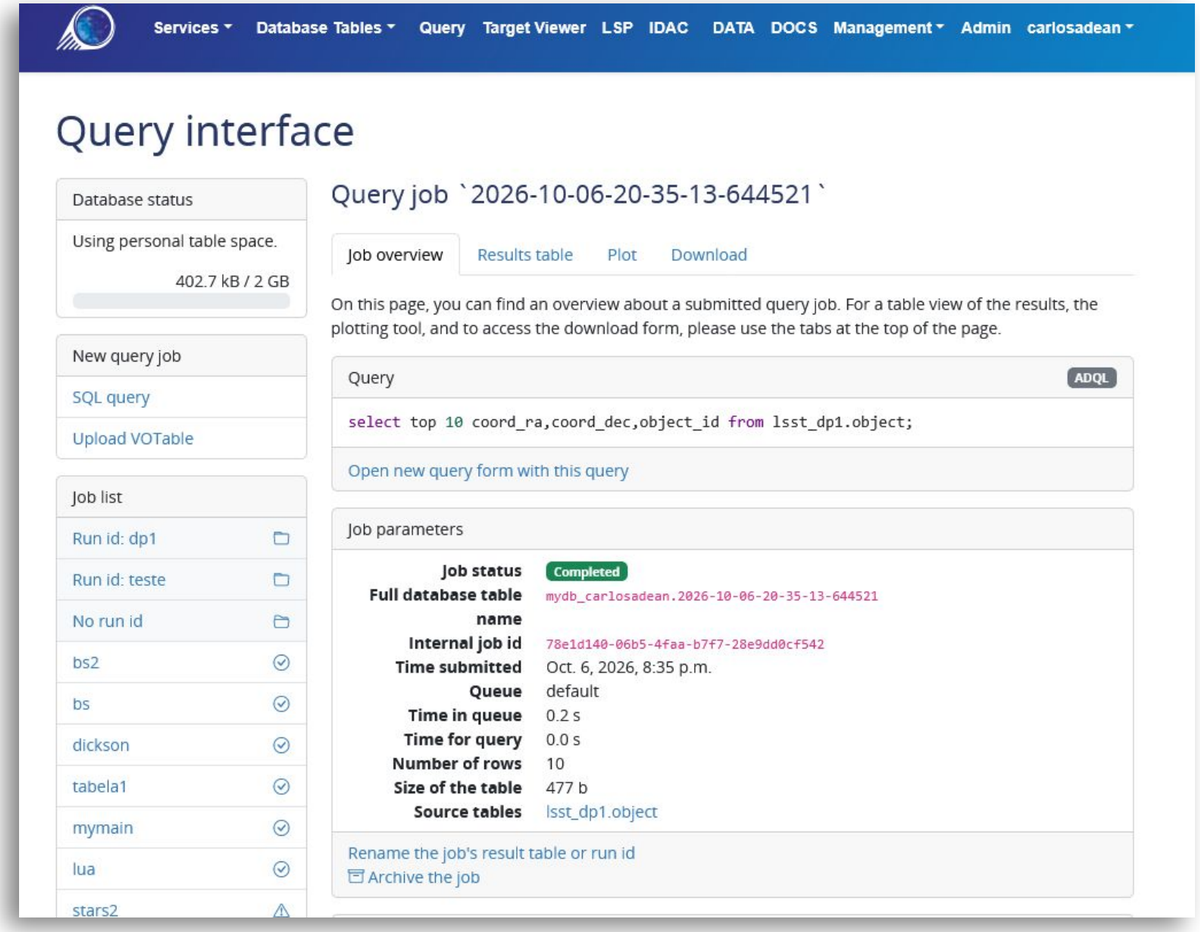


Perfil Público

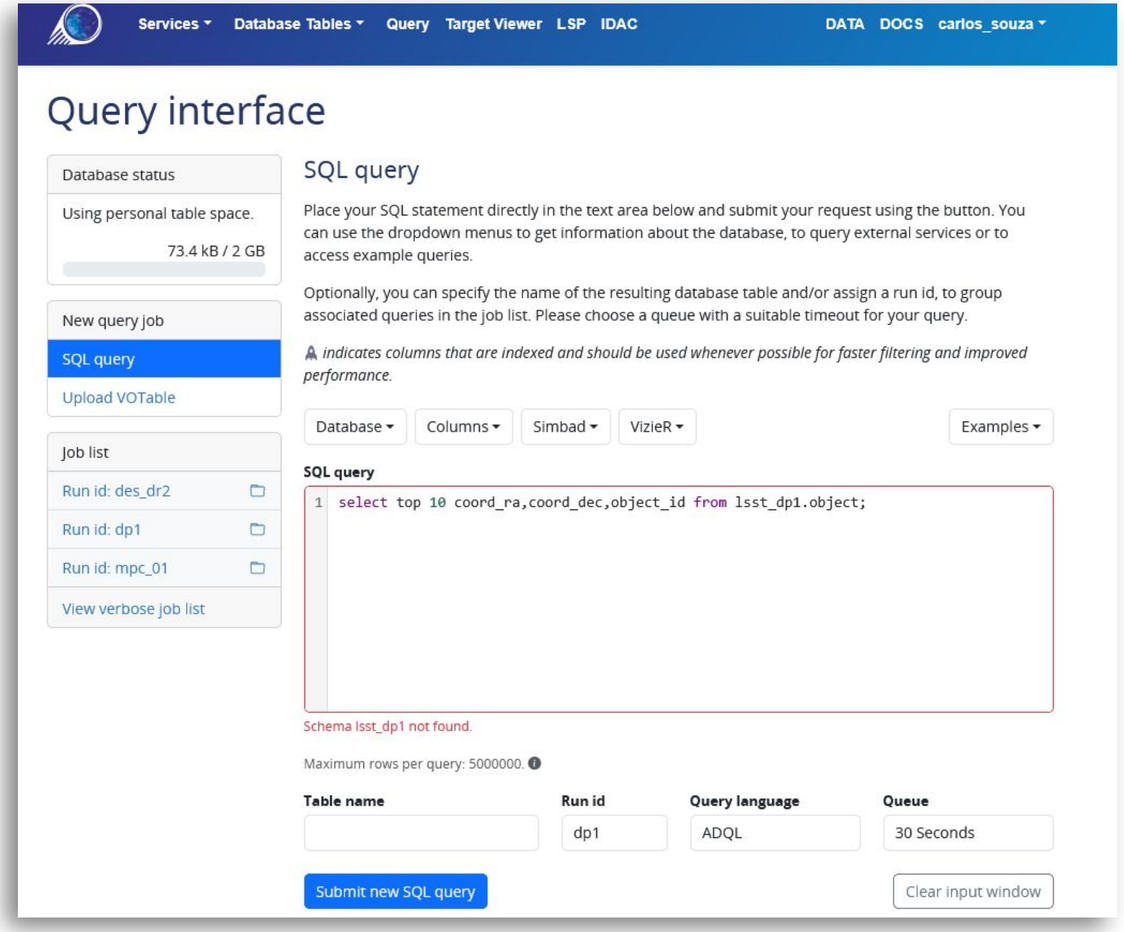
Como a aplicação se comporta para o usuário

User Query

https://scienceplatform.linea.org.br



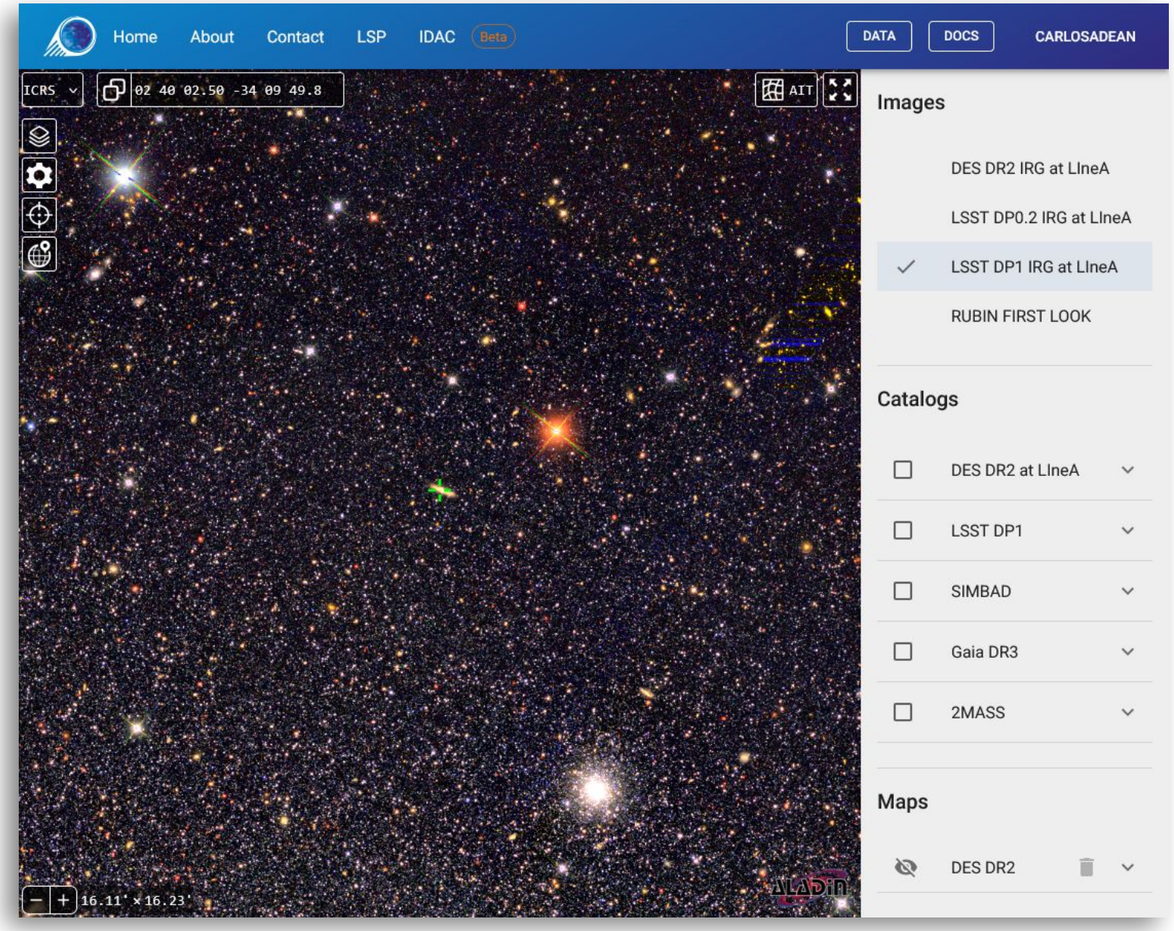
Perfil Colaboração



Perfil Público

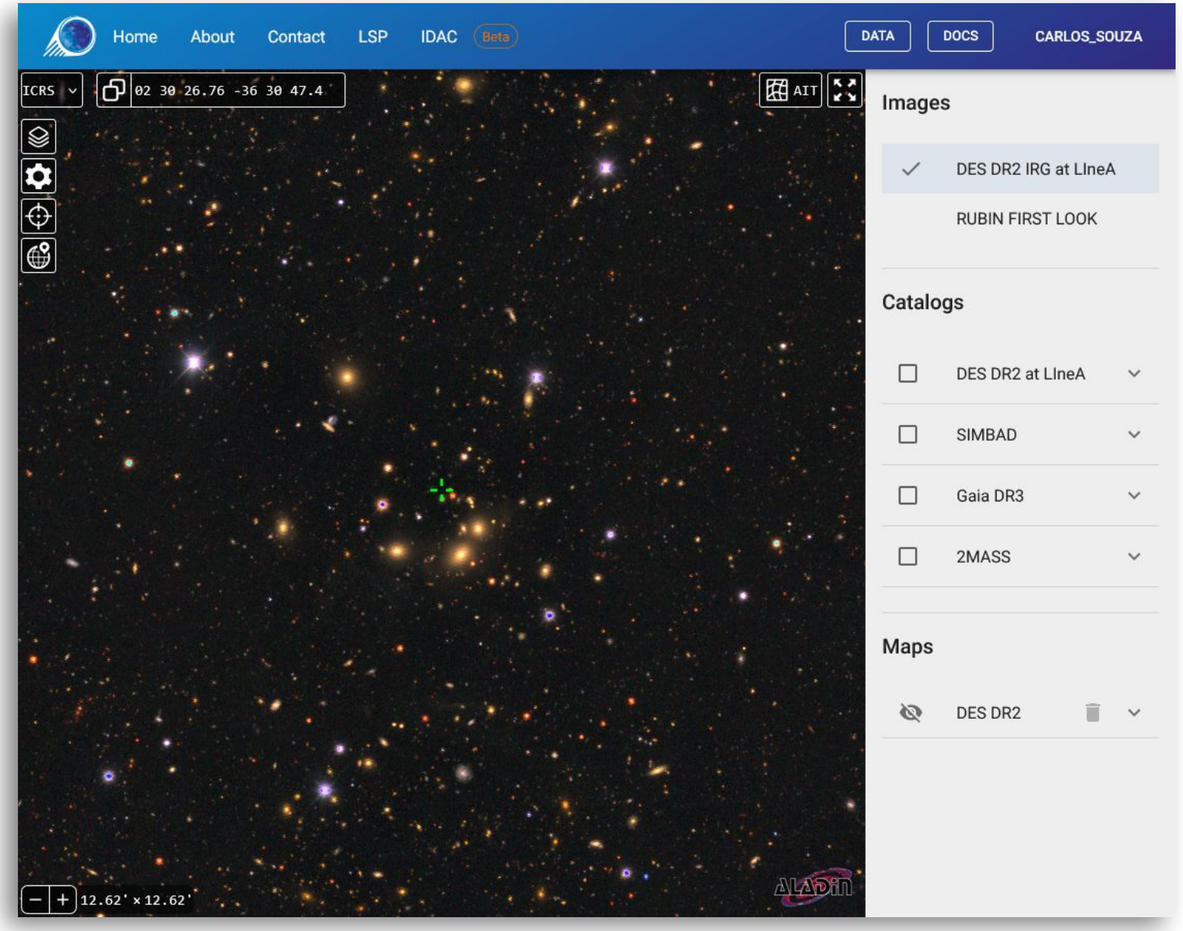
Como a aplicação se comporta para o usuário

Sky Viewer



Perfil Colaboração

https://scienceplatform.linea.org.br



Perfil Público

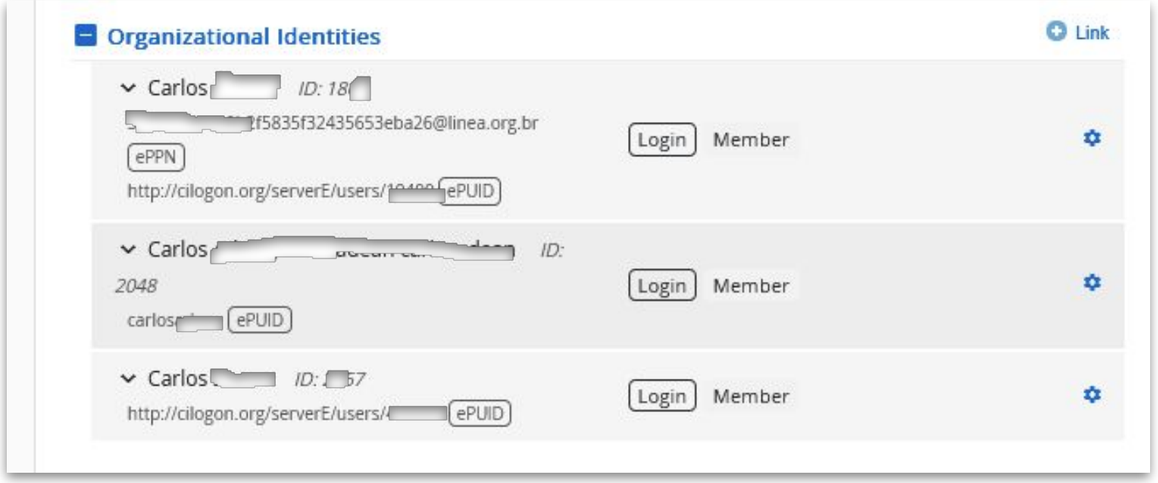
Exemplo de Identidades Organizacional no COmanage

Atualização de atributos necessária após a adoção do CILogon.

Múltiplas identidades organizacionais linkadas a mesma conta de um usuário.

Isso também permite que um usuário utilize mais de uma credencial para acessar a sua conta no ambiente.

Muito útil para pesquisadores que mudam de instituição e não querem perder o acesso aos seus dados.



SIRTFI, governança e compromissos de segurança

- Referências de governança
  - A política utiliza propósito, papéis, controle de versões, revisão e conceitos de risco, ativo e incidente da família ISO/IEC 27000.
  - A ISO 27001 e a ISO 27002, edição 2013, são citadas na política de cópia de segurança.
- Compromissos assumidos com o SIRTFI
  - Entre entidades declaradas no Sirtfi: responder, avisar quem estiver envolvido, colaborar e usar o Traffic Light Protocol.
- Registro da autodeclaração na CAFe
  - A CAFe estabelece requisitos de contato de segurança e cooperação em incidentes para IdPs e SPs.
  - Algumas integrações do CILogon exigem a tag https://refeds.org/sirtfi nos metadados do IdP.
  - A autodeclaração do LIneA foi registrada na CAFe. Não houve certificadora externa.