

MENTORED *Testbed*: Pesquisa Experimental em Cibersegurança

Apresentadores:

- Michelle S. Wingham, UNIVALI/RNP
- Davi Gemmer, RNP

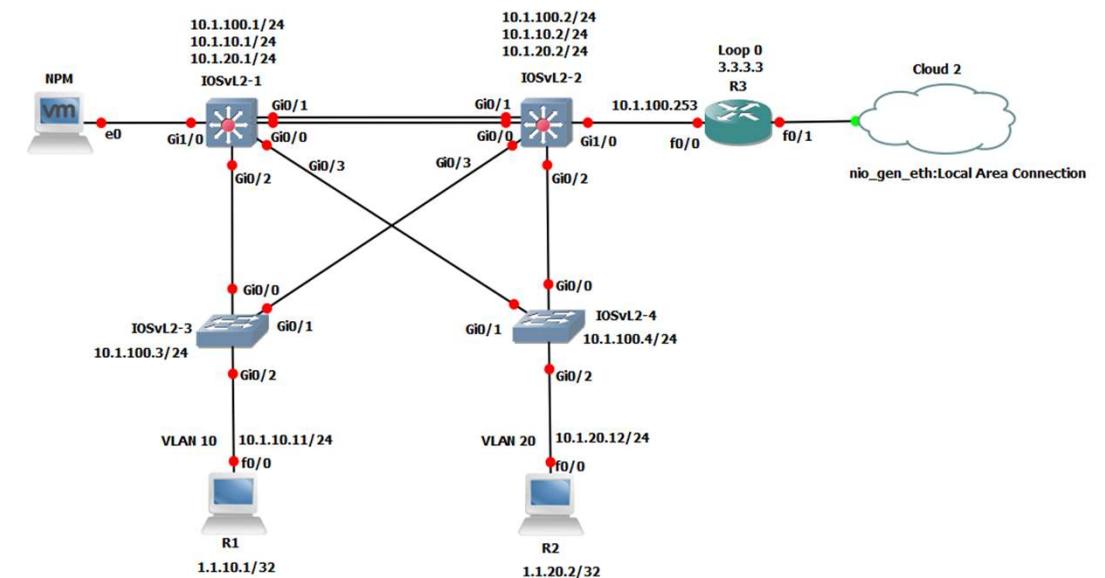


Introdução

- 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

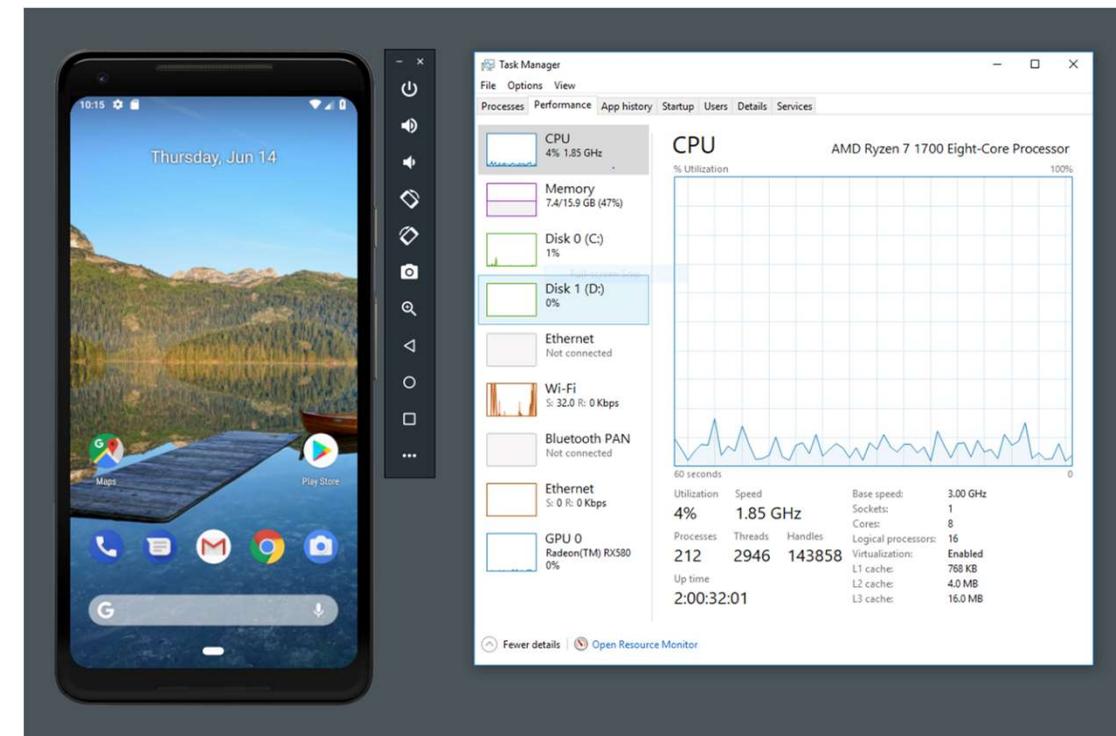
- **Simuladores**
 - Ambientes virtuais que replicam cenários reais
- **Emuladores**
 - Replicam o comportamento de software e hardware
- **Testbeds**
 - Reproduzem uma infraestrutura de rede e sistemas de informação
 - Realismo e fidelidade



Fonte: <https://gns3.com>

Ambientes de experimentação em cibersegurança

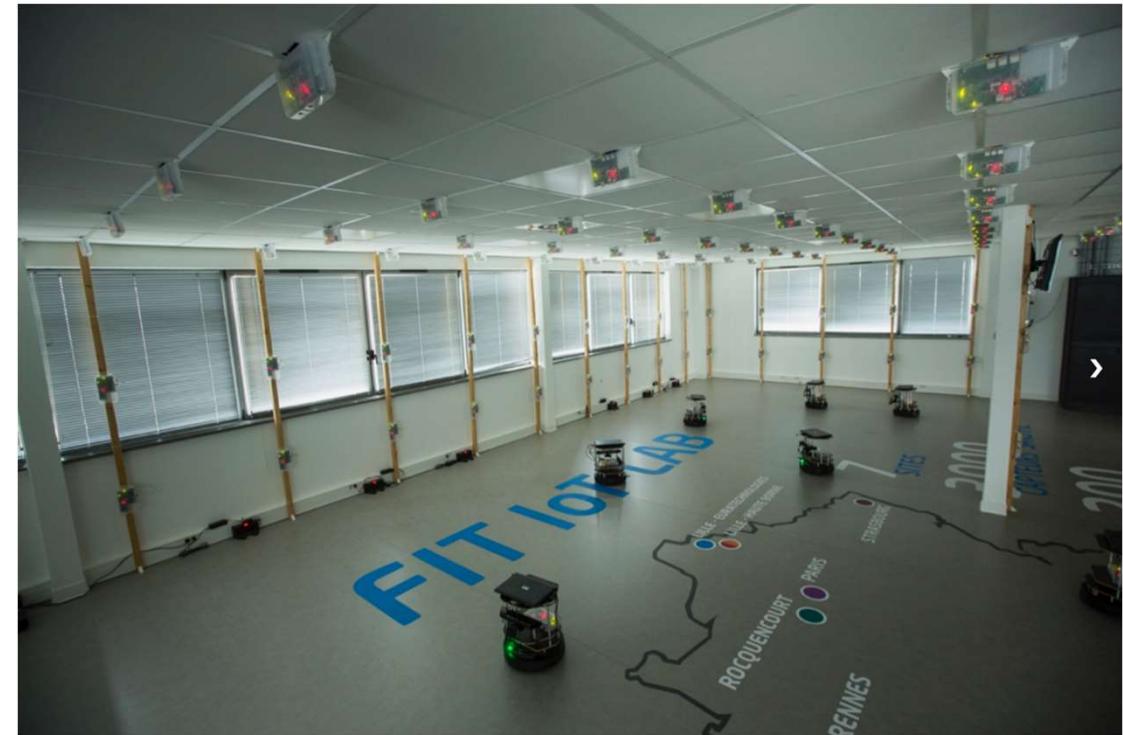
- **Simuladores**
 - Ambientes virtuais que replicam cenários reais
- **Emuladores**
 - Replicam o comportamento de software e hardware
- **Testbeds**
 - Reproduzem uma infraestrutura de rede e sistemas de informação
 - Realismo e fidelidade



Fonte: <https://developer.android.com>

Ambientes de experimentação em cibersegurança

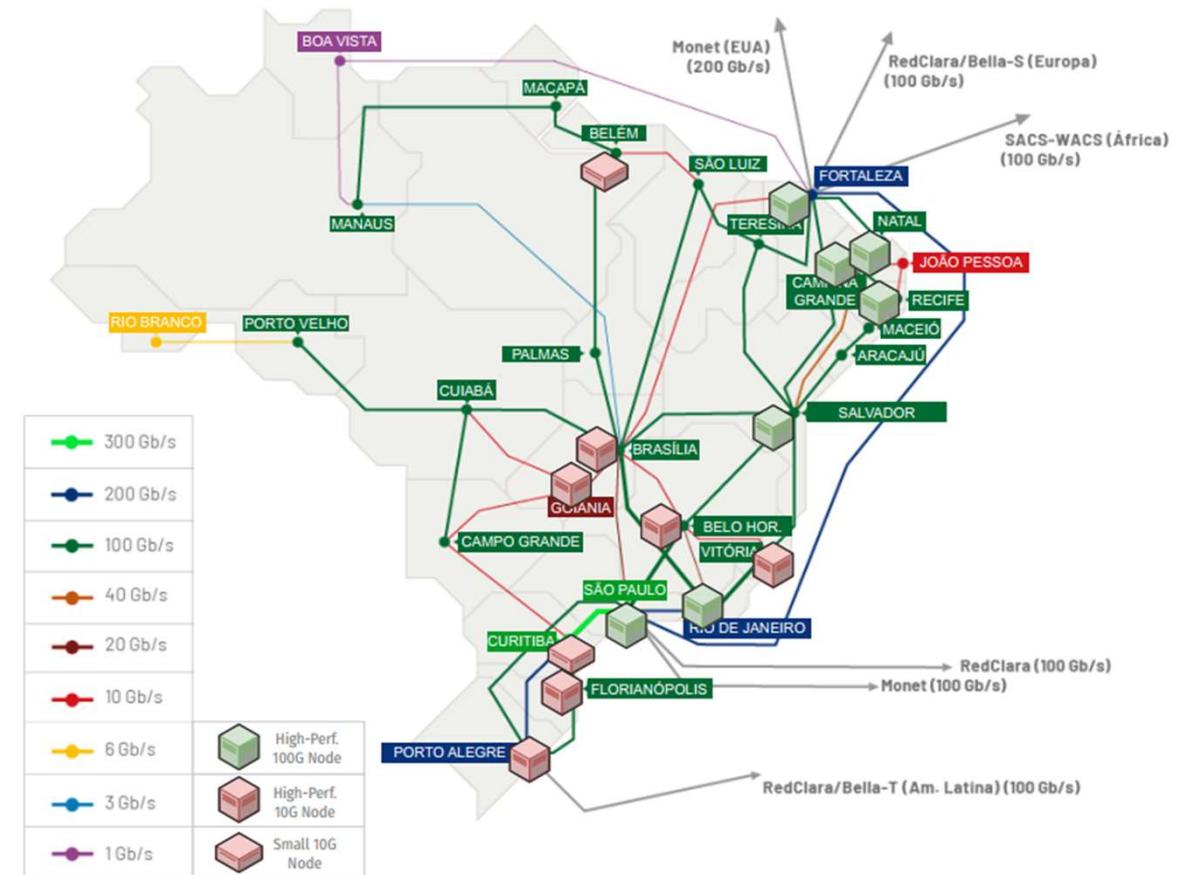
- **Simuladores**
 - Ambientes virtuais que replicam cenários reais
- **Emuladores**
 - Replicam o comportamento de software e hardware
- **Testbeds**
 - Reproduzem uma infraestrutura de rede e sistemas de informação
 - Realismo e fidelidade



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

Desafios para conduzir experimentos em cibersegurança

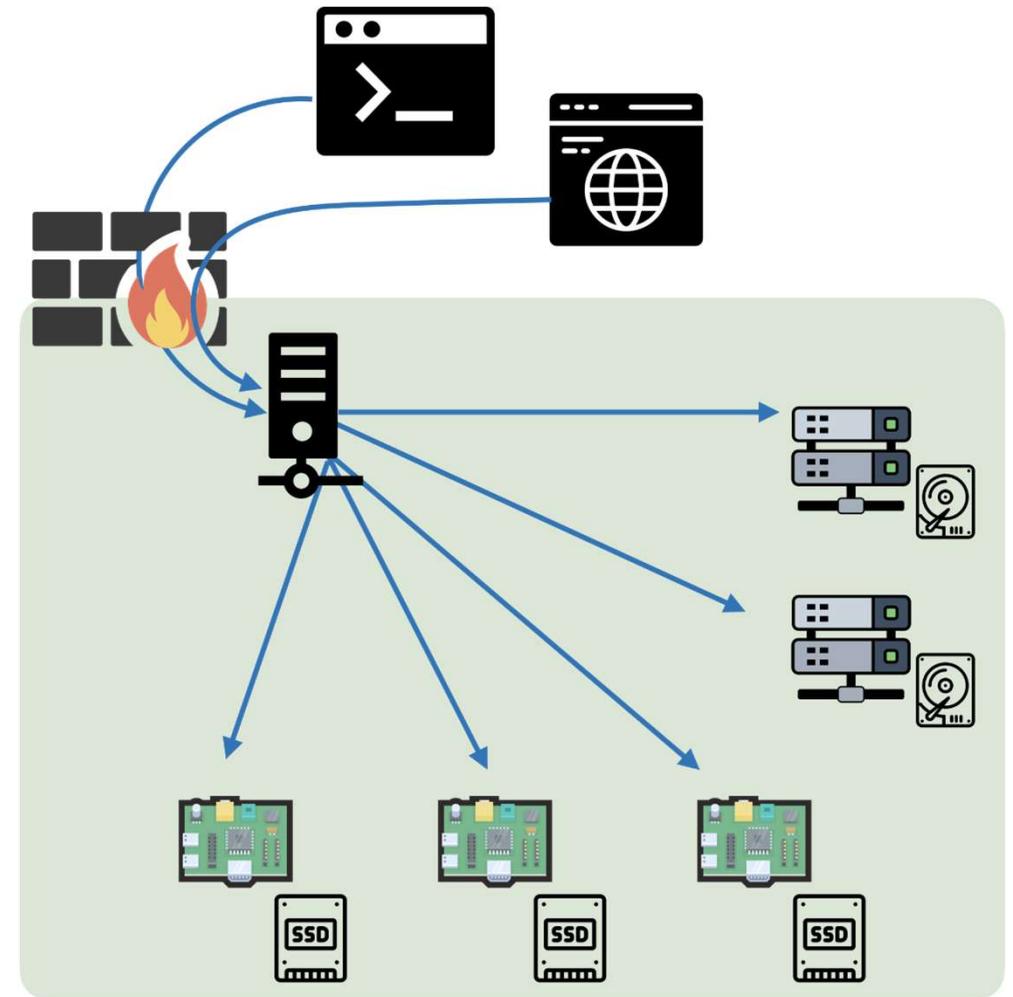
- **Gerenciamento de recursos geograficamente distribuídos**
 - Agendamento e sincronização por todos os dispositivos
- **Capacidade dos dispositivos e dos enlaces**
 - Limita o tipo de experimento ou número de experimentos em paralelo
- **Automatização e orquestração para início e término dos experimentos**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



Fonte: RNP

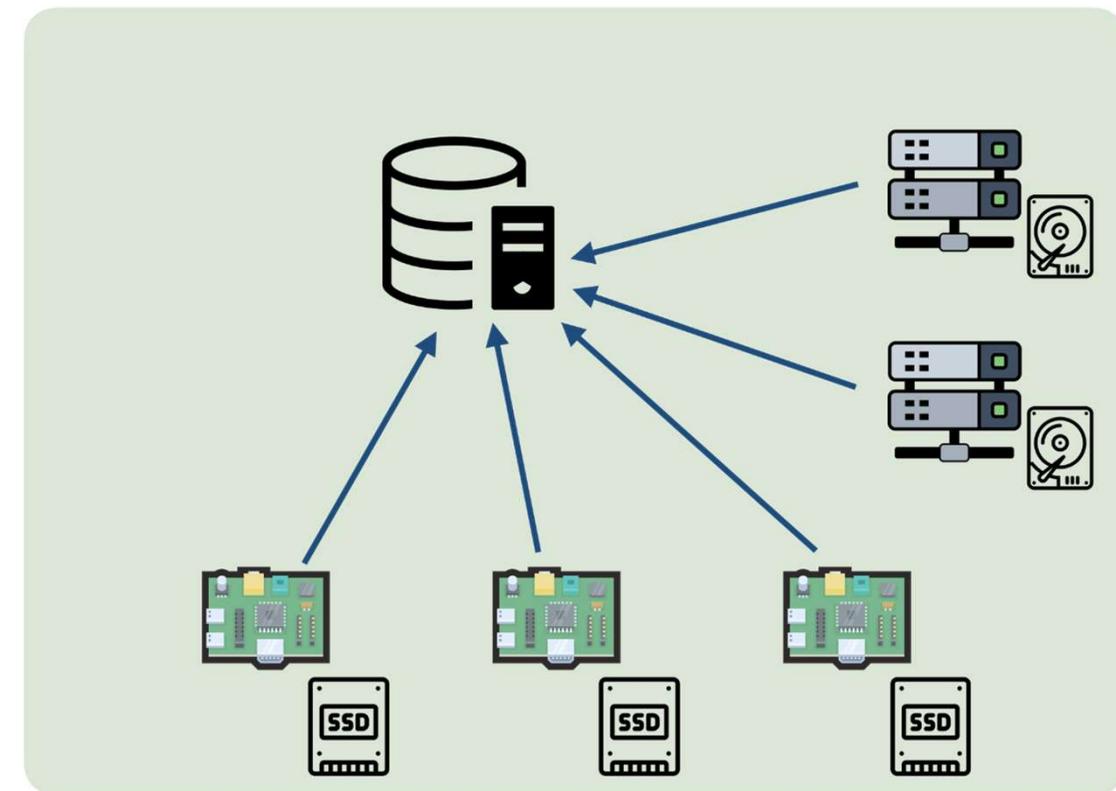
Desafios para conduzir experimentos em cibersegurança

- **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



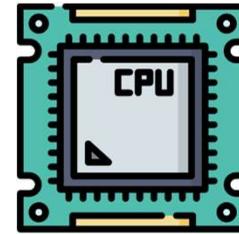
Requisitos de *testbeds* de cibersegurança

- **Fidelidade**

- Replicar com precisão ambiente alvo do estudo

- **Flexibilidade**

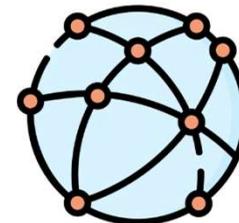
- Adaptar para diferentes cenários e experimentos



**ARM
x86-64**



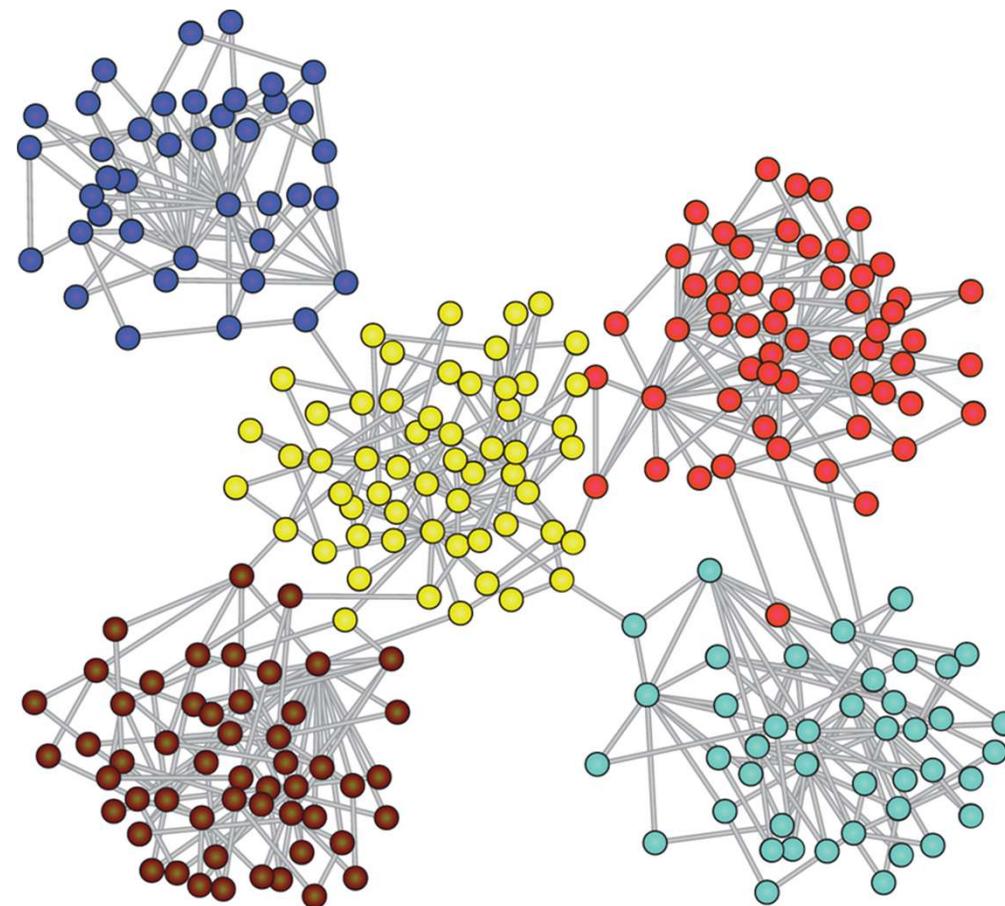
**WiFi
802.15.4**



**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**

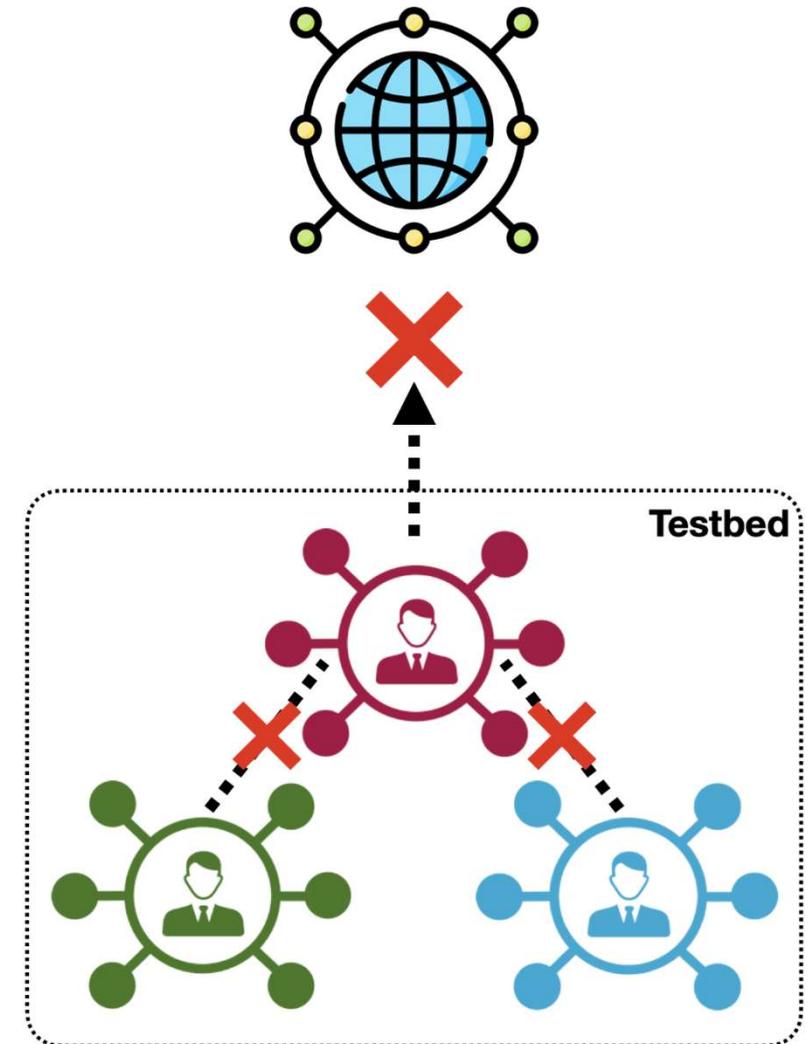
- Repetir experimentos e obter resultados estaticamente semelhantes:



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 vazarem para Internet



MENTORED

Testbed

Projeto MENTORED



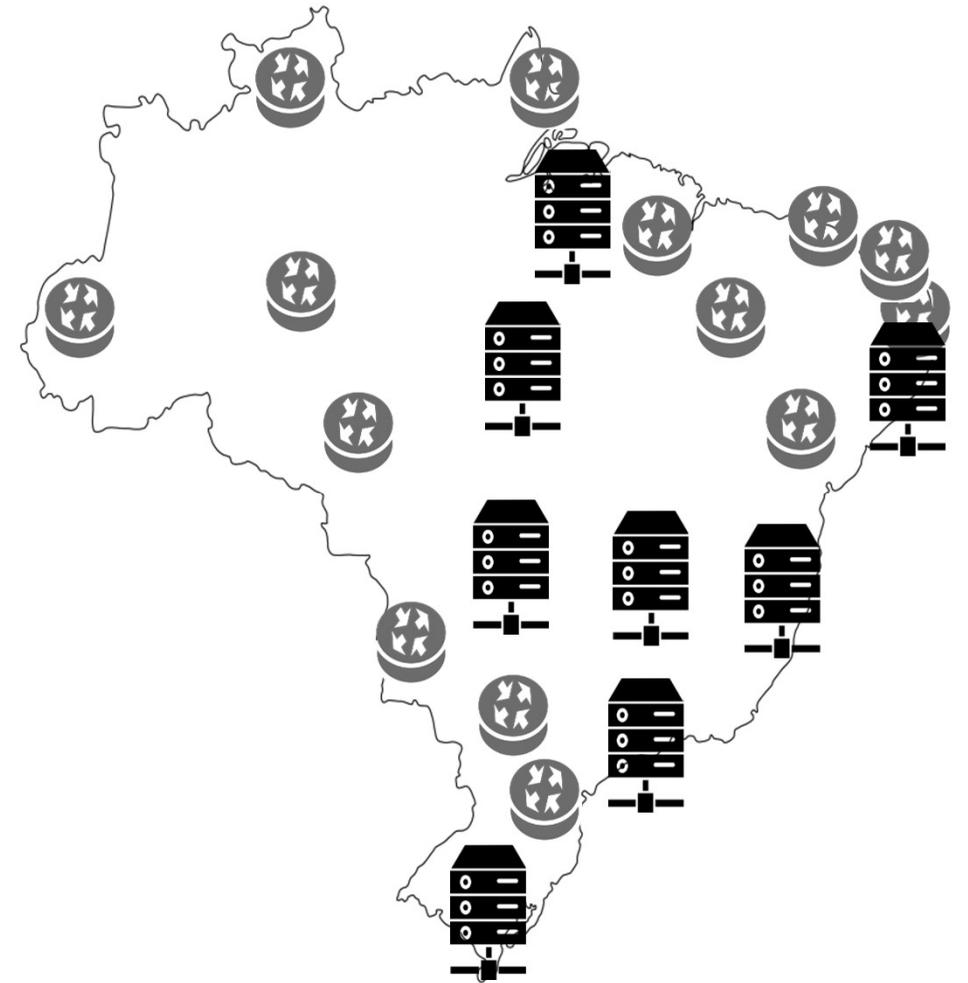
- Identificar, modelar e avaliar comportamentos maliciosos relacionados
- Auxiliar na construção de soluções avançadas e coordenadas para possibilitar à **prevenção, predição, detecção e mitigação de ataques DDoS**;
- Fornecer a comunidade científica em Cibersegurança um **testbed** para permitir que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



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.

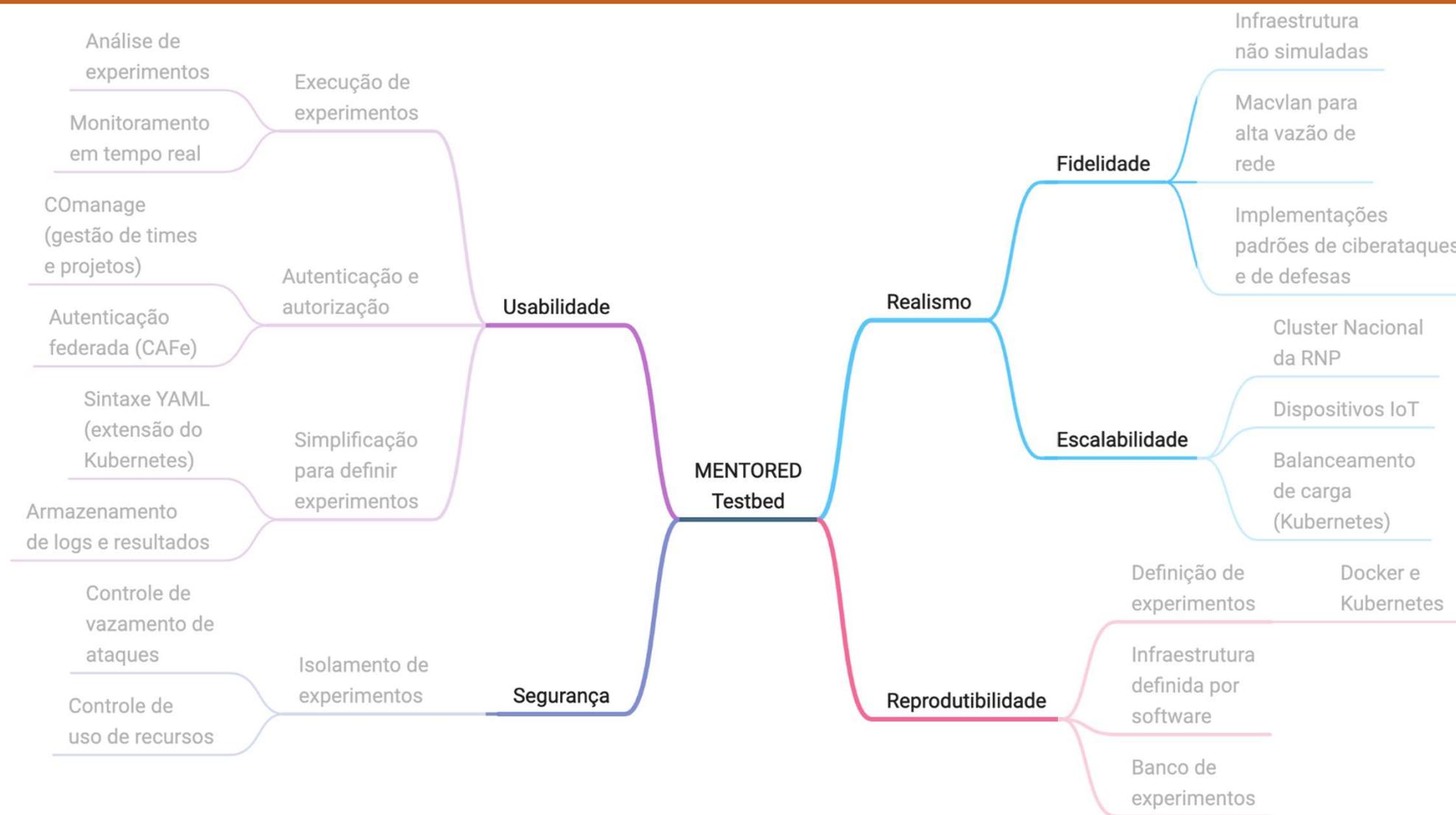


MENTORED *Testbed*

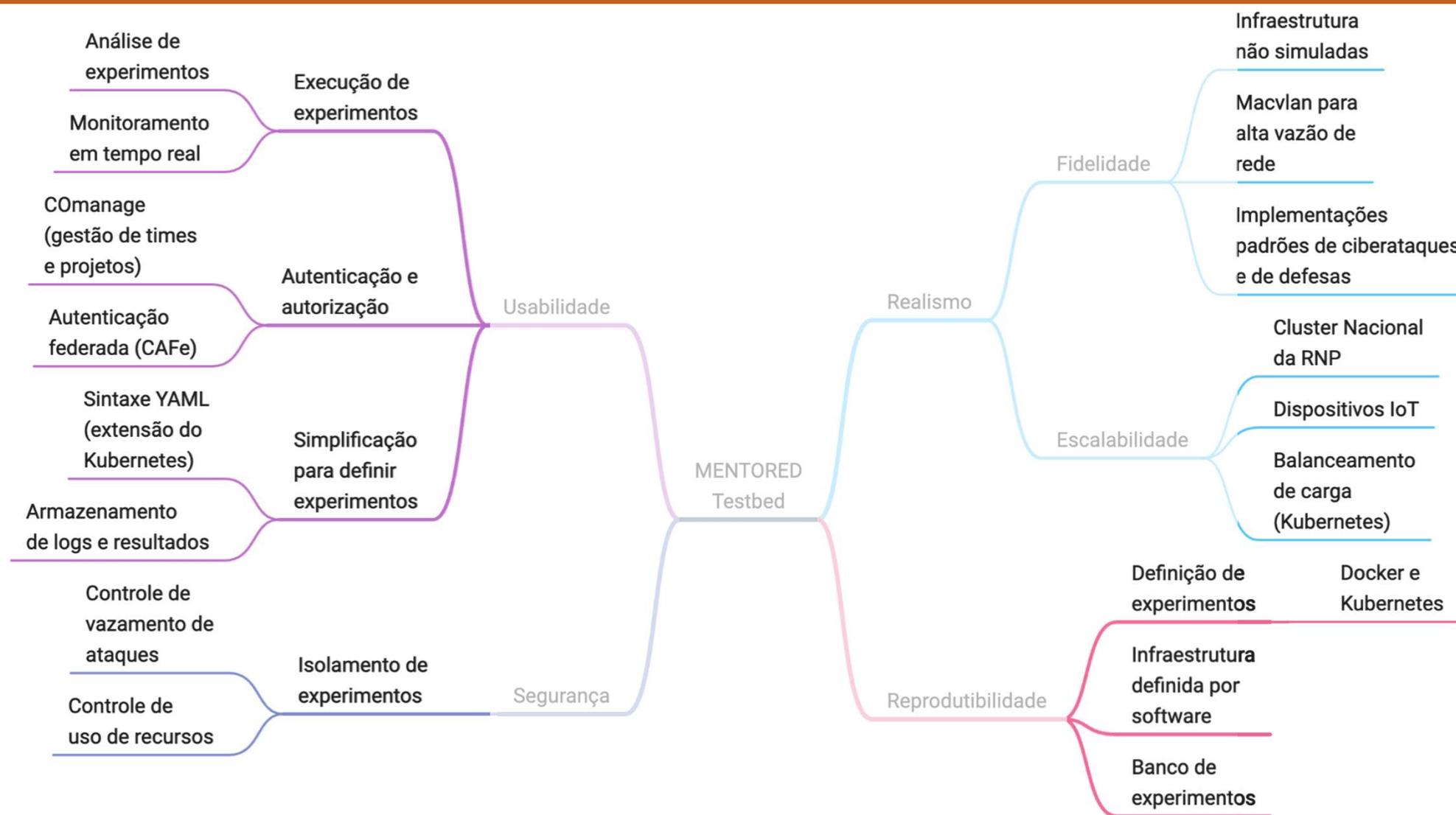
Atributos



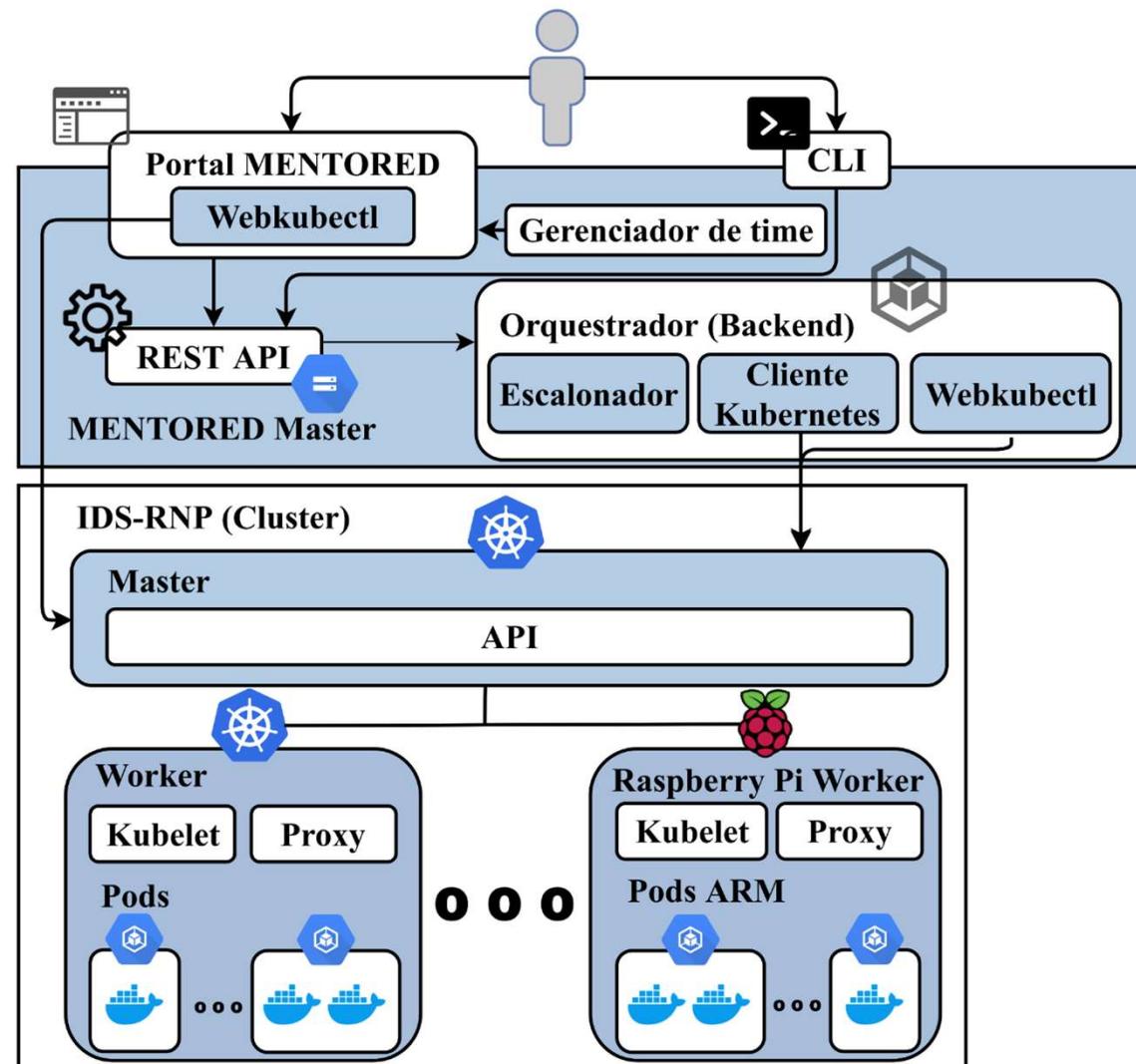
Requisitos e Características



Requisitos e Características



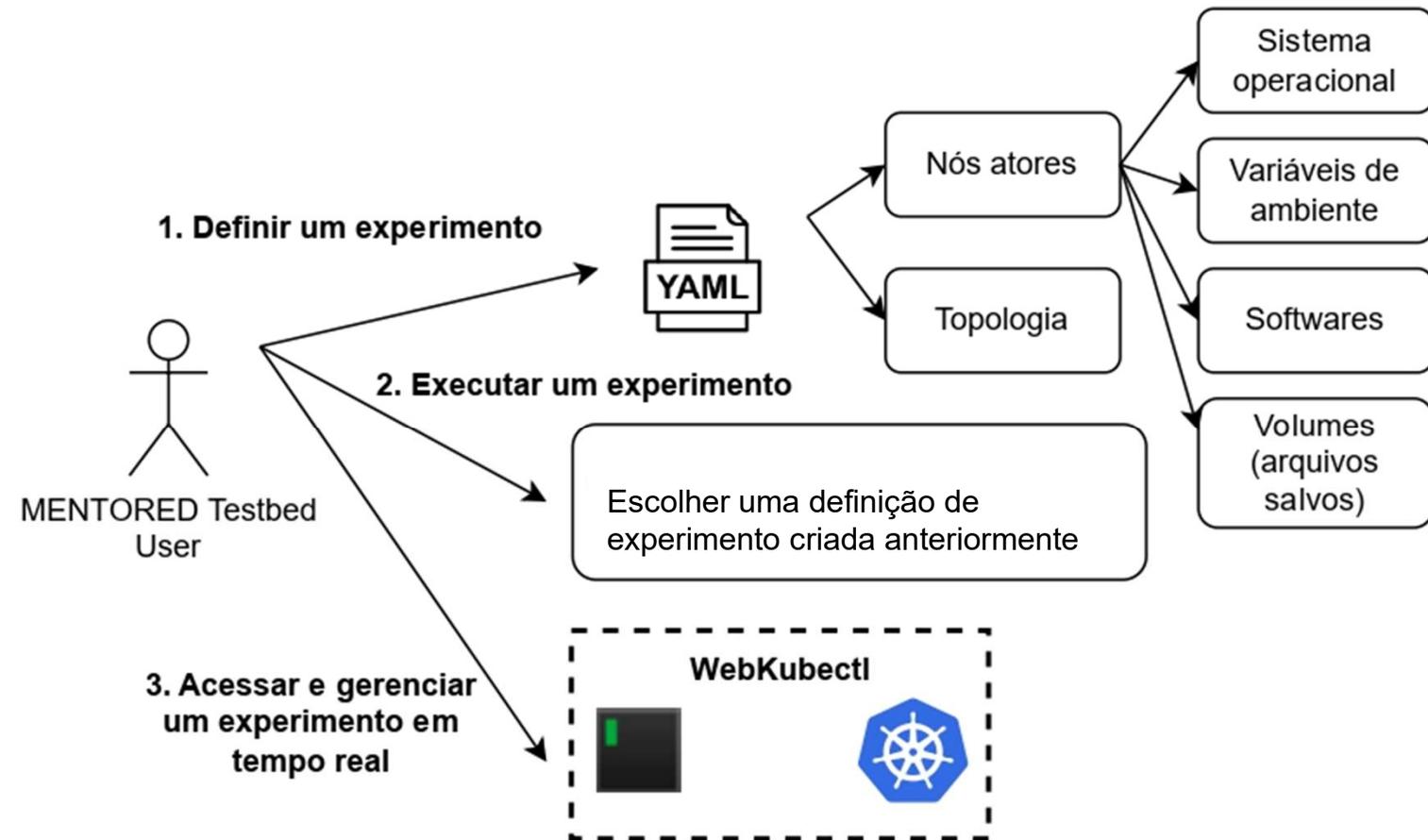
Arquitetura do MENTORED *Testbed*



MENTORED *Testbed*

Ponto de vista do experimentador

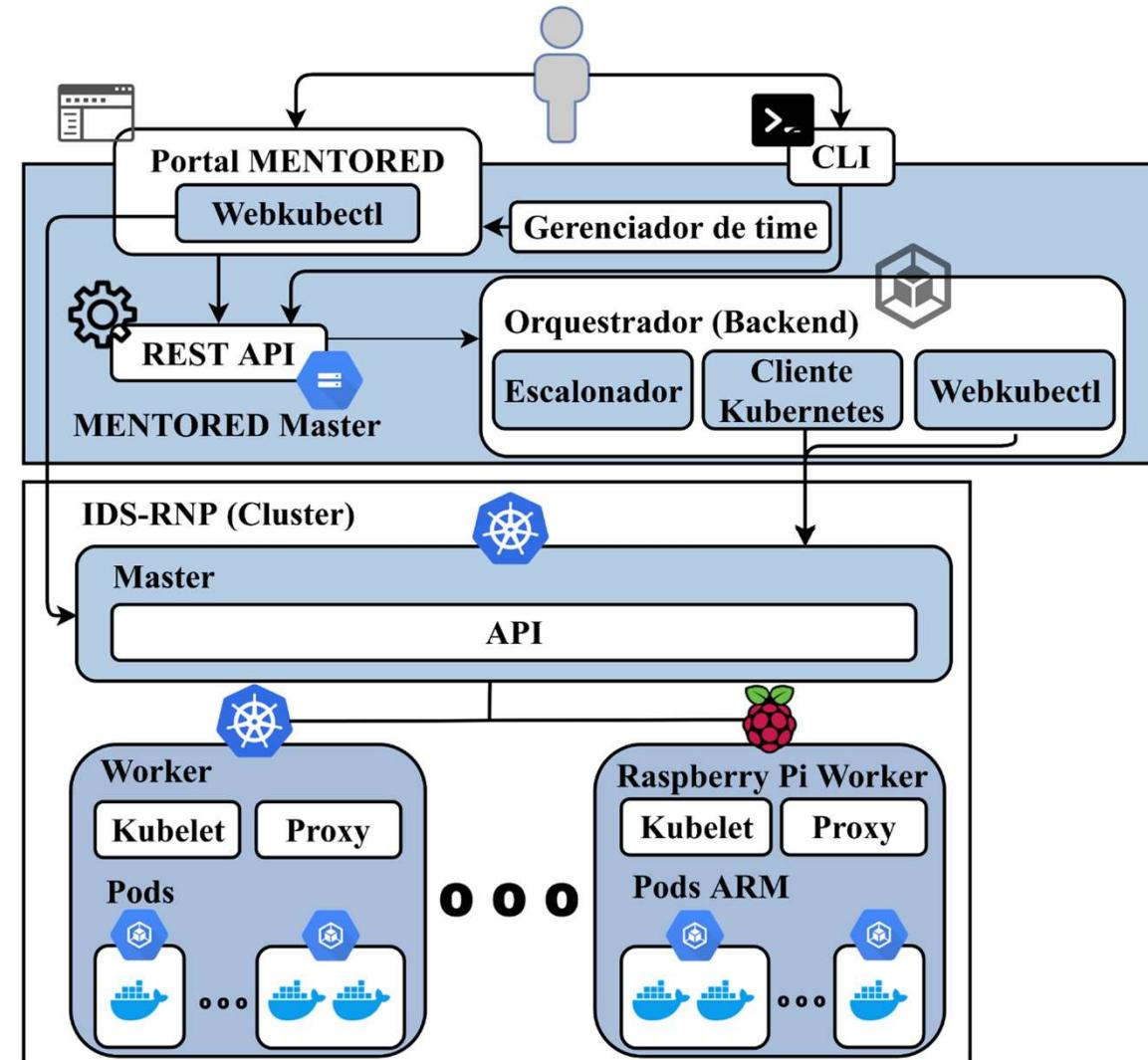
- Visão do Experimentador
 - **Minimizar tempo para definir experimento**
 - Reduzir desafios técnicos
 - Acompanhar o experimento
- Visão do *Testbed*
 - Segurança e Autorização
 - Minimizar ociosidade de recursos
 - Reaproveitar definições de experimentos



MENTORED *Testbed*

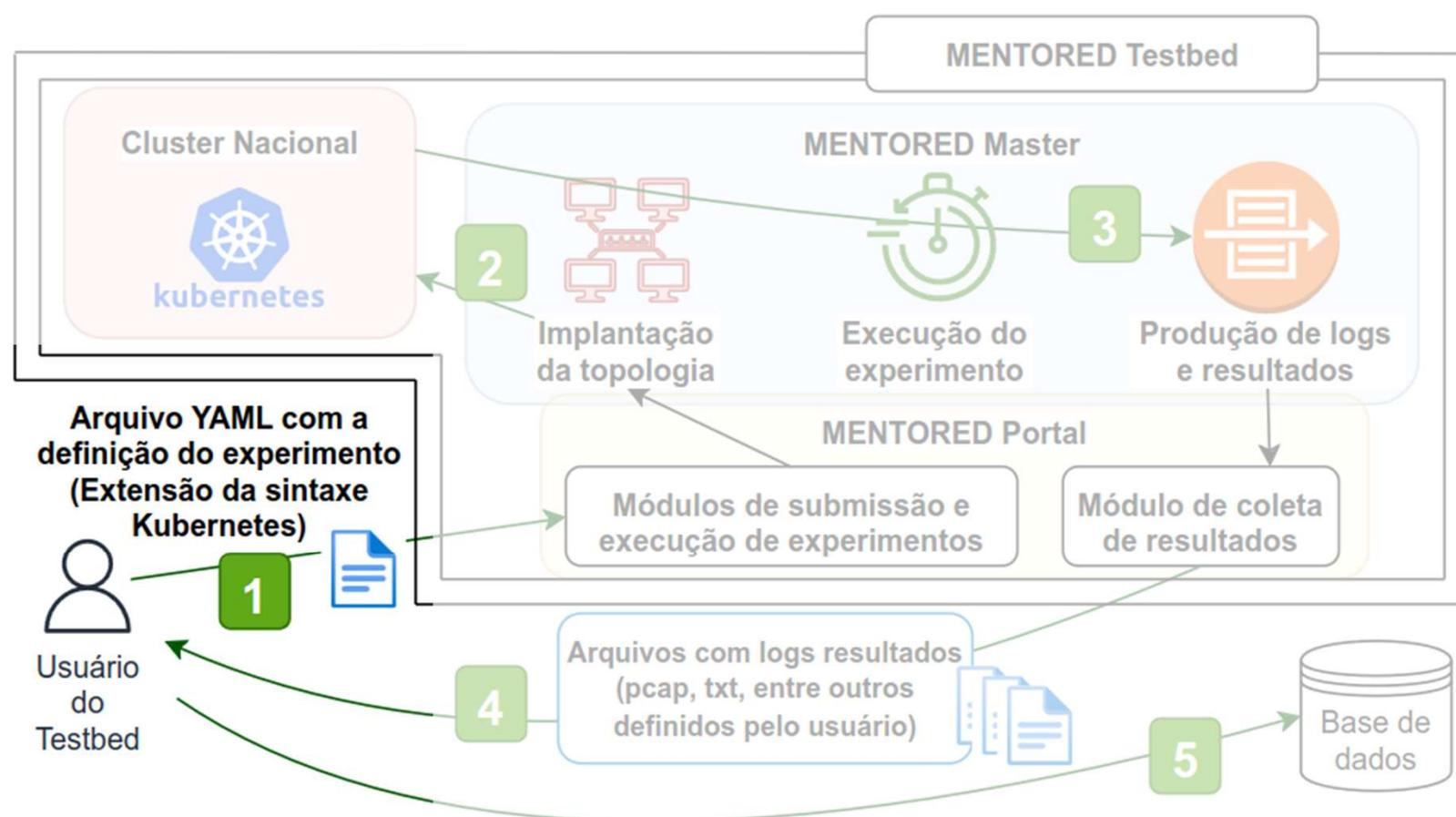
Arquitetura da implementação

- 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*

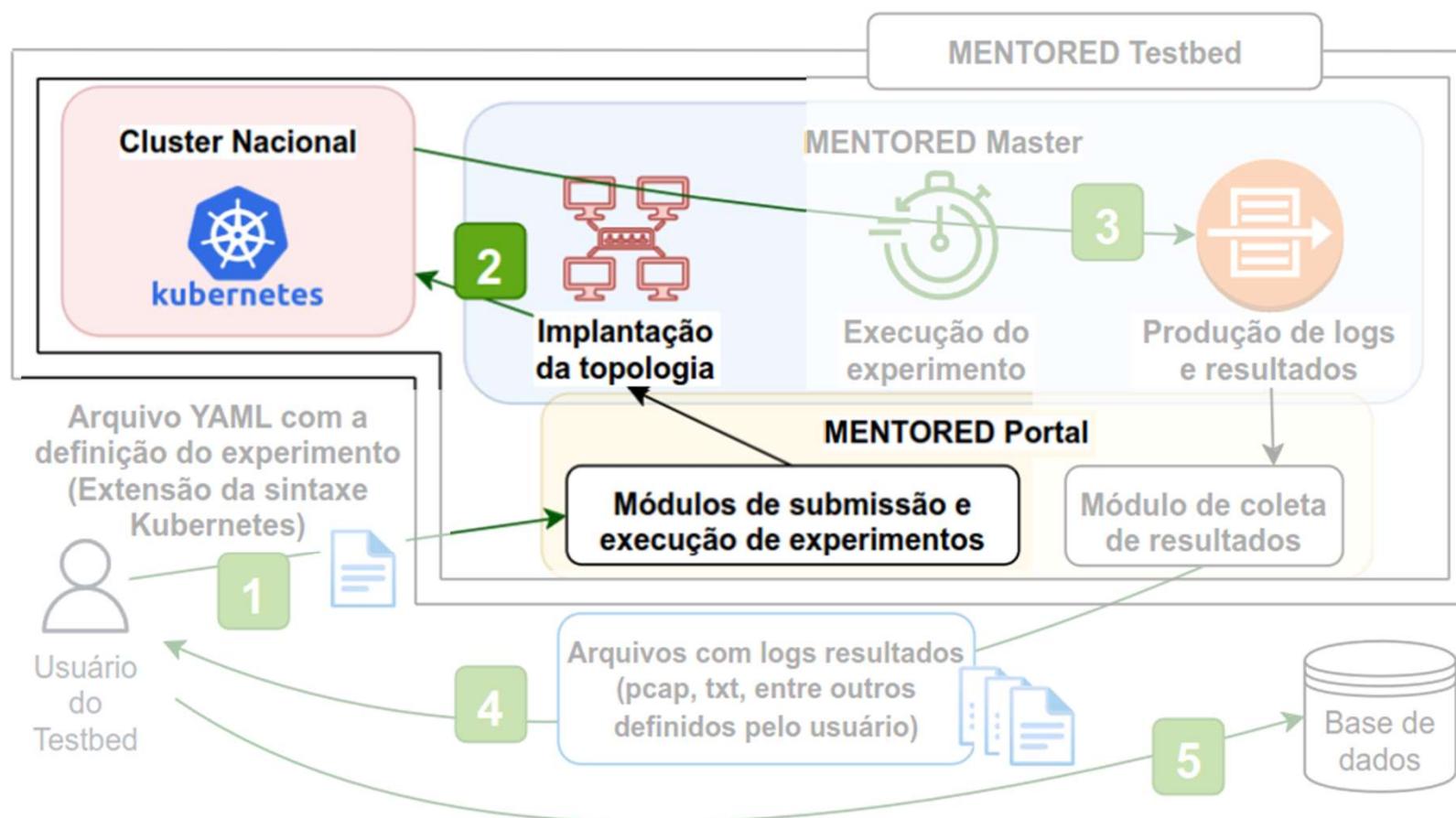
Criando bases de dados



- 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*

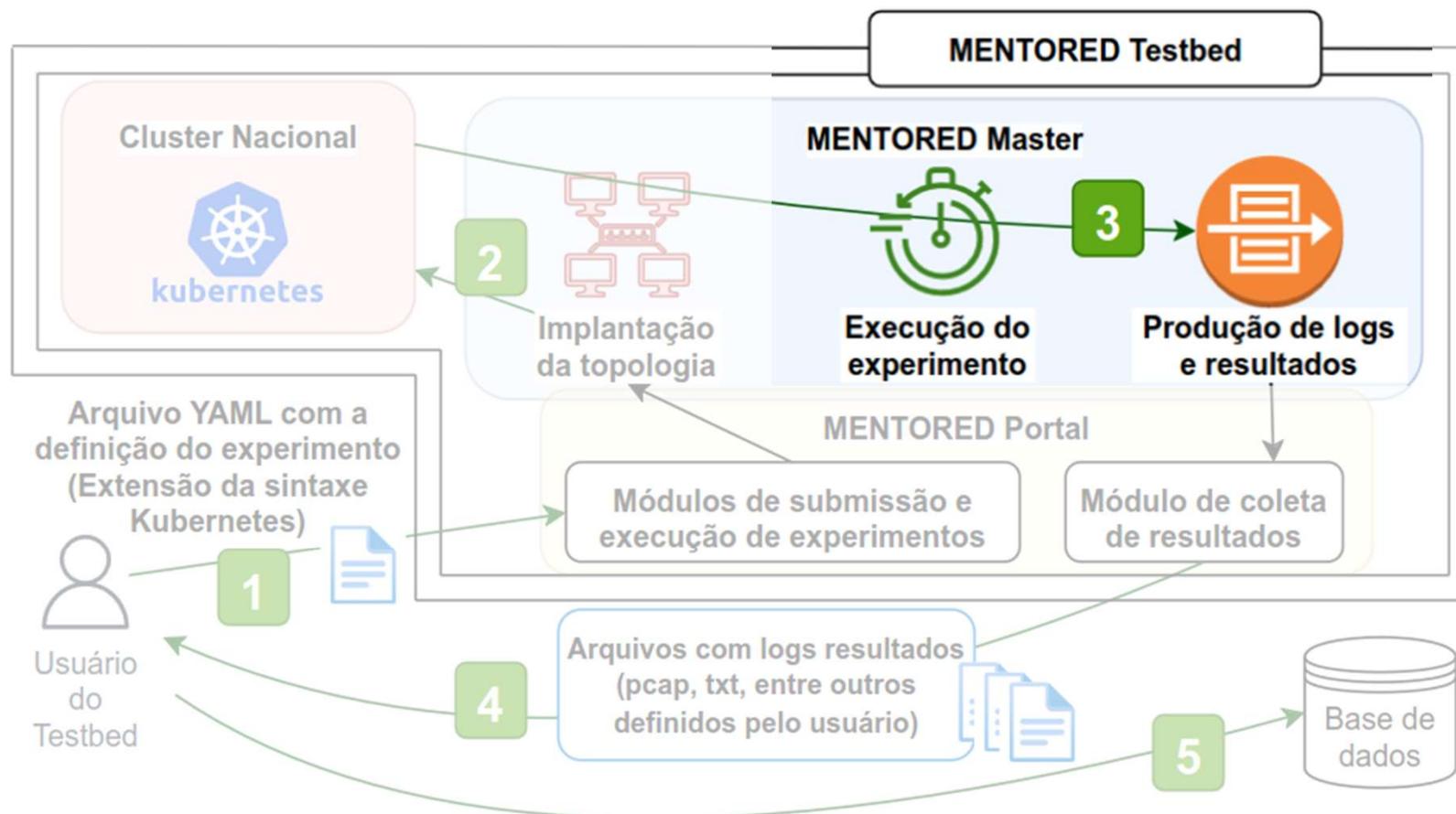
Criando bases de dados



- 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*

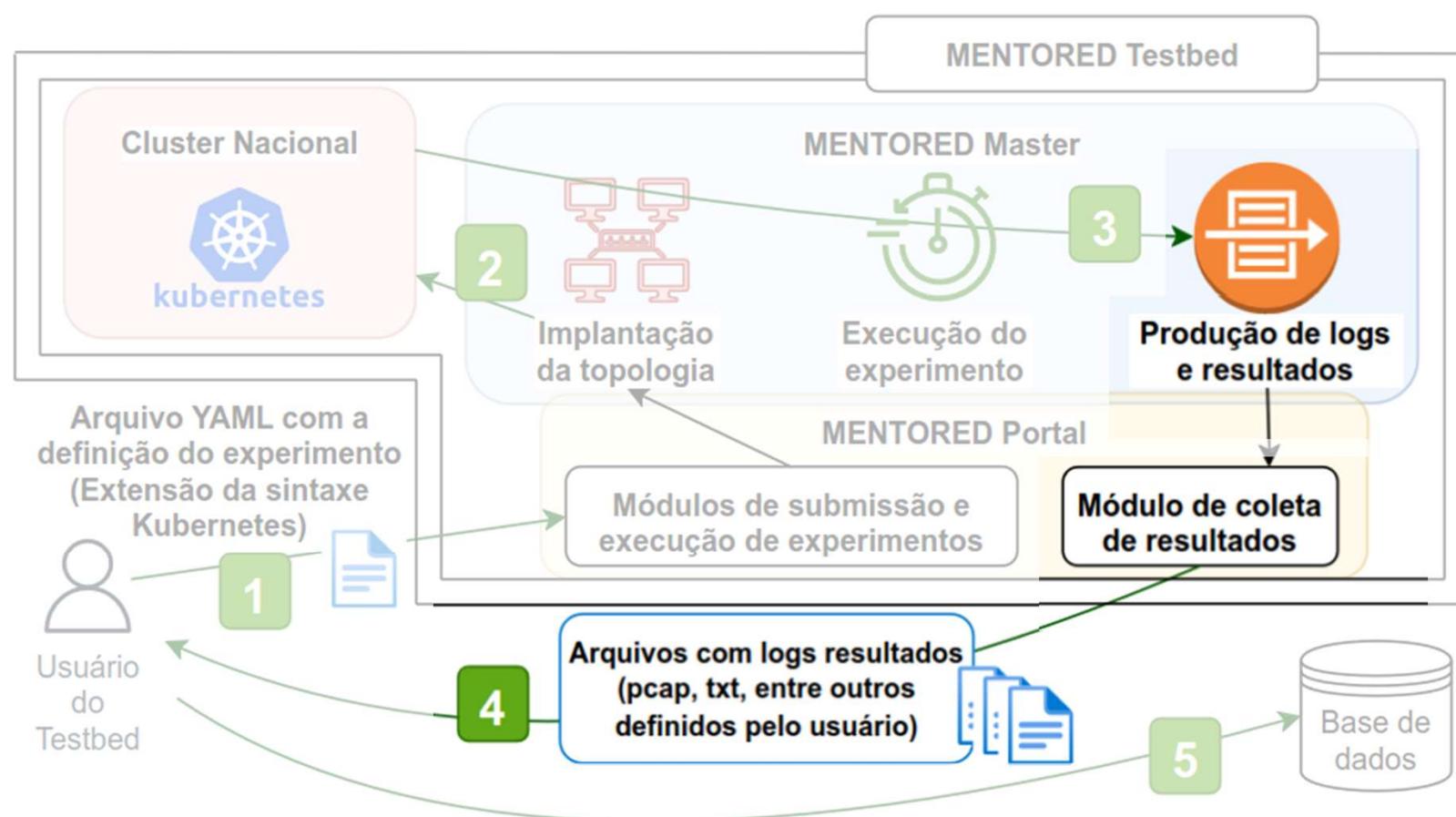
Criando bases de dados



- 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*

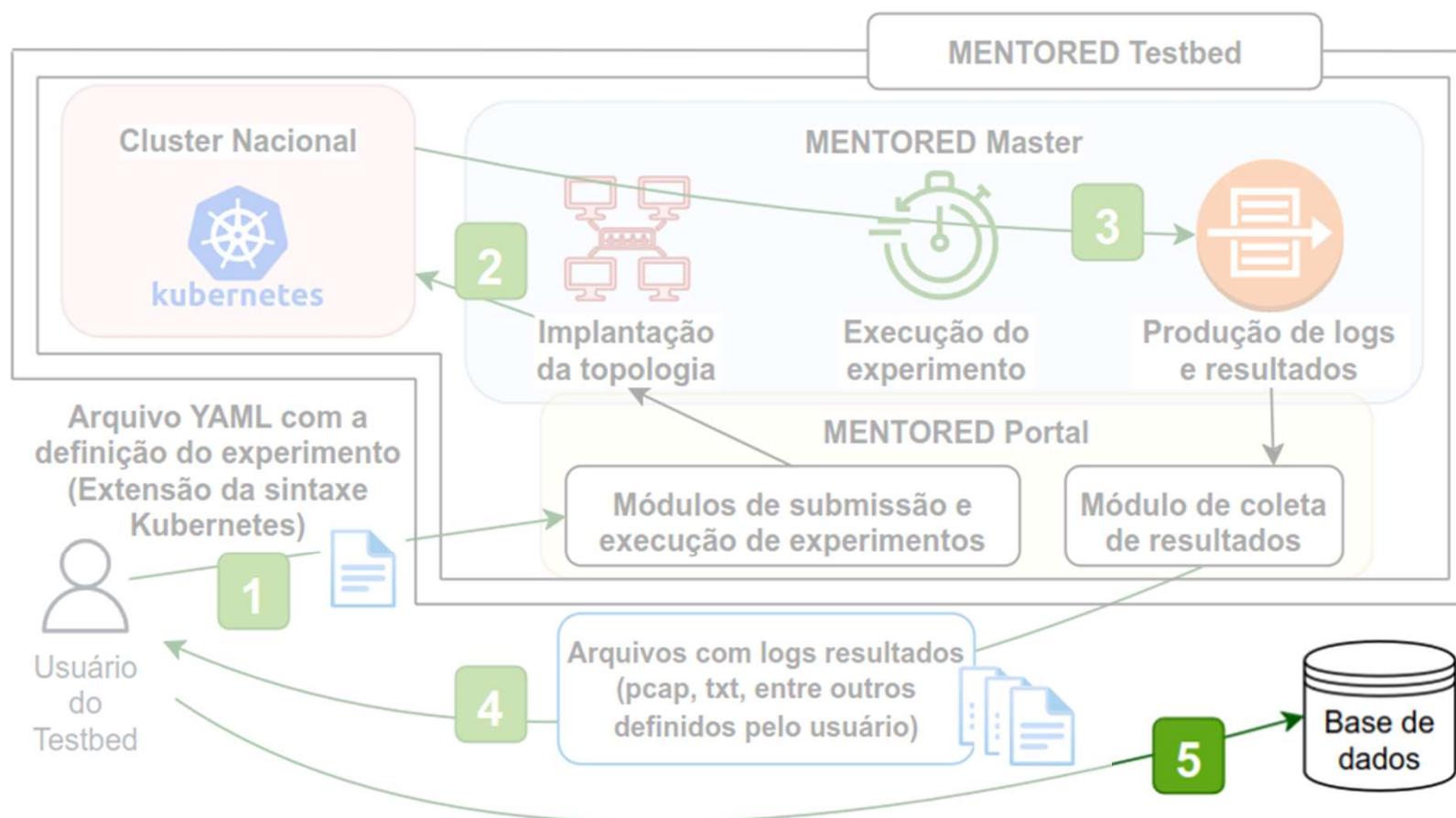
Criando bases de dados



- 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*

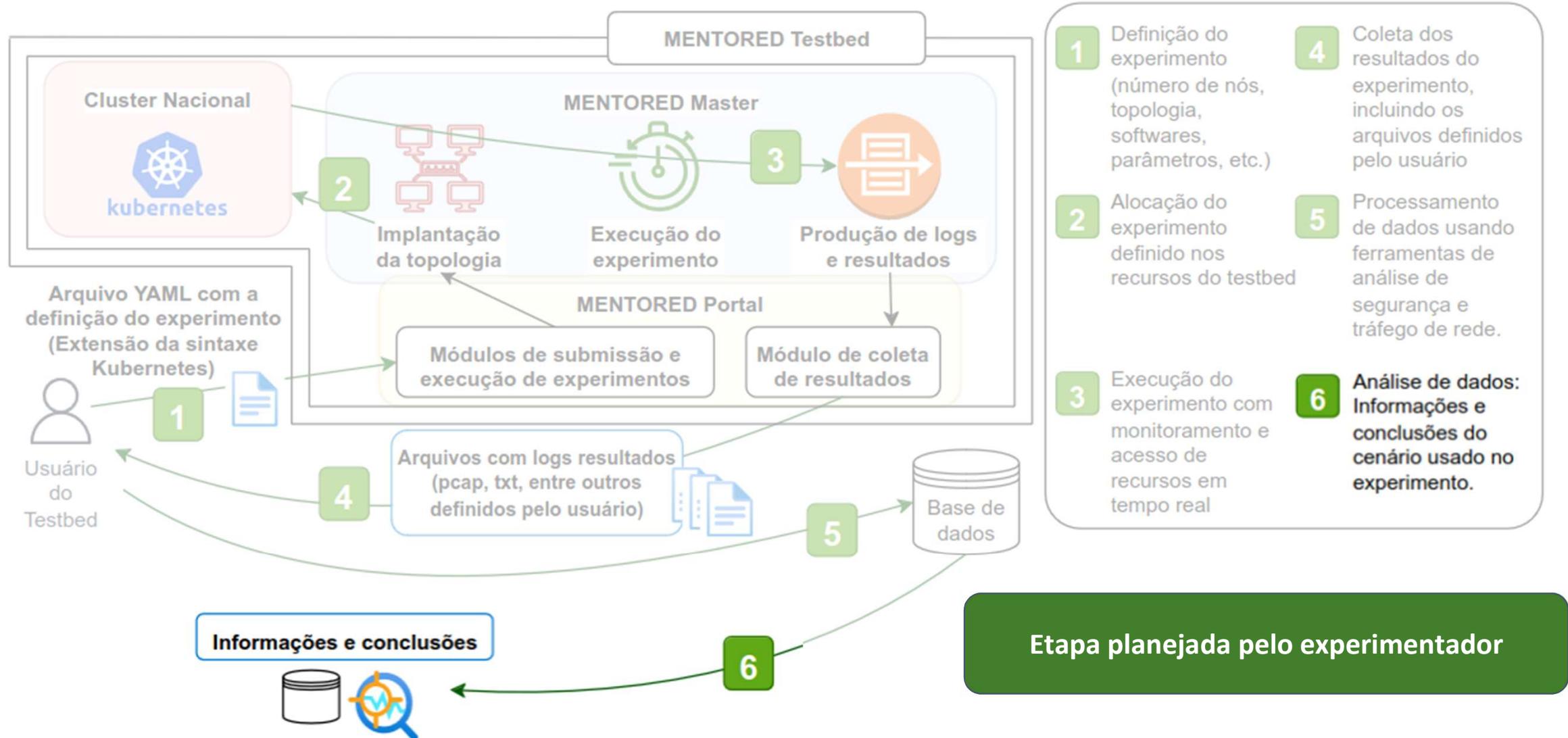
Criando bases de dados



- 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*

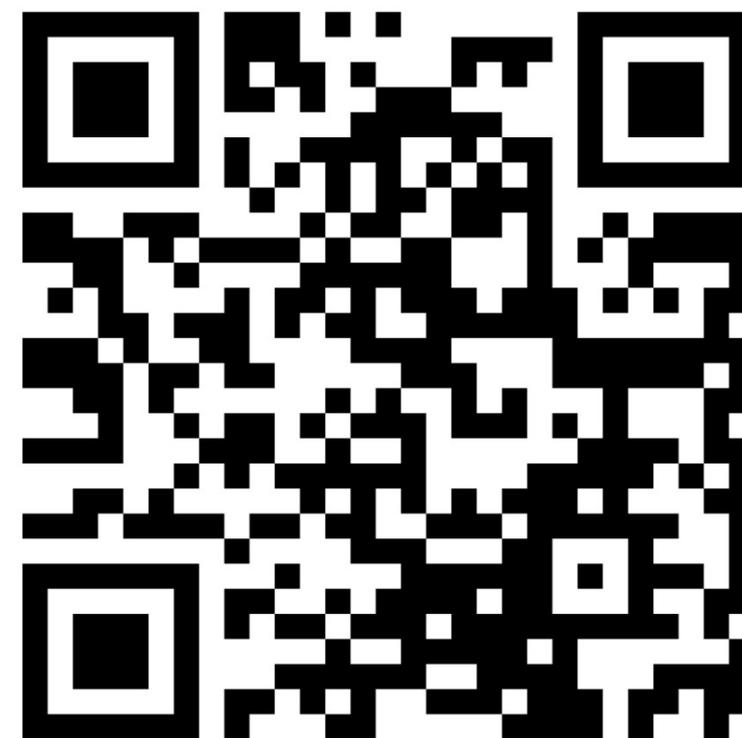
Criando bases de dados



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. Wingham



MENTORED *Testbed*

Telas - *Dashboard*

The dashboard interface for MENTORED Testbed features a dark blue header with the logo on the left and user information on the right. The user is identified as 'Aluno' with the email 'Aluno.Gidlab@Idp3.Cafeexpresso.Rnp.Br'. The main content area is light blue and includes a sidebar with navigation buttons: 'Início', 'Projetos', 'Pedidos de projetos', and 'Configurações'. The central area is divided into several sections: a 'Notícias' (News) section with a welcome message; a 'Tutorial' section with a link to the user manual; a grid of project cards showing details for 'Project 1' with various experiments and their 'Finished' status; and a bottom row of red cards displaying experiment IDs and names, each with a visibility icon.

MENTORED TESTBED

Aluno
Aluno.Gidlab@Idp3.Cafeexpresso.Rnp.Br

Início
Projetos
Pedidos de projetos
Configurações

Notícias
Bem-vindo(a) ao MENTORED Testbed!
Futuras atualizações e notícias serão notificadas neste cartão.

Tutorial
Se você tiver dúvidas sobre como usar o Mentored Testbed, você pode seguir o tutorial disponível em portal.mentored.cpsc-research.org/tutorial/.

Projeto: Project 1
Experimento: slowloris-sbrc-final
Status: Finished

Projeto: Project 1
Experimento: slowloris-sbrc-final
Status: Finished

Projeto: Project 1
Experimento: slowloris-sbrc-final
Status: Finished

Projeto: Project 1
Experimento: hping-sbrc-final
Status: Finished

ID do Experimento: 94
Nome: slowloris-sbrc-final

ID do Experimento: 93
Nome: hping-sbrc-final

ID do Experimento: 81
Nome: test-server-and-ubuntu

ID do Experimento: 80
Nome: new-hping-2

MENTORED *Testbed*

Telas - Projetos

The screenshot displays the MENTORED TESTBED interface. At the top left is the logo and name 'MENTORED TESTBED'. At the top right, there is a notification bell icon, the user's name 'Aluno', and an email address 'Aluno.Gidlab@ldp3.Cafeexpresso.Rnp.Br'. Below the header is a sidebar with four buttons: 'Inicio', 'Projetos' (highlighted in blue), 'Pedidos de projetos', and 'Configurações'. The main content area is divided into two sections: 'Meus Projetos' and 'Projetos Públicos'. Each section has a search bar with the placeholder text 'Escreva algo aqui!'. The 'Meus Projetos' section contains a table with five rows of project data. The 'Projetos Públicos' section contains a table with one row of project data.

| Nome do projeto | Visualizar | Líder do projeto | Apagar |
|-----------------|------------|------------------|--------|
| Project 6 | 👁 | Leader 6 | ✕ |
| Project 7 | 👁 | Leader 7 | ✕ |
| Project 8 | 👁 | Leader 8 | ✕ |
| Project 9 | 👁 | Leader 9 | ✕ |
| Project 10 | 👁 | Leader 10 | ✕ |

| Nome do projeto | Identificador | Visualizar | Líder do projeto | Participar |
|-----------------|---------------|------------|------------------|------------|
| Project 1 | Identifler 1 | 👁 | Leader 1 | ✎ |

MENTORED *Testbed*

Telas - Definição de Experimentos

The screenshot displays the MENTORED TESTBED web application interface. At the top left, the logo and name 'MENTORED TESTBED' are visible. The top right corner shows the user's role as 'Aluno' and their email address 'Aluno.Gidlab@ldp3.Cafeexpresso.Rnp.Br'. A sidebar on the left contains navigation buttons: 'Início', 'Projetos' (highlighted in blue), 'Pedidos de projetos', and 'Configurações'. The main content area features three buttons: 'Projeto 1', 'Membros', and 'Nova Definição'. Below these is a search bar with the placeholder text 'Escreva algo aqui!'. The central part of the interface is a table titled 'Definições De Experimentos' with the following structure:

| Nome do experimento | Visualizar | Editar | Apagar |
|---------------------|------------|--------|--------|
| Experiment 1 | | | |
| Experiment 2 | | | |
| Experiment 3 | | | |
| Experiment 4 | | | |
| Experiment 5 | | | |
| Experiment 6 | | | |

At the bottom of the page, there are logos for various institutions: UFZG, USP, UNICAMP, UNIFESP, UNINOVE, USP, and Instituto Testbed. There are also flags for the United States and Brazil, and logos for MCTIC, egi.br, and FAPESP.

MENTORED *Testbed*

Telas - Monitoramento em Tempo Real

The screenshot displays the MENTORED TESTBED interface. The top navigation bar includes the logo, the text 'MENTORED TESTBED', a notification bell, the user name 'Aluno', the email 'Aluno.Gidlab@dp3.Cafeexpresso.Rnp.Br', and a profile icon. A left sidebar contains buttons for 'Início', 'Projetos', 'Pedidos de projetos', and 'Configurações'. The main content area is titled 'Pods' and features a search bar with the placeholder text 'Escreva algo aqui!'. Below the search bar are three buttons representing pods: 'mentorednetworking156-2-mentored-generic-client-0', 'mentorednetworking156-2-mentored-generic-client-1', and 'mentorednetworking156-2-mentored-generic-client-2'. A terminal window is open on the right, showing the following output:

```
Welcome to Web Kubectl, try kubectl --help.
root@mentorednetworking156-2-mentored-generic-client-0
:/# ls
MENTORED_ENV.source          dev      proc
MENTORED_IP_LIST.json       entry.sh root
MENTORED_IP_LIST.yaml       etc      run
MENTORED_READY              home     sbin
bin                          lib      srv
boot                        lib64    sys
client_delay.csv            media    tmp
client_web_metrics.py       mnt      usr
create_env_from_mentored_ip_list.py  opt      var
root@mentorednetworking156-2-mentored-generic-client-0:/#
█
```

At the bottom of the interface, there is a status bar with 'Execução 137', a mobile device icon, a download icon, and a close icon. The footer contains logos for UFPA, UNPA, UNIVALI, USP, and MCTIC, along with the flags of the United States and Brazil, and the CGI logo.