MENTORED *Testbed*: Pesquisa Experimental em Cibersegurança

Apresentadores:

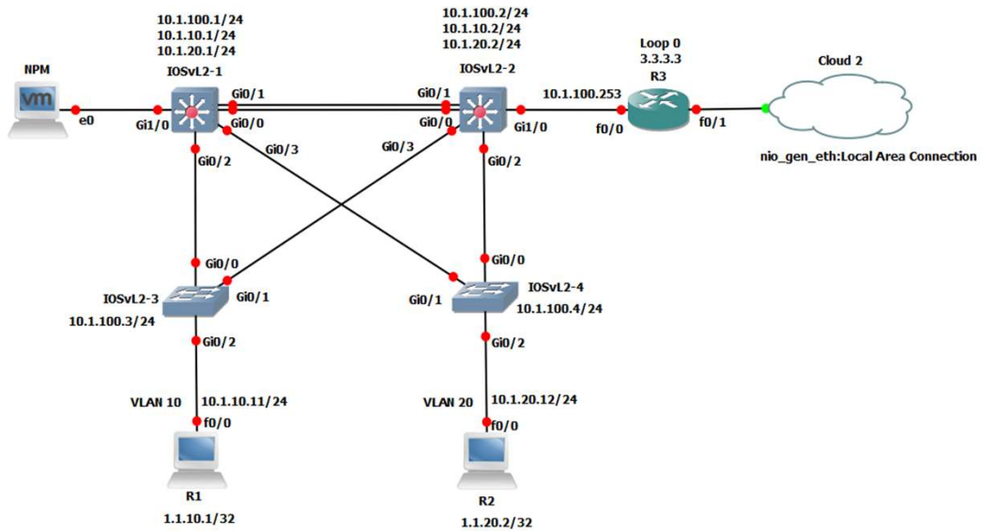
- **Michelle S. Wangham, UNIVALI/RNP**
- **Davi Gemmer, RNP**

Introdução

- Ataques cibernéticos continuam entre os maiores riscos globais (*World Economic Forum* 2024)
  - infraestrutura crítica, redes de telefonia, IoT, plataformas automotivas
- Desenvolvimento de soluções para prevenir, detectar e mitigar ataques requer ferramentas, ambiente e métodos para validá-las
  - Não é possível usar ambientes de produção ou mesmo replicar ambientes reais
- Diferentes tecnologias podem ser empregadas para experimentação
  - Simuladores, emuladores e *testbeds*

Ambientes de experimentação em cibersegurança

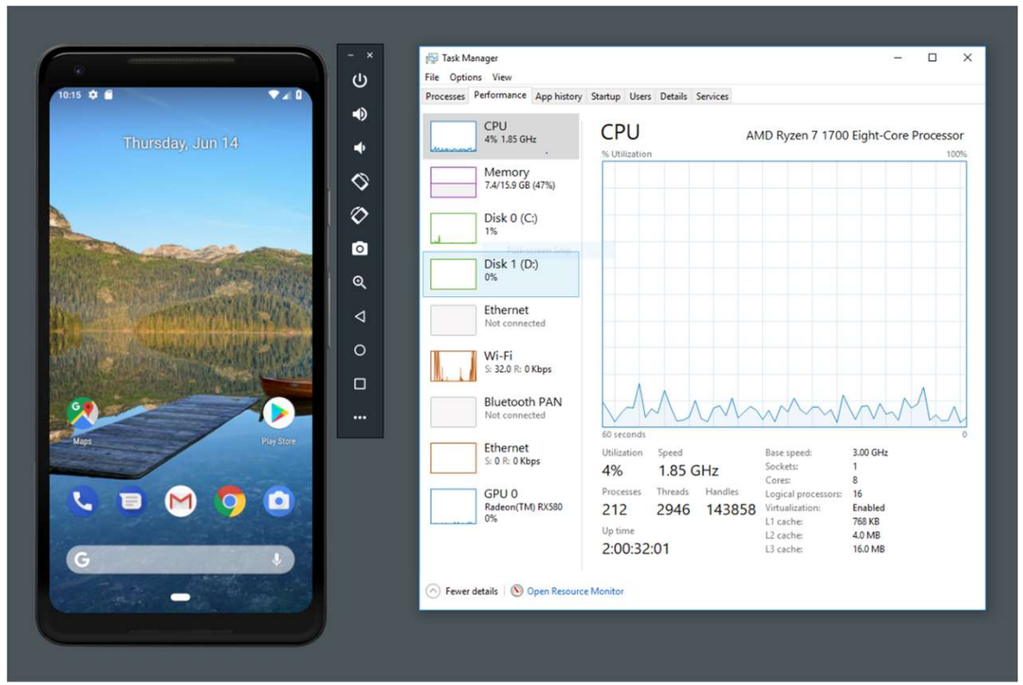
- **Simuladores**
  - Ambientes virtuais que replicam cenários reais
- **Emuladores**
  - Replicam o comportamento de software e hardware
- ***Testbeds***
  - Reproduzem uma infraestrutura de rede e sistemas de informação
  - Realismo e fidelidade



Fonte: https://gns3.com

Ambientes de experimentação em cibersegurança

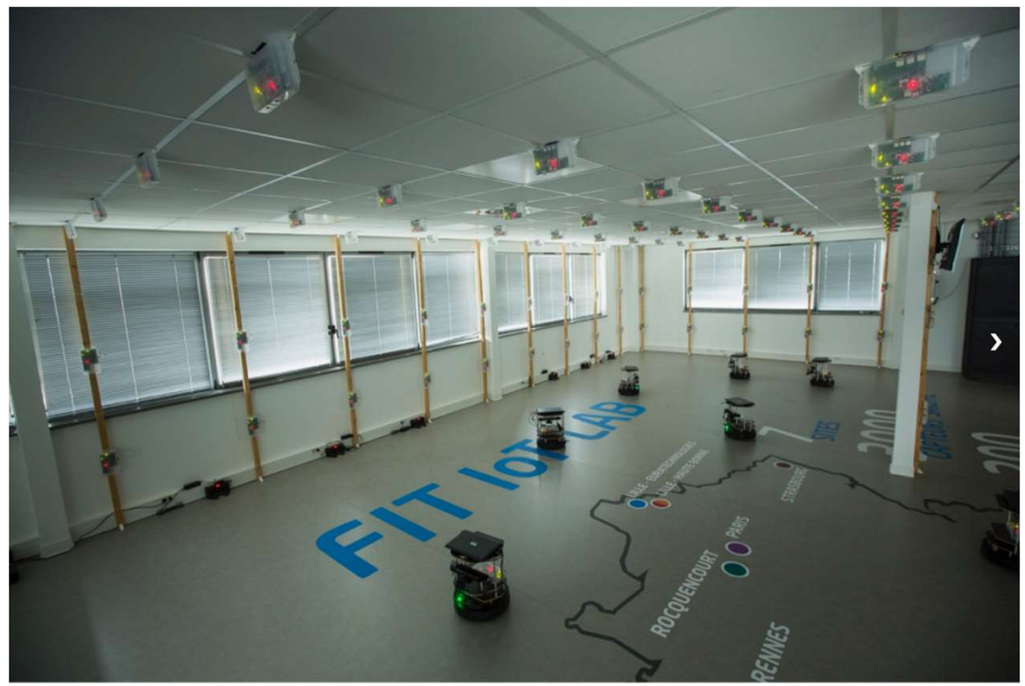
- **Simuladores**
  - Ambientes virtuais que replicam cenários reais
- **Emuladores**
  - Replicam o comportamento de software e hardware
- ***Testbeds***
  - Reproduzem uma infraestrutura de rede e sistemas de informação
  - Realismo e fidelidade



Fonte: https://developer.android.com

Ambientes de experimentação em cibersegurança

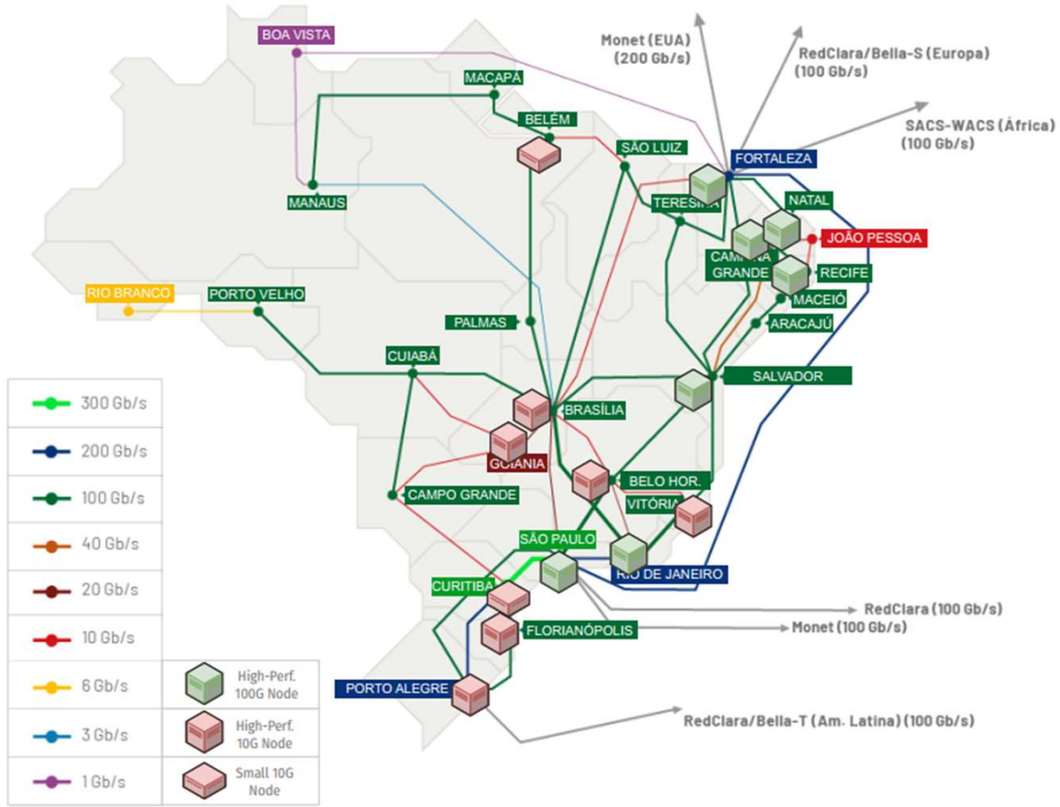
- **Simuladores**
  - Ambientes virtuais que replicam cenários reais
- **Emuladores**
  - Replicam o comportamento de software e hardware
- ***Testbeds***
  - Reproduzem uma infraestrutura de rede e sistemas de informação
  - Realismo e fidelidade



Fonte: https://www.iot-lab.info

Desafios para conduzir experimentos em cibersegurança

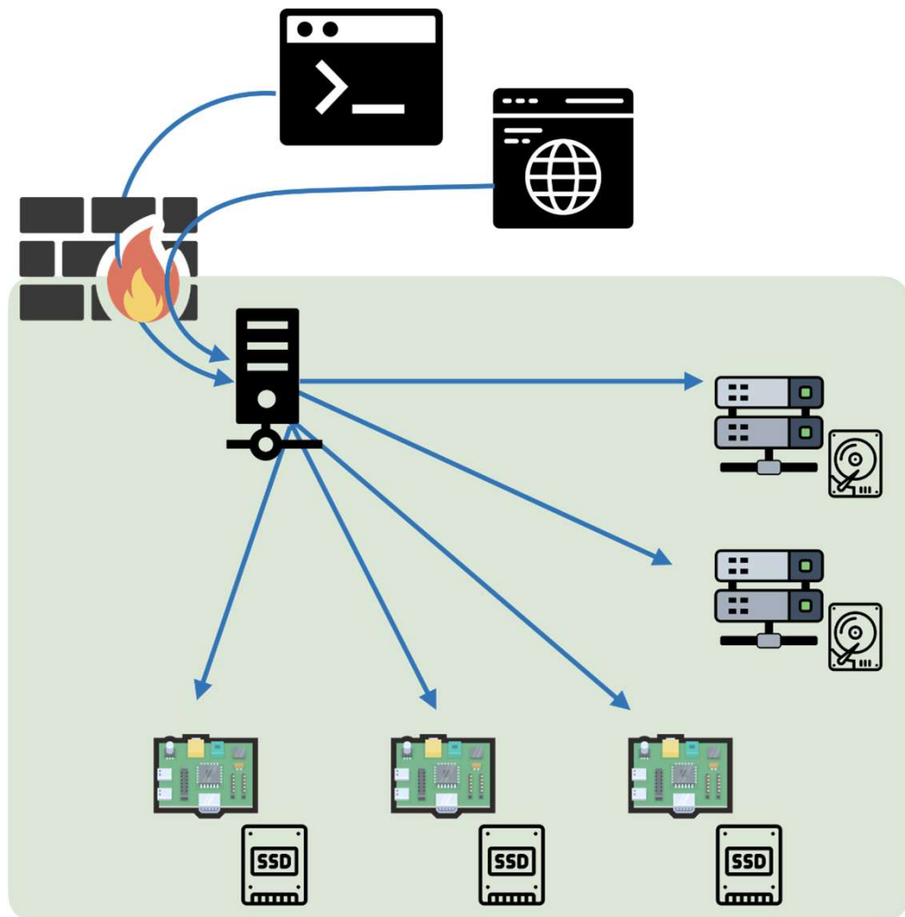
- **Gerenciamento de recursos geograficamente distribuídos**
  - Agendamento e sincronização por todos os dispositivos
- **Capacidade dos dispositivos e dos enlaces**
  - Limita o tipo de experimento ou número de experimentos em paralelo
- **Automatização e orquestração para início e término dos experimentos**
  - Reservar e liberar recursos



Fonte: RNP

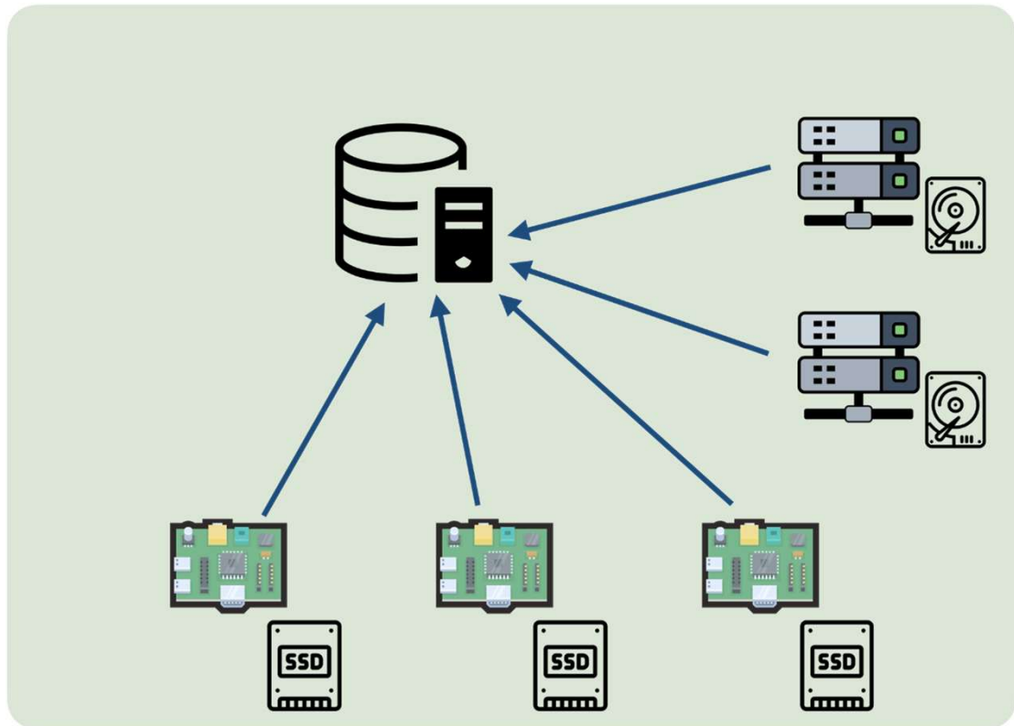
Desafios para conduzir experimentos em cibersegurança

- **Acesso em tempo real aos dispositivos durante a execução do experimento**
  - Acesso seguro e interface amigável
  - Ferramentas de monitoramento



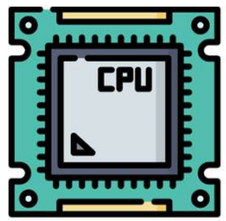
Desafios para conduzir experimentos em cibersegurança

- **Armazenamento e compartilhamento dos dados gerados no experimento**
  - Grande volume de dados
  - Tempo de retenção dos dados



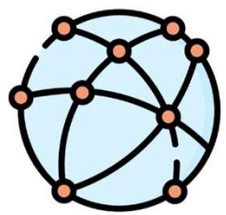
Requisitos de *testbeds* de cibersegurança

- **Fidelidade**
  - Replicar com precisão ambiente alvo do estudo
- **Flexibilidade**
  - Adaptar para diferentes cenários e experimentos



ARM
x86-64

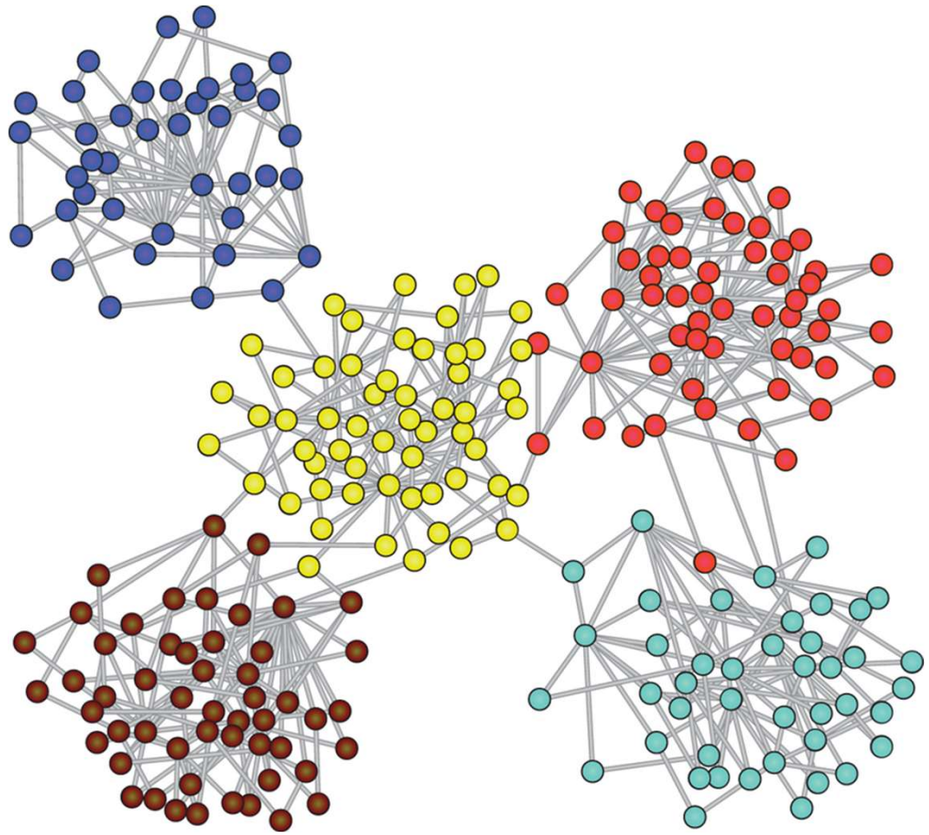
WiFi
802.15.4



Distância geográfica
Capacidade dos enlaces

Requisitos de *testbeds* de cibersegurança

- **Escalabilidade**
  - Permitir o uso de um grande número de dispositivos e geograficamente dispersos



Fonte: Wikipedia

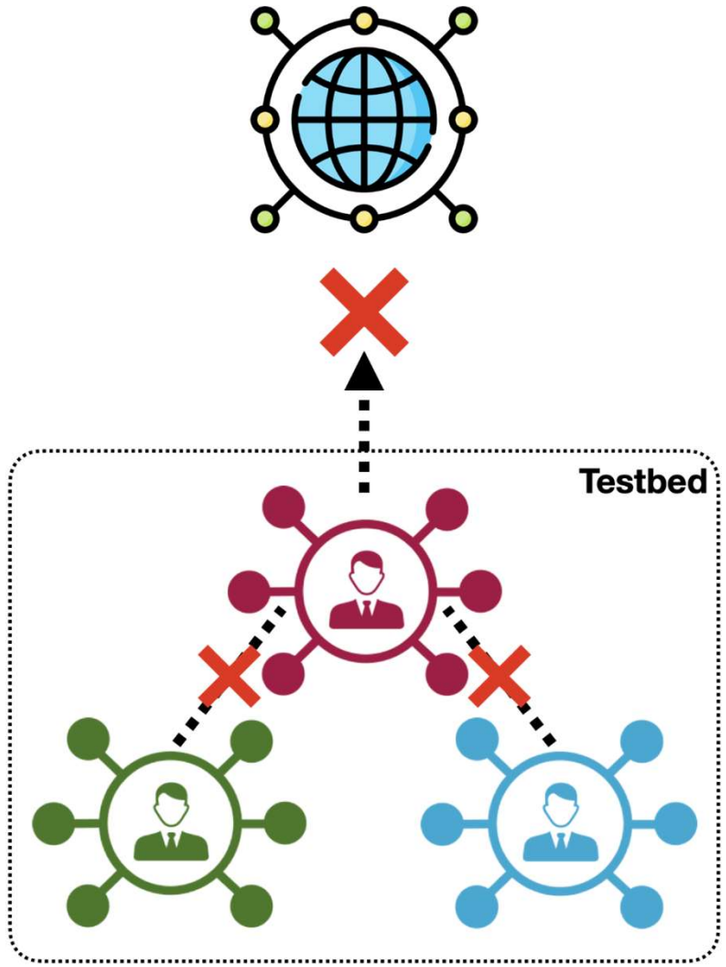
Requisitos de *testbeds* de cibersegurança

- **Reprodutibilidade**
  - Repetir experimentos e obter resultados estaticamente semelhantes

Fonte: The Turing Way project.
DOI: 10.5281/zenodo.3332807.

Requisitos de *testbeds* de cibersegurança

- **Isolamento**
  - Um experimento em execução não pode afetar outro experimento
- **Execução segura**
  - Experimentos não podem comprometer a infraestrutura do *testbed* ou vazar para Internet



MENTORED

Testbed

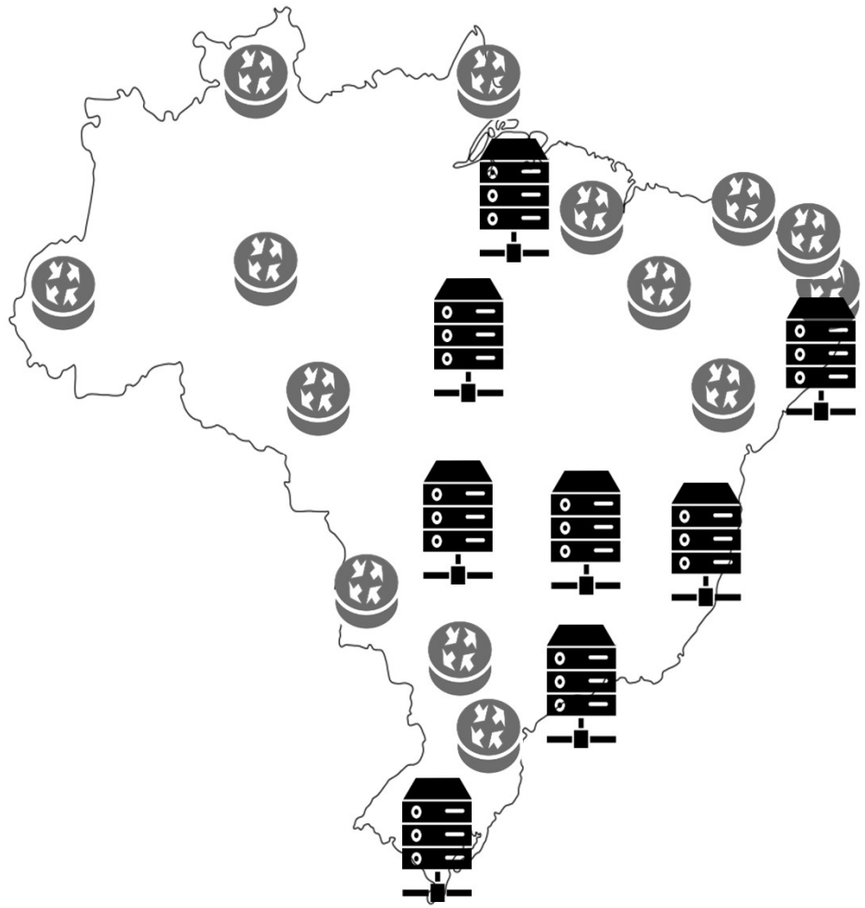
Projeto MENTORED

- Identificar, modelar e avaliar comportamentos maliciosos relacior
- Auxiliar na construção de soluções avançadas e coordenadas para possibilitar à **prevenção**, **predição**, **detecção** e **mitigação** de **ataques DDoS**;
- Fornecer a comunidade científica em Cibersegurança um ***testbed*** para permitir que pesquisadores experimentem suas soluções em relação a ataques DDoS.

FAPESP MCTIC cgi.br Comitê Gestor da Internet no Brasil

Projeto MENTORED
MENTORED *Testbed*

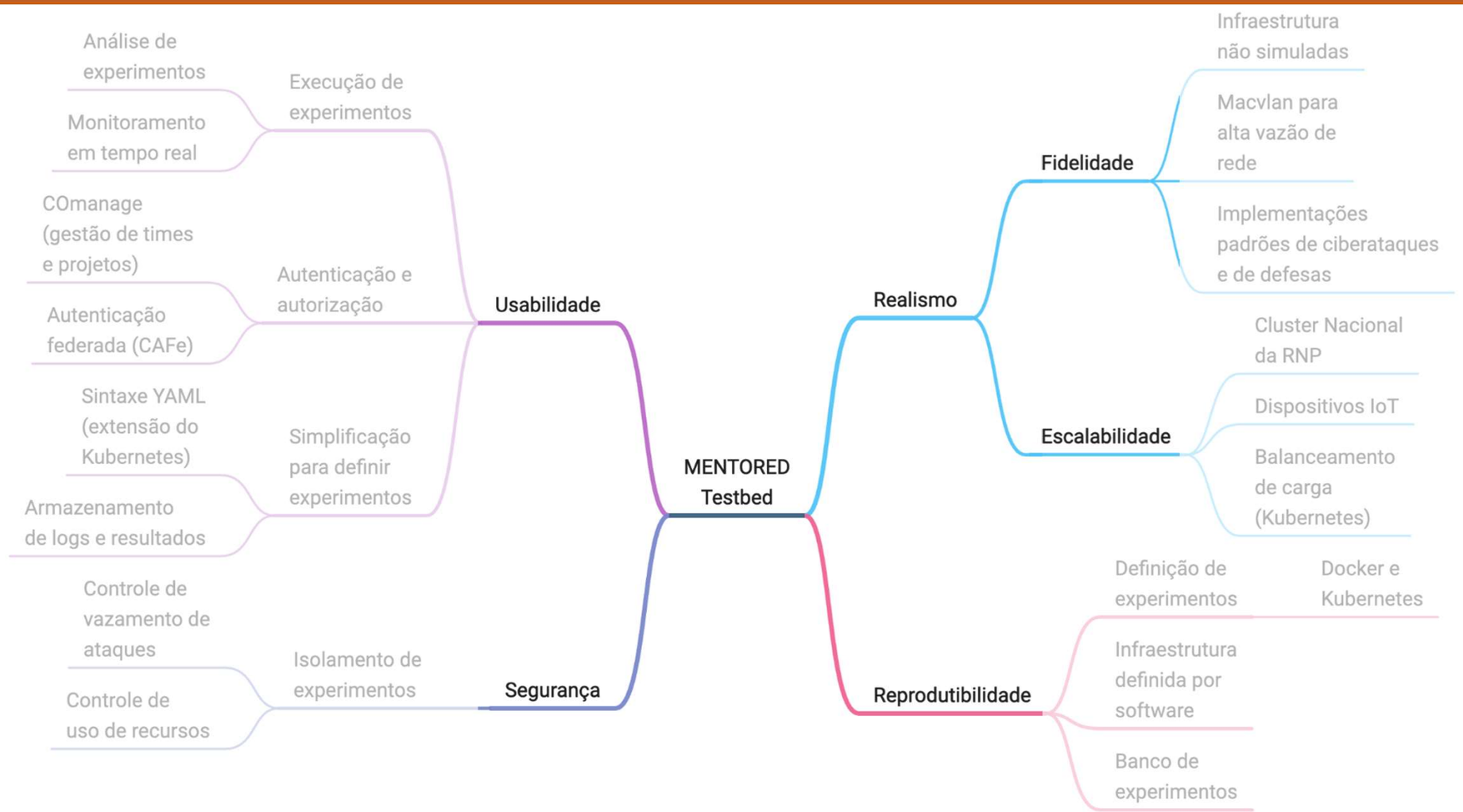
- Prover um ambiente controlado para experimentação em cibersegurança;
- Utiliza a Infraestrutura Definida por Software da Rede Nacional de Ensino e Pesquisa (Cluster Nacional):
  - Oferece escala realista e alto volume de tráfego de rede;
  - É baseado no **Kubernetes** e possui suporte a diferentes tecnologias para a virtualização de interfaces de rede.



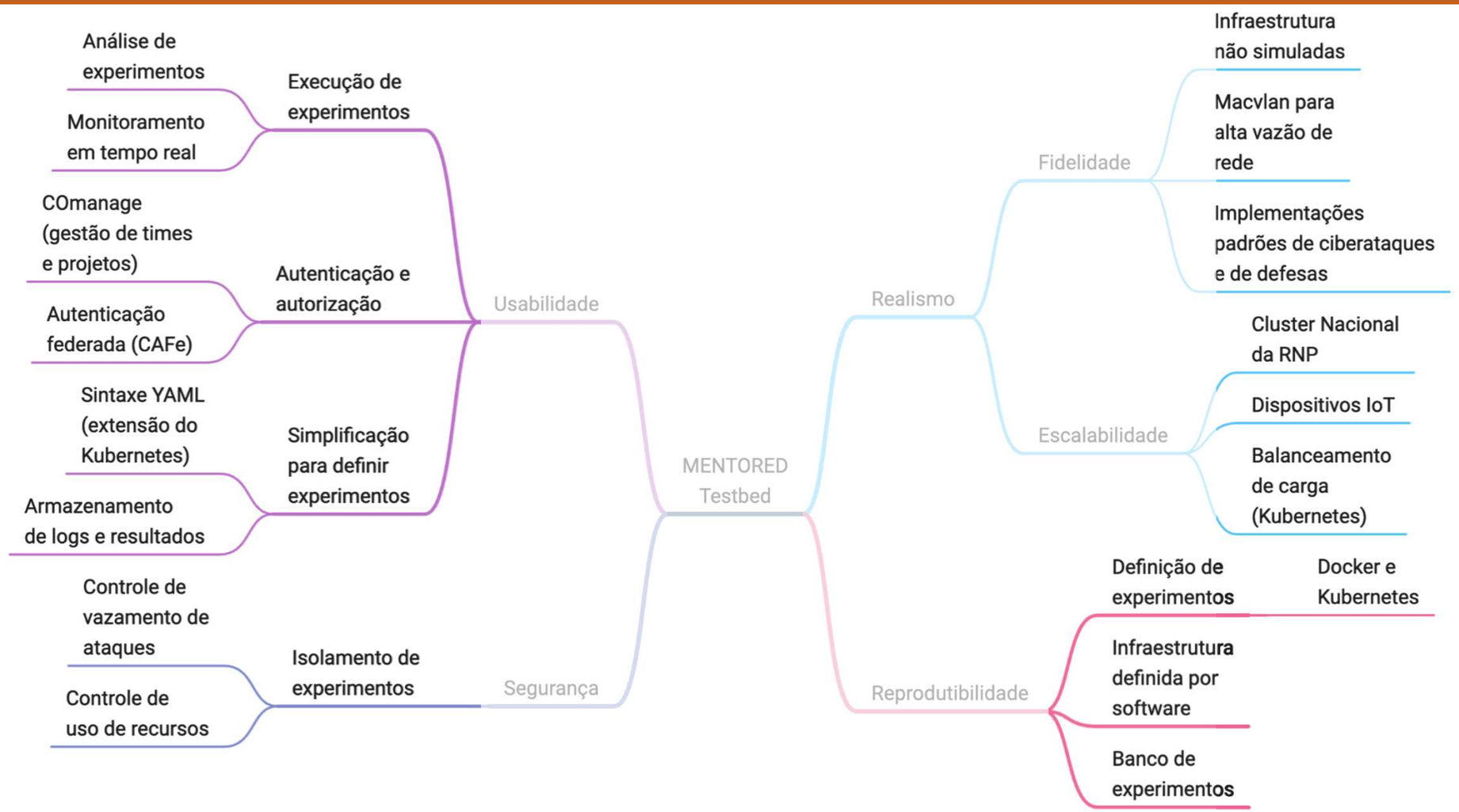
MENTORED *Testbed*

Atributos

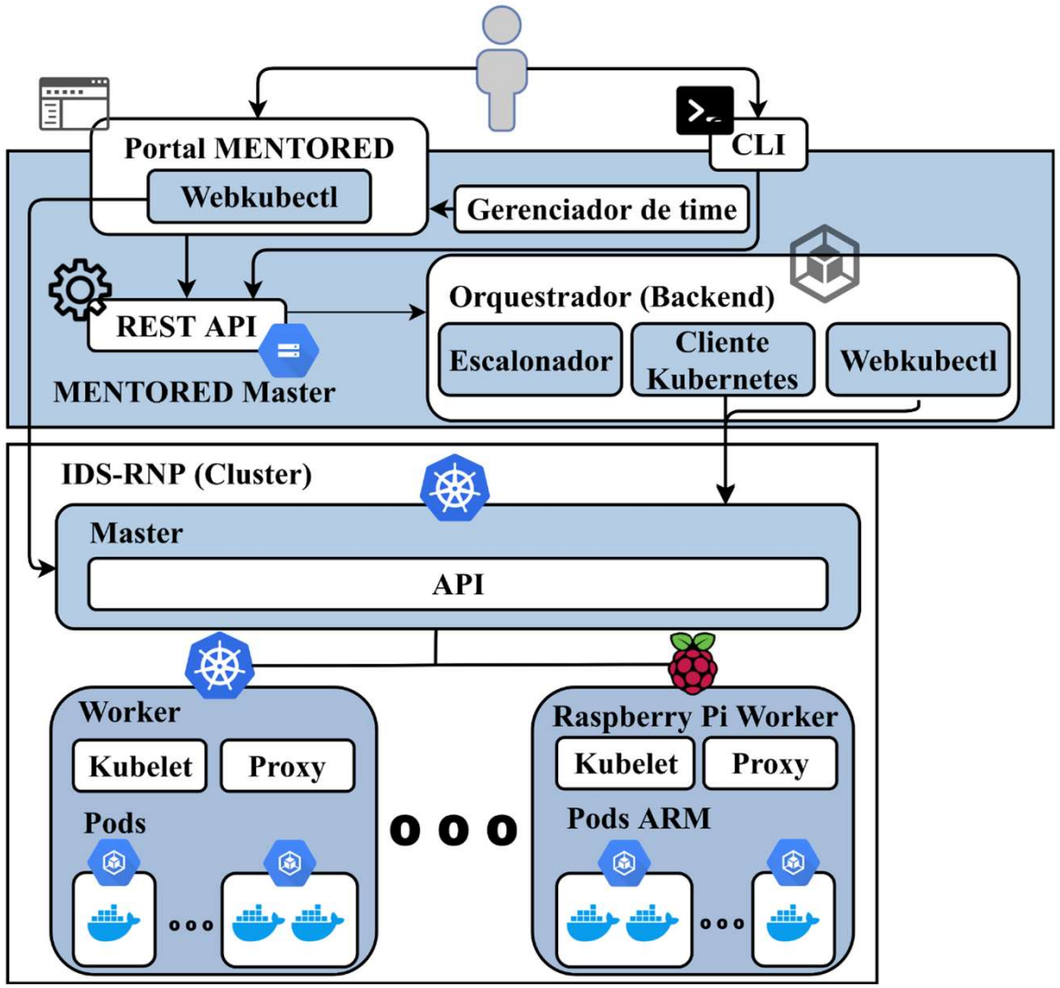
Requisitos e Características



Requisitos e Características

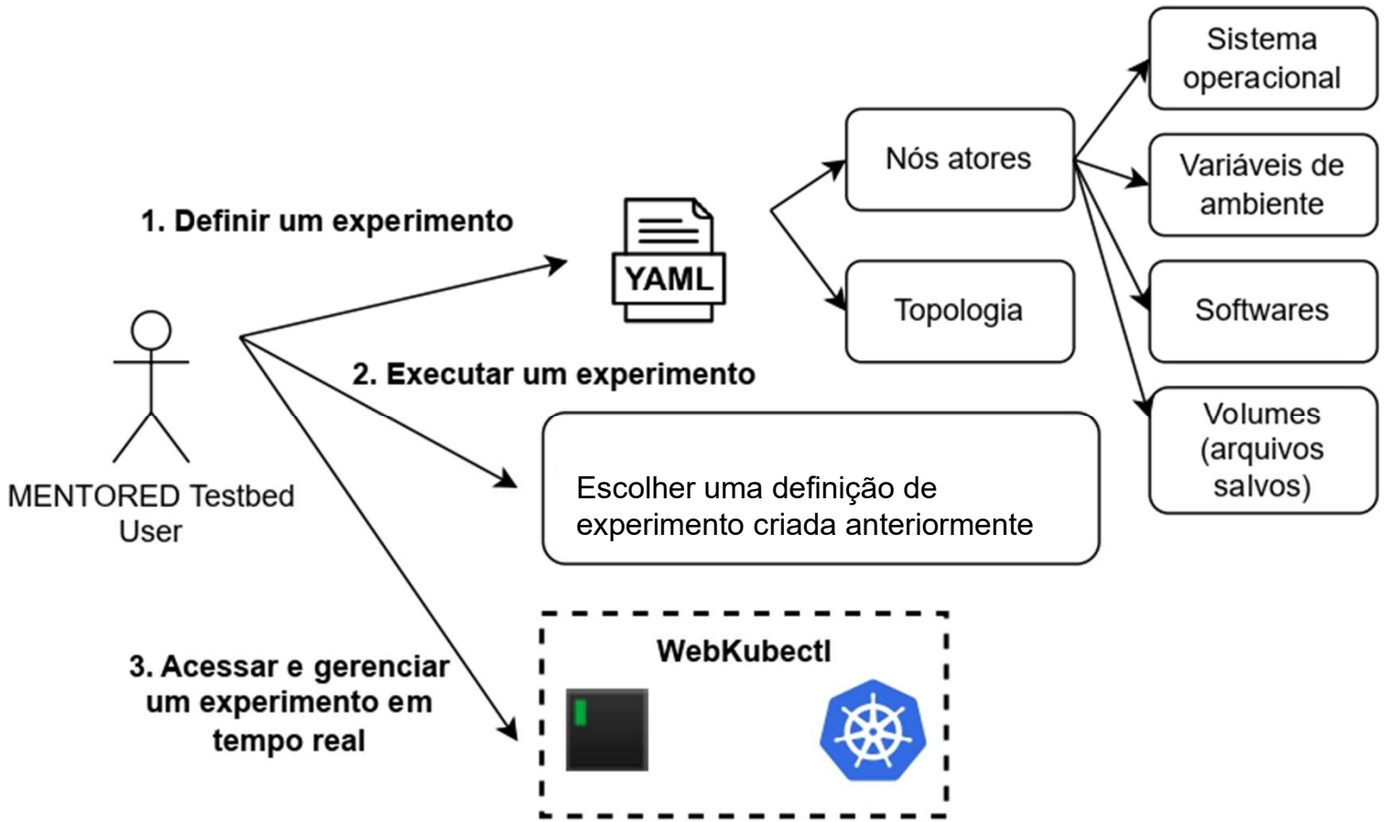


Arquitetura do MENTORED *Testbed*



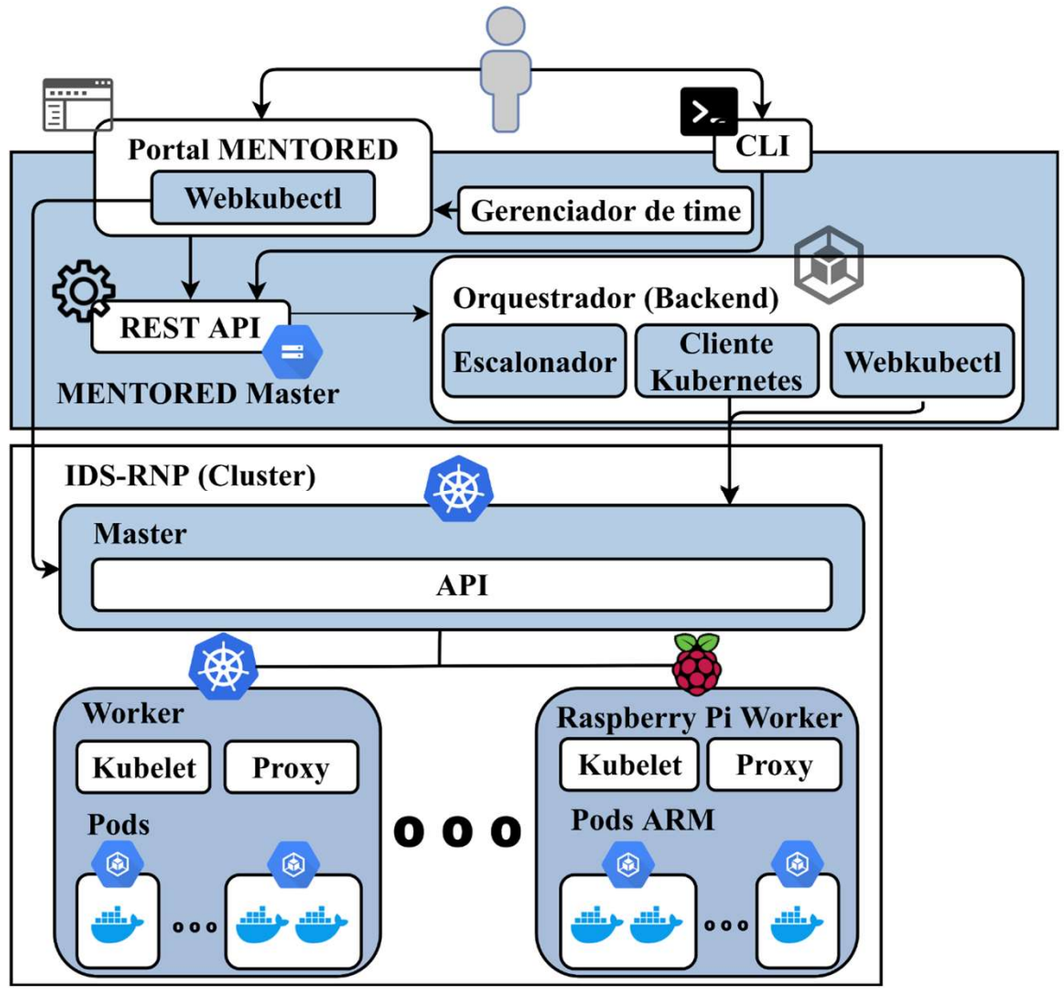
MENTORED *Testbed*
Ponto de vista do experimentador

- Visão do Experimentador
  - **Minimizar tempo para definir experimento**
  - Reduzir desafios técnicos
  - Acompanhar o experimento
- Visão do *Testbed*
  - Segurança e Autorização
  - Minimizar ociosidade de recursos
  - Reaproveitar definições de experimentos

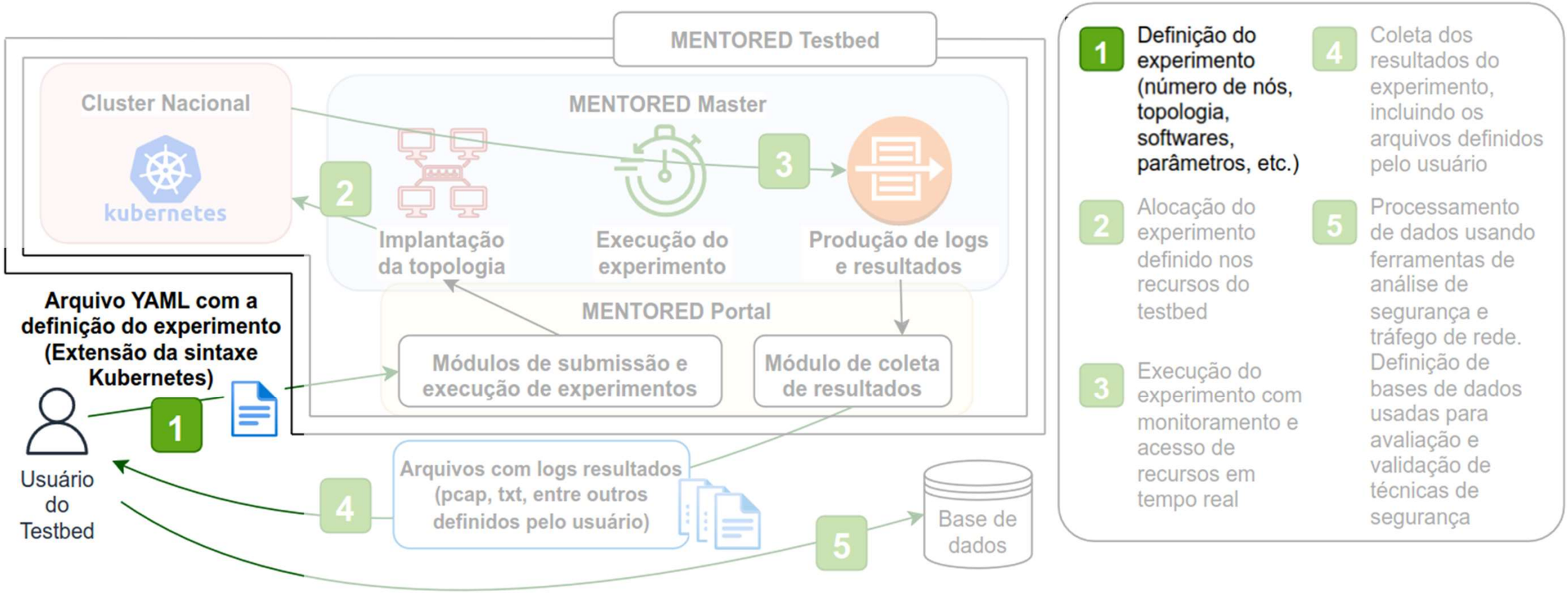


MENTORED *Testbed*
Arquitetura da implementação

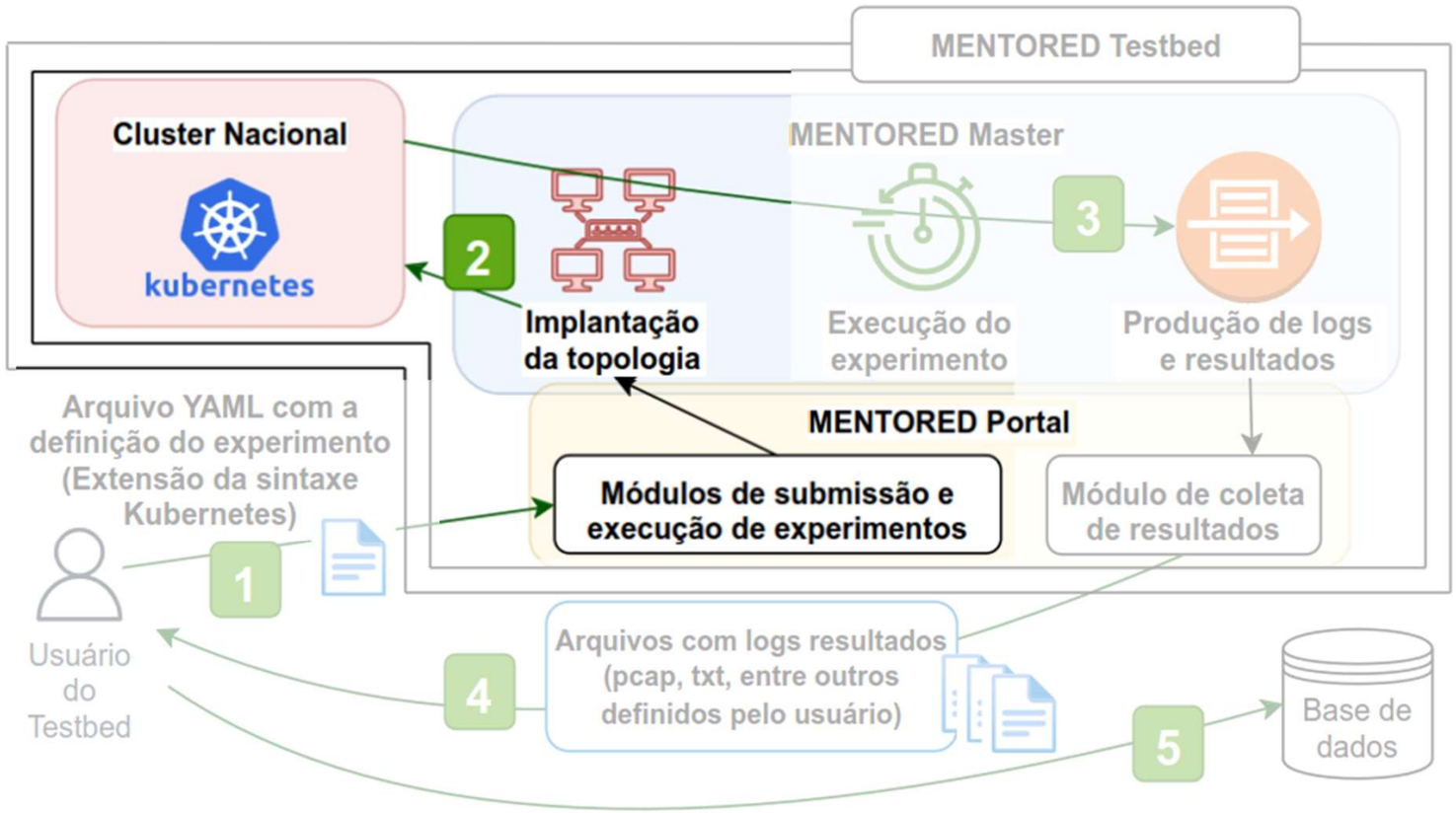
- Principais tecnologias:
  - Kubernetes (cluster)
  - WebKubectl (**Terminal no *browser***)
  - React (**Portal**)
  - Django REST (**API**)
  - COmanage (Gerenciador de time)
- Desafios
  - Cluster é dinâmico
  - Múltiplos experimentadores
  - **Recursos finitos**



MENTORED *Testbed*
Criando bases de dados

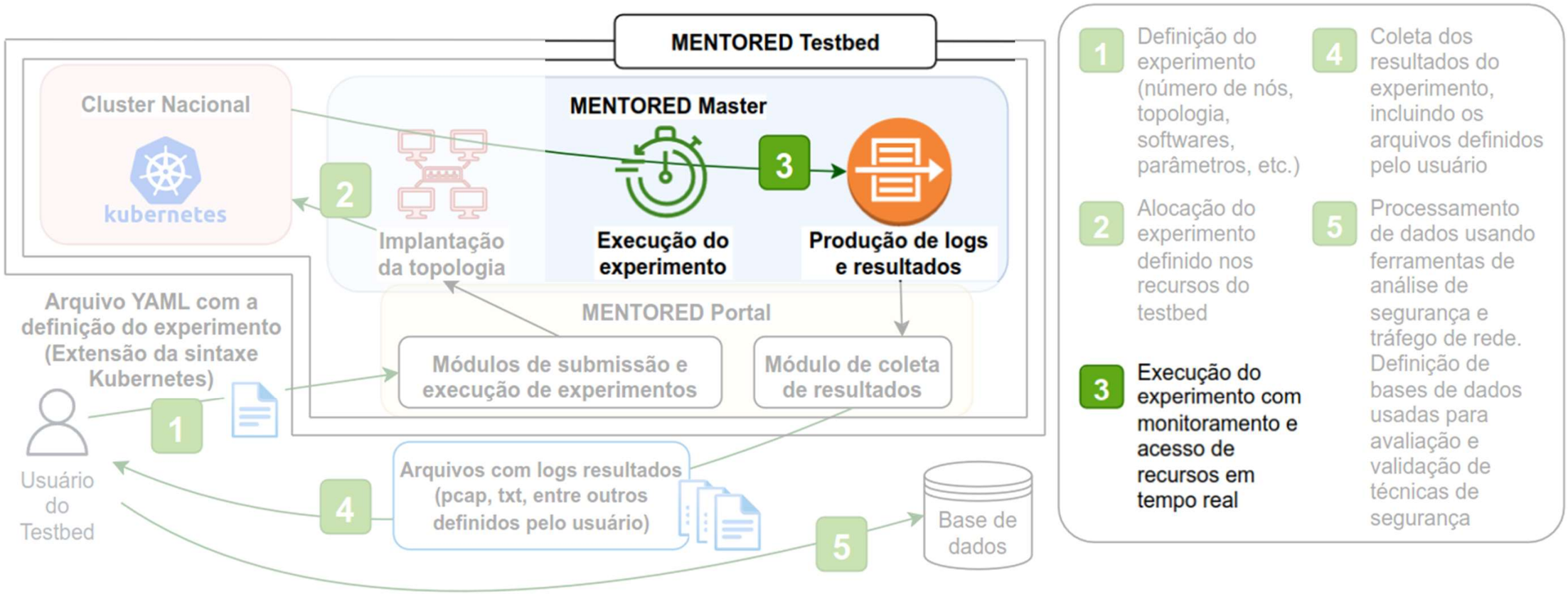


MENTORED *Testbed*
Criando bases de dados

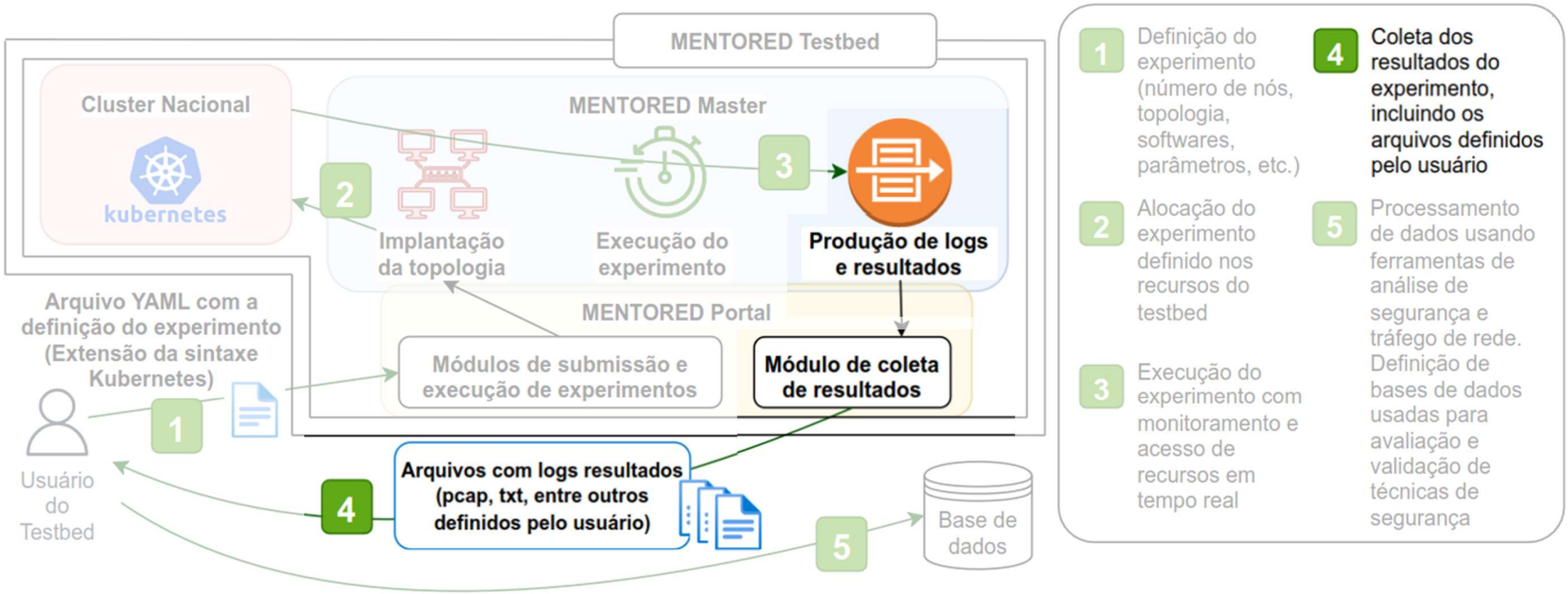


1. Definição do experimento (número de nós, topologia, softwares, parâmetros, etc.)
2. Alocação do experimento definido nos recursos do testbed
3. Execução do experimento com monitoramento e acesso de recursos em tempo real
4. Coleta dos resultados do experimento, incluindo os arquivos definidos pelo usuário
5. Processamento de dados usando ferramentas de análise de segurança e tráfego de rede. Definição de bases de dados usadas para avaliação e validação de técnicas de segurança

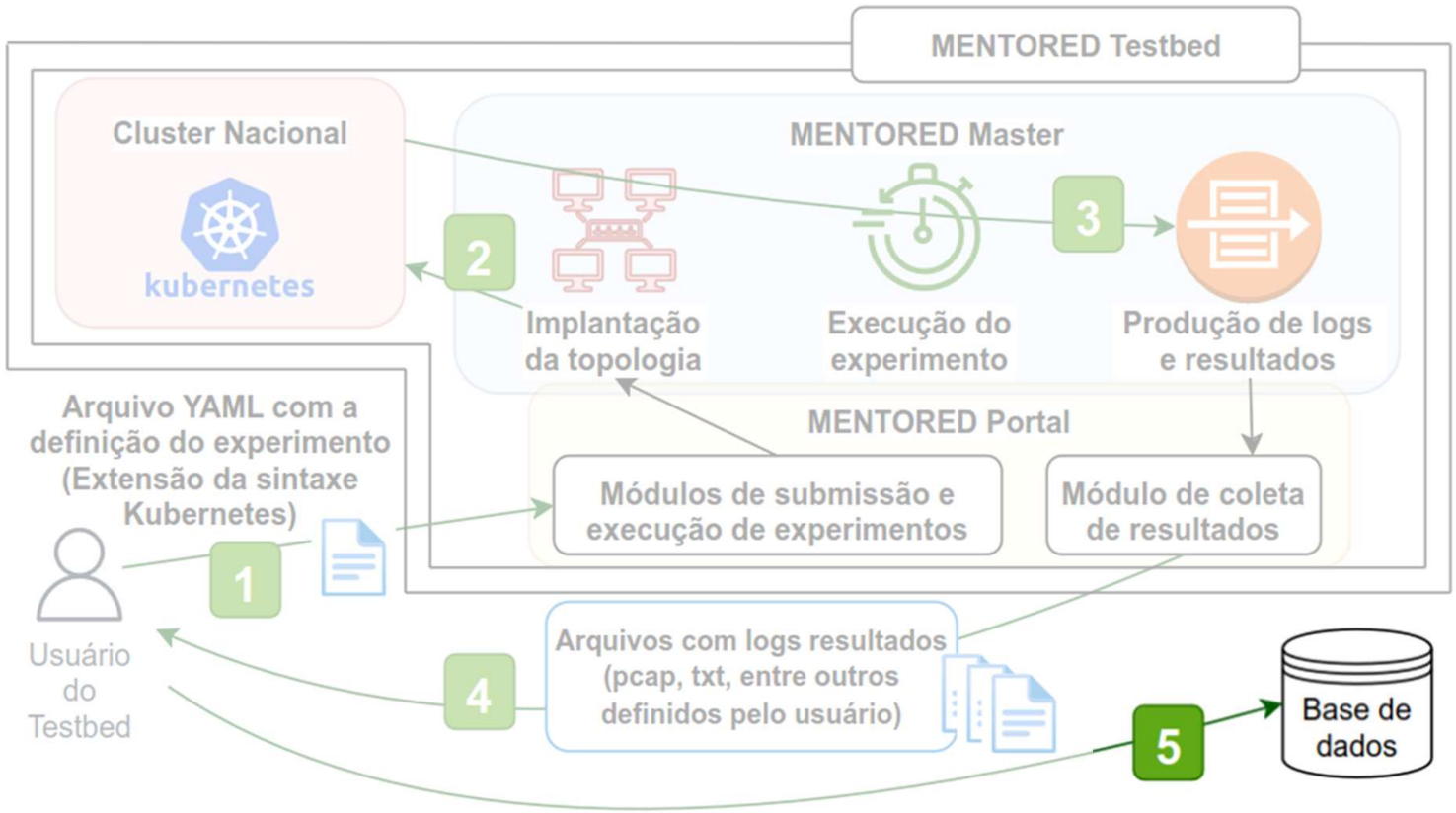
MENTORED *Testbed*
Criando bases de dados



MENTORED *Testbed*
Criando bases de dados



MENTORED *Testbed*
Criando bases de dados



1. Definição do experimento (número de nós, topologia, softwares, parâmetros, etc.)
2. Alocação do experimento definido nos recursos do testbed
3. Execução do experimento com monitoramento e acesso de recursos em tempo real
4. Coleta dos resultados do experimento, incluindo os arquivos definidos pelo usuário
5. **Processamento de dados usando ferramentas de análise de segurança e tráfego de rede. Definição de bases de dados usadas para avaliação e validação de técnicas de segurança**

MENTORED *Testbed*
Criando bases de dados

Considerações Finais

Considerações finais

- Complexidade e evolução das ameaças exigem uma abordagem robusta e dinâmica para P&D
- MENTORED testbed: tecnologias avançadas e design estratégico
  - objetivo: simplicidade para definir, executar e monitorar experimentos
  - Integração com cluster de IoT
  - ampliar os experimentos

Minicurso SBRC 2024

Considerações finais

- **Futuro da experimentação em cibersegurança**
  - IA
  - Blockchain
  - Computação quântica
  - Experimentos mais complexos - respostas a incidentes automatizadas, privacidade e gestão de informações sensíveis
- **Formação qualificada em cibersegurança**

Q&A

Site do Projeto Mentored

Minicurso SBRC 2024

MENTORED *Testbed*: Pesquisa Experimental em Cibersegurança

Apresentadores:

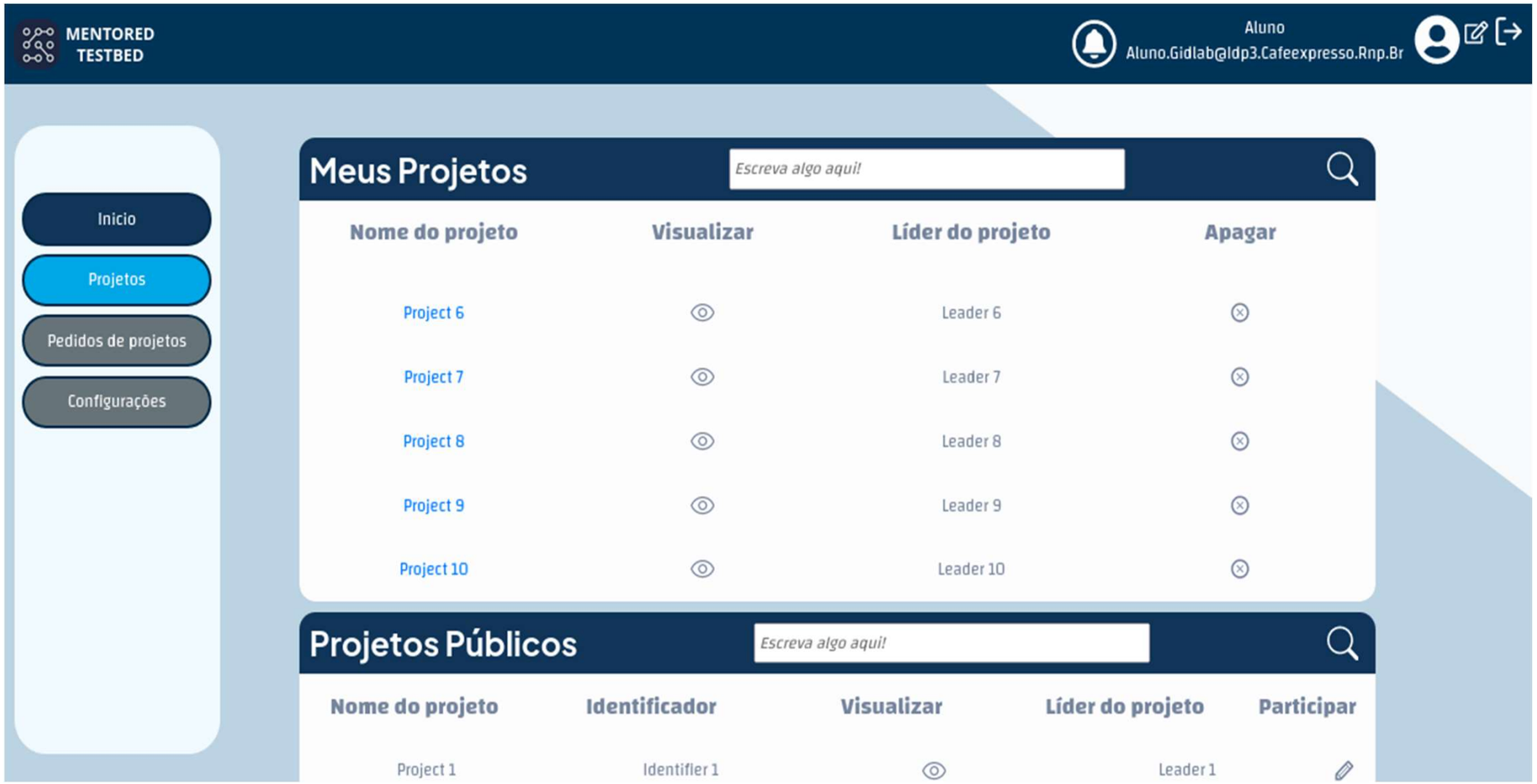
- **Michelle S. Wangham**

MENTORED *Testbed*

Telas - *Dashboard*

MENTORED *Testbed*

Telas - Projetos



MENTORED *Testbed*

Telas - Definição de Experimentos

MENTORED *Testbed*

Telas - Monitoramento em Tempo Real