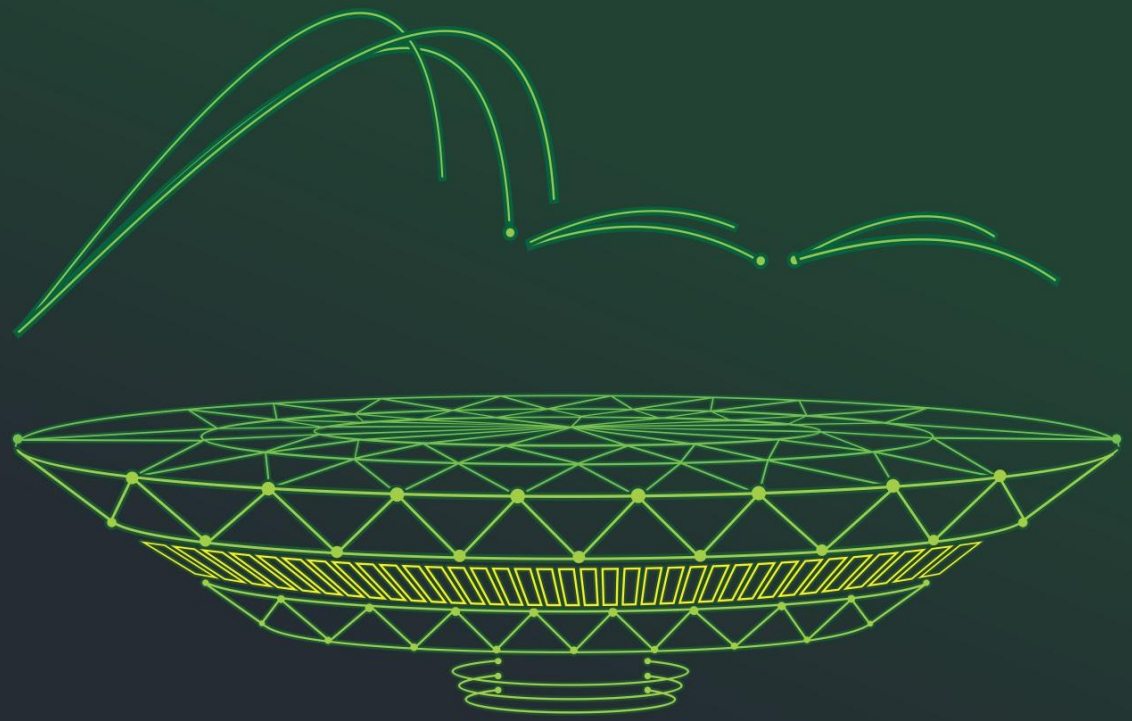
Testbeds para Pesquisa Experimental em Cibersegurança: Da Teoria à Prática

Apresentadores:

- Michelle S. Wangham
- Bruno H. Meyer
- Davi D. Gemmer
- Khalil G. Q. de Santana
- Luiz Eduardo Folly de Campos
- Emerson Ribeiro de Mello



SBRC'24

Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos.

Autores deste minicurso

https://mentored.dcc.ufmg.br

- Profa. Michelle Silva Wangham, Dra. (RNP/Univali)
- Bruno H. Meyer, Me. (UFPR)
- Davi D. Gemmer, Me. (RNP)
- Khalil G. Q. de Santana (Univali)
- Lucas Rodrigues Frank, Me. (UFJF)
- Luiz Eduardo Folly de Campos (RNP)
- Prof. Emerson Ribeiro de Mello, Dr. (IFSC)
- Marcos Felipe Schwarz, Me. (RNP)

Introdução
Objetivo geral deste minicurso

Apresentar *testbeds* em cibersegurança, com destaque ao MENTORED *Testbed*, com o qual serão conduzidos experimentos práticos de DDoS

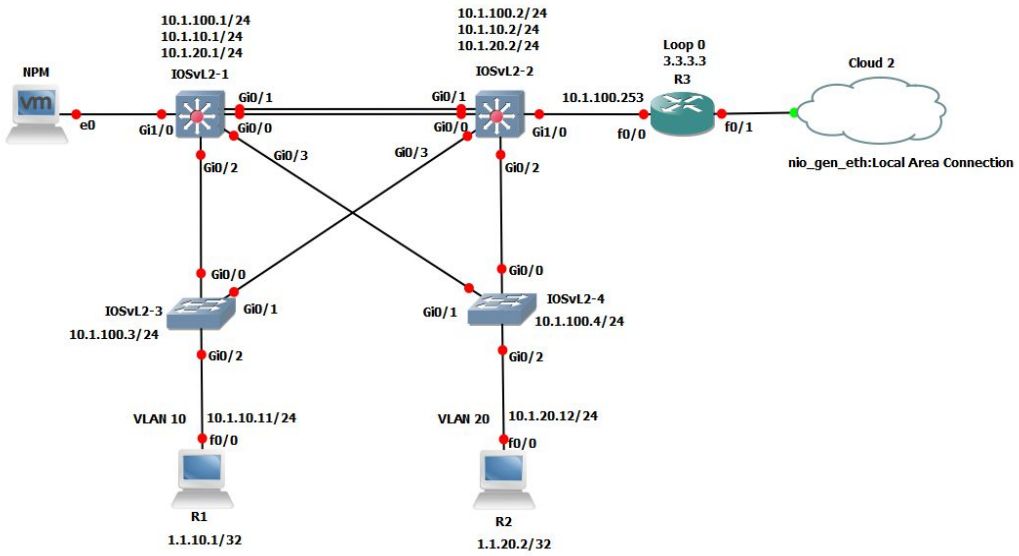
- Desafios e requisitos para *testbeds* de cibersegurança
- *Cluster* Nacional RNP e *testbeds* de cibersegurança na literatura
- MENTORED *Testbed*
- Prática com o MENTORED em dois estudos de caso

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

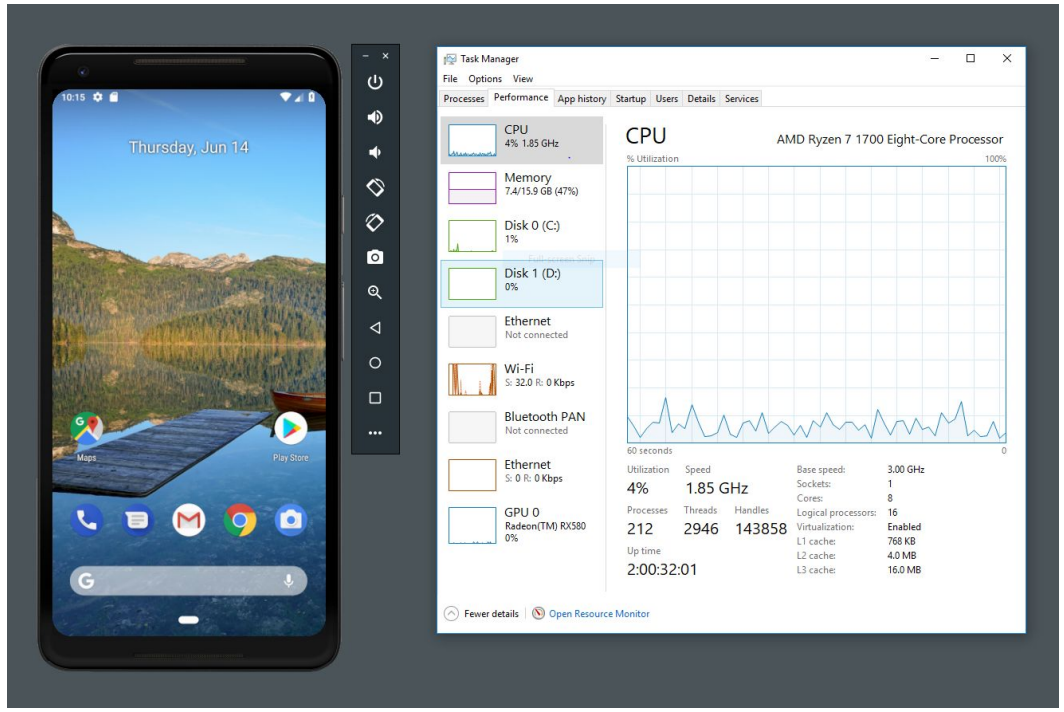
- **Simuladores**
  - Ambientes virtuais que replicam cenários reais
- **Emuladores**
  - Replicam o comportamento de software e hardware
- ***Testbeds***
  - Reproduzem uma infraestrutura de rede e sistemas de informação
  - Realismo e fidelidade



Fonte: https://gns3.com

Ambientes de experimentação em cibersegurança

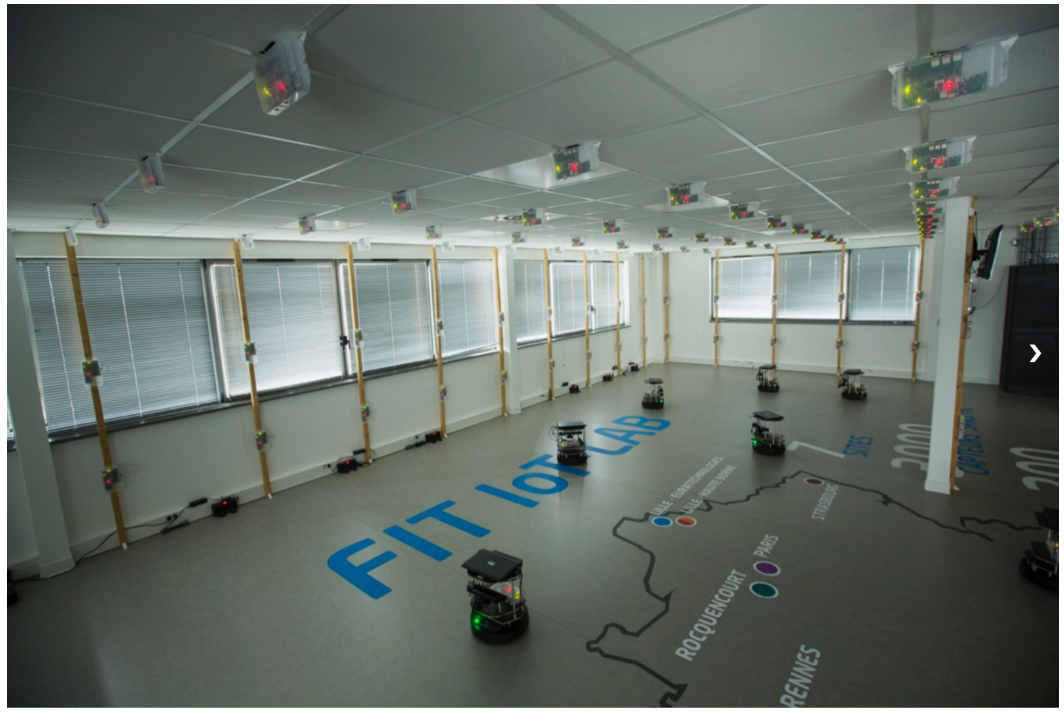
- **Simuladores**
  - Ambientes virtuais que replicam cenários reais
- **Emuladores**
  - Replicam o comportamento de software e hardware
- ***Testbeds***
  - Reproduzem uma infraestrutura de rede e sistemas de informação
  - Realismo e fidelidade



Fonte: https://developer.android.com

Ambientes de experimentação em cibersegurança

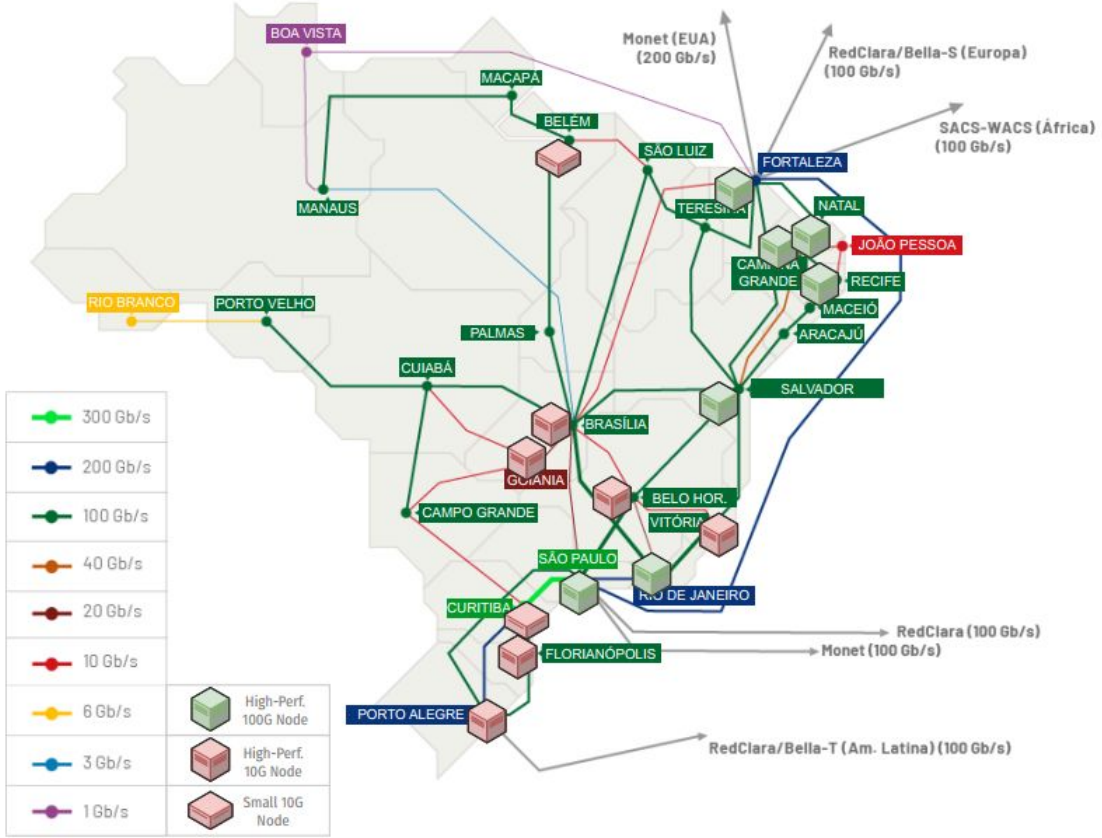
- **Simuladores**
  - Ambientes virtuais que replicam cenários reais
- **Emuladores**
  - Replicam o comportamento de software e hardware
- ***Testbeds***
  - Reproduzem uma infraestrutura de rede e sistemas de informação
  - Realismo e fidelidade



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

Desafios para conduzir experimentos em cibersegurança

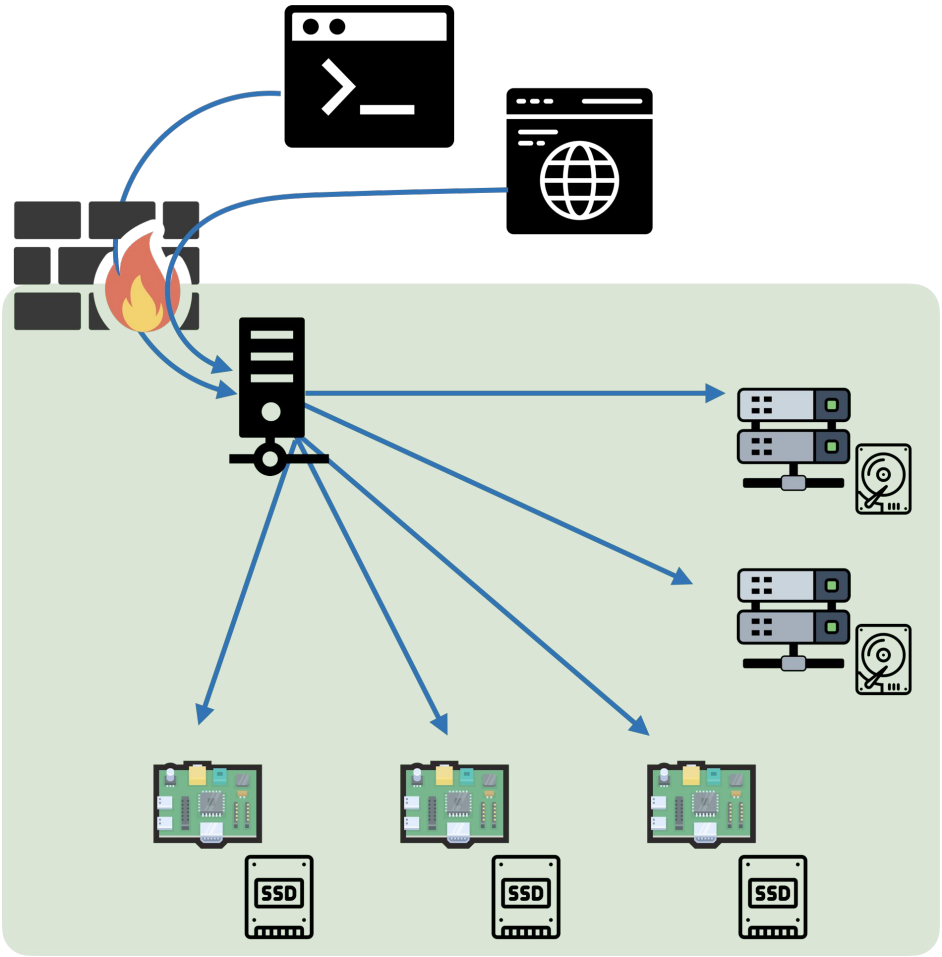
- **Gerenciamento de recursos geograficamente distribuídos**
  - Agendamento e sincronização por todos os dispositivos
- **Capacidade dos dispositivos e dos enlaces**
  - Limita o tipo de experimento ou número de experimentos em paralelo
- **Automatização e orquestração para início e término dos experimentos**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



Fonte: RNP

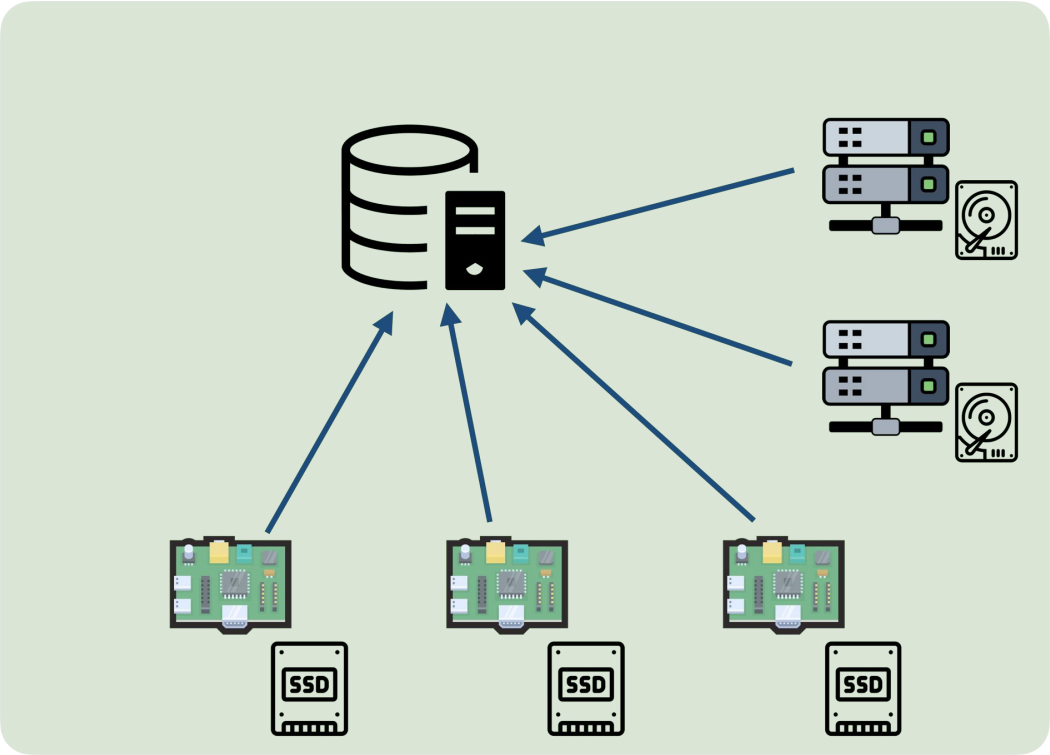
Desafios para conduzir experimentos em cibersegurança

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



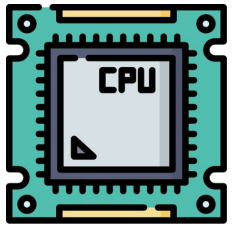
Desafios para conduzir experimentos em cibersegurança

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

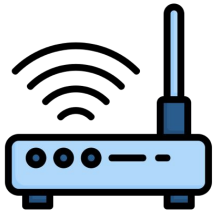


Requisitos de *testbeds* de cibersegurança

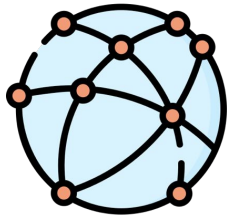
- **Fidelidade**
  - Replicar com precisão ambiente alvo do estudo
- **Flexibilidade**
  - Adaptar para diferentes cenários e experimentos



ARM
x86-64



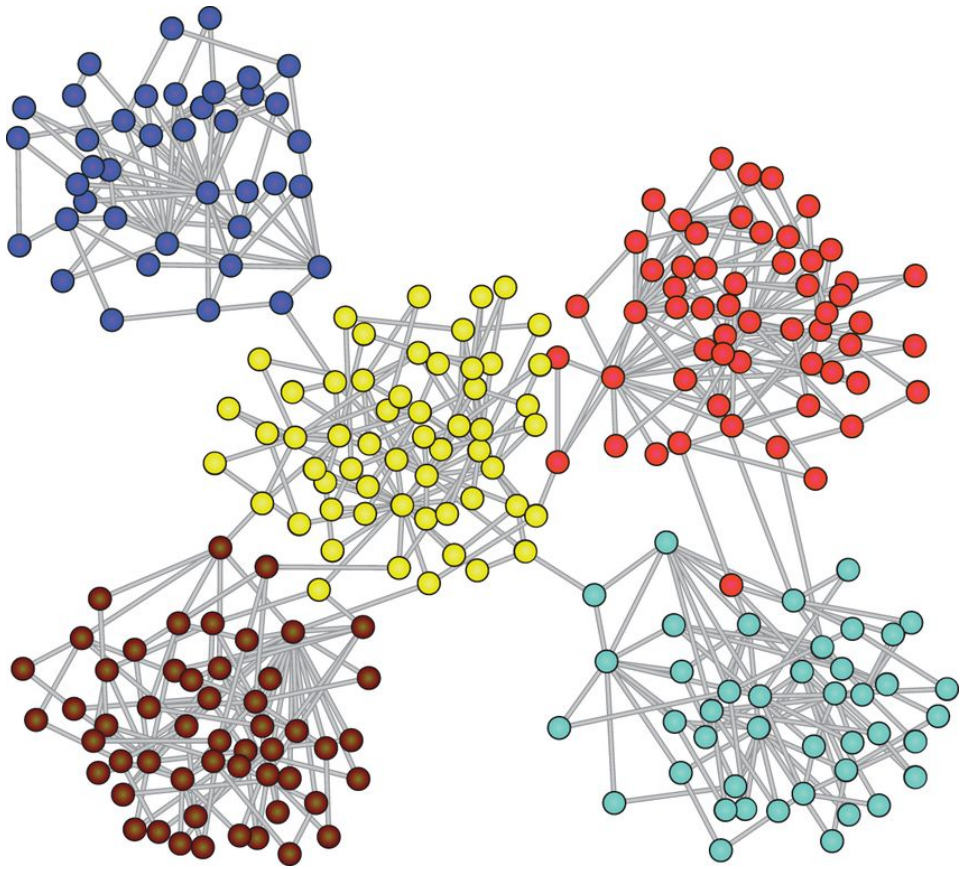
WiFi
802.15.4



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

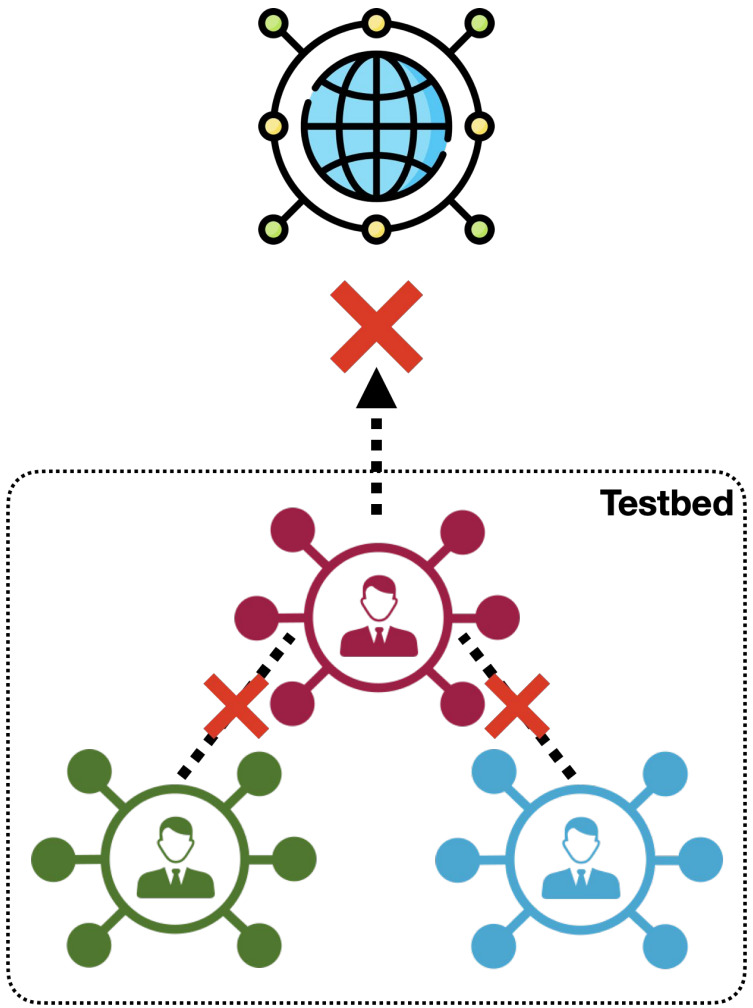
Requisitos de *testbeds* de cibersegurança

- **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



Testbeds para Experimentação

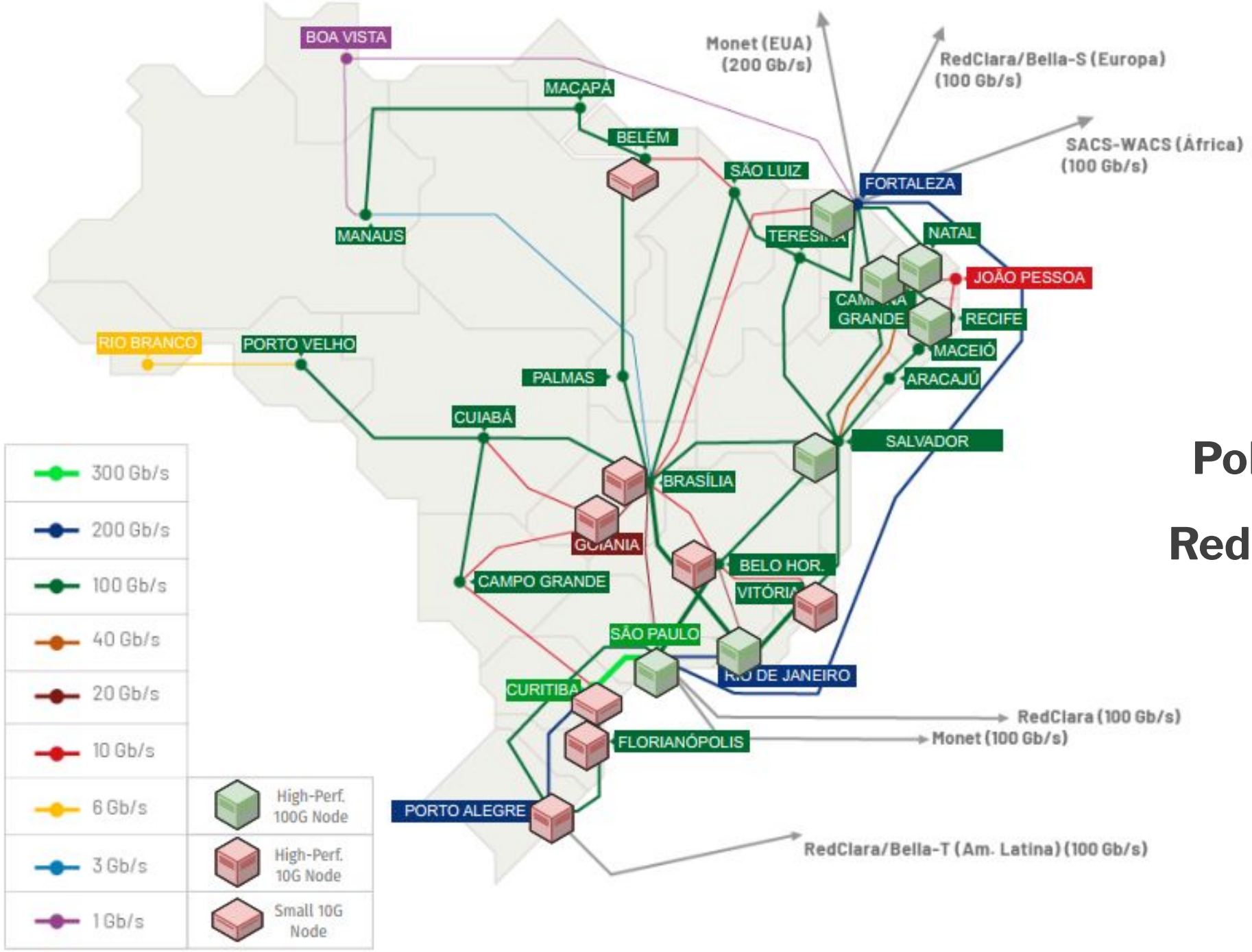
Testbeds para experimentação

- Cluster Nacional
- DeterLab e MergeTB
- FIT IoT LAB
- Gotham Testbed
- GENI e FABRIC
- Fed4Fire+
- Testbeds para geração de datasets
  - TON_IOT
  - Bot_IoT

Cluster Nacional RNP

- **Infraestrutura de computação em nuvem distribuída**
  - Experimentos remotos para pesquisa em TIC.
  - Servidores em PoPs RNP, até 12 capitais do Brasil.

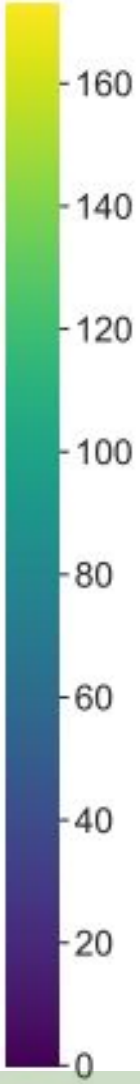
- **Conectividade**
  - Conectividade via Backbone RNP
  - Links de 10 e 100Gbps
  - Latências geográficas “reais”



PoPs e Rede IPÊ

Heatmap de Latências

De \ Para	AC	AL	AM	AP	BA	CE	DF	ES	GO	MA	MG	MS	MT	PA	PB	PE	PI	PR	RJ	RN	RO	RR	RS	SC	SE	SP	TO
AC	0	61	98	92	52	89	36	87	32	86	54	29	20	106	72	94	86	47	52	96	7	173	55	50	92	46	63
AL	61	0	60	66	9	21	26	21	30	38	27	43	41	52	6	3	32	41	30	8	54	79	49	45	5	35	34
AM	98	61	0	15	52	56	35	62	38	43	45	52	50	28	62	64	49	56	58	64	63	43	74	60	56	51	43
AP	95	66	15	0	58	67	38	67	40	59	74	97	117	14	51	66	72	90	57	74	85	25	98	92	59	84	29
BA	111	9	52	57	0	12	18	12	20	29	19	35	33	44	10	12	23	33	42	12	46	62	41	52	4	27	26
CE	89	21	56	67	12	0	30	24	32	13	31	60	79	54	10	24	7	47	51	8	76	91	57	53	16	46	38
DF	36	26	35	38	18	30	0	31	3	22	10	18	15	24	27	29	28	21	24	30	29	67	31	25	21	17	9
ES	88	20	63	67	12	24	31	0	32	46	31	68	103	54	22	24	35	75	58	32	89	92	56	51	16	70	38
GO	33	29	38	40	20	32	3	32	0	25	13	15	12	27	30	32	31	26	24	36	26	56	34	29	24	20	12
MA	86	38	43	59	29	14	22	46	25	0	58	65	92	11	23	51	6	64	52	21	79	83	63	58	38	59	31
MG	54	27	45	74	19	31	10	31	13	58	0	34	42	60	28	30	42	14	10	47	48	104	22	18	23	8	45
MS	29	43	52	97	35	62	18	68	15	65	32	0	9	84	44	71	63	22	32	63	22	84	29	24	64	25	40
MT	20	41	50	117	33	80	15	103	13	92	42	9	0	76	42	102	86	30	40	82	14	141	37	32	95	33	60
PA	106	52	28	14	44	54	24	54	27	11	60	84	76	0	38	53	52	48	43	61	99	38	56	79	45	99	16
PB	62	6	62	51	10	10	27	22	30	23	28	44	42	38	0	3	17	42	29	3	56	69	50	46	10	37	35
PE	94	3	64	66	12	24	29	24	32	51	30	72	102	53	3	0	35	75	40	31	88	90	68	63	8	38	37
PI	86	32	49	72	23	7	28	36	31	6	42	63	86	52	17	34	0	58	58	15	79	103	64	58	27	53	49
PR	46	41	56	90	33	47	21	75	26	64	14	23	30	48	42	75	58	0	12	56	44	141	9	4	67	5	61
RJ	53	30	58	57	42	51	24	58	24	52	10	32	40	43	29	40	58	12	0	60	53	80	21	16	32	7	28
RN	96	8	64	74	12	8	30	32	36	21	47	63	82	61	3	31	14	56	60	0	80	98	62	58	24	53	45
RO	7	54	64	85	46	77	29	89	26	79	48	23	14	72	55	88	79	44	53	80	0	128	51	46	80	46	56
RR	137	78	10	24	73	91	72	104	56	83	98	84	141	43	68	90	96	149	80	99	129	0	86	79	85	81	53
RS	55	49	74	98	41	57	31	56	34	63	22	29	37	56	50	68	64	9	21	62	51	122	0	6	60	14	40
SC	50	45	60	92	52	53	25	51	29	58	18	24	32	79	46	63	58	4	16	58	46	79	6	0	56	9	35
SE	87	5	56	59	4	16	21	16	24	38	23	66	95	45	10	8	27	67	32	23	80	82	60	56	0	61	30
SP	46	35	51	84	27	46	17	70	20	59	8	26	33	99	37	38	53	5	7	53	46	79	14	9	61	0	55
TO	63	34	44	29	26	38	9	38	12	31	45	40	60	16	35	37	49	61	28	45	56	53	40	35	30	55	0



Cluster Nacional RNP

- **Temas de experimentação (ambiente genérico)**
  - **Redes e Redes programáveis (SDN)**
  - **Computação em Nuvem, Edge, e Sistemas Distribuídos**
  - Microsserviços e Funções de Rede (NFV)
  - Redes de Distribuição de Conteúdo (CDN)
  - Orquestração de Recursos
  - Segurança Cibernética
  - Machine Learning
  - IoT - Internet das Coisas
  - Blockchain
  - 5G

Cluster Nacional RNP

- **Recursos Computacionais**
  - Servidores e VMs

Modelo 1

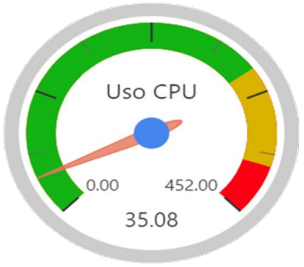
- **CPU: 12+12 = 24 Cores**
- **192 GB RAM**
- **10 TB SSD + 1 TB NVMe**
- **Rede: 2x1G + 2x10G (5 com 100G)**

Modelo 2

- **CPU: 4 Cores / 8 Threads**
- **16 GB RAM**
- **300GB SSD**
- **Rede: 6x1G + 2x 10G**
- **(VMs)**

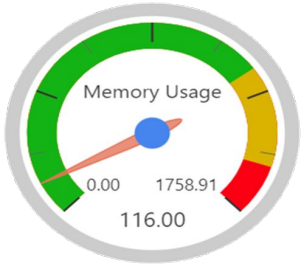
Cluster Nacional RNP

- **Recursos Computacionais**
  - Recursos Totais variáveis



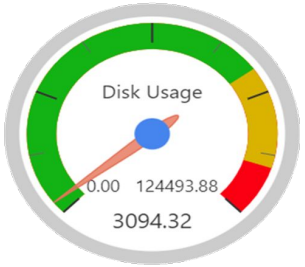
CPUs usadas em Média durante o período (Unidade: CPU)

150+ Cores de CPU



Memória usada no Cluster durante o período (Unidade: Gbytes)

1,2+ Terabytes de Memória RAM



Uso de Disco No Cluster Nacional (Unidade: Gbytes)

100+ Terabytes de Armazenamento

Cluster Nacional RNP

- **Middleware OpenSource**
  - Software preferencialmente OpenSource
  - Comunidades reconhecidas e ativas
  - SO Ubuntu LTS
  - Kubernetes 1.27
  - Componentes adicionais CNCF
    - landscape.cncf.io
    - coredns, ingress-nginx, cert-manager, helm, etc
  - Serviços externos:
    - Armazenamento centralizado, Repositório docker, DNS

Filters | GROUP: Projects and products | Members | Certified partners and providers | Serverless | Wasm | CNAI | VIEW MODE: Grid | Card | ZOOM: - +

App Definition and Development

Application Definition & Image Build

- HELM — CNCF GRADUATED
- Backstage — CNCF INCUBATING
- Buildpacks.io — CNCF INCUBATING
- dapr — CNCF INCUBATING
- KubeVela — CNCF INCUBATING
- KubeVirt — CNCF INCUBATING
- OPERATOR FRAMEWORK — CNCF INCUBATING
- CARVEL
- CHEF HABITAT
- KubePlus
- codezero
- Cyclops
- Daytona
- depot
- Devfile.io
- DevSpace
- Eclipse Che
- fabricB
- Gefyra
- Gitpod
- Glasskube
- Gradle
- itopia
- Kaniko
- Kapeta
- ko
- KONVEYOR
- kots
- KUBERMATIC
- Kui_
- lagoon
- Platform
- MICROCKS
- mirrord
- Nocalhost
- okteto
- Open Application Model
- OPENAPI INITIATIVE
- Packer
- plural
- podman
- Porter
- QUARKUS
- radius
- raftt
- sealer
- ServiceComb
- SHIPWRIGHT
- SKAFFOLD
- squash
- Tanka
- TILT
- vmware Application Catalog
- Walrus

Continuous Integration & Delivery

- argo — CNCF GRADUATED
- flux — CNCF GRADUATED
- keptn — CNCF INCUBATING
- OpenKruise — CNCF INCUBATING
- agola
- AKUITY
- AppVeyor
- Bamboo
- BRIGADE
- Buildkite
- Bytebase
- circleci
- Skycap
- CloudBees
- codefresh
- Concourse
- D2IQ Dispatch
- devtron
- flagger
- GitLab
- gitness
- go
- harness
- HELMWAVE
- hyscale
- Jenkins
- JENKINS X
- k6
- Keploy
- Liquibase
- Mergify
- Northflank
- OpenGitOps
- OpsMx
- ozone
- PipeCD
- Razee
- semaphore
- spacelift
- Spinnaker
- TeamCity
- TEKTON
- Travis CI
- unleash
- weaveworks
- werf
- DEPLOY
- kube-burner

Database

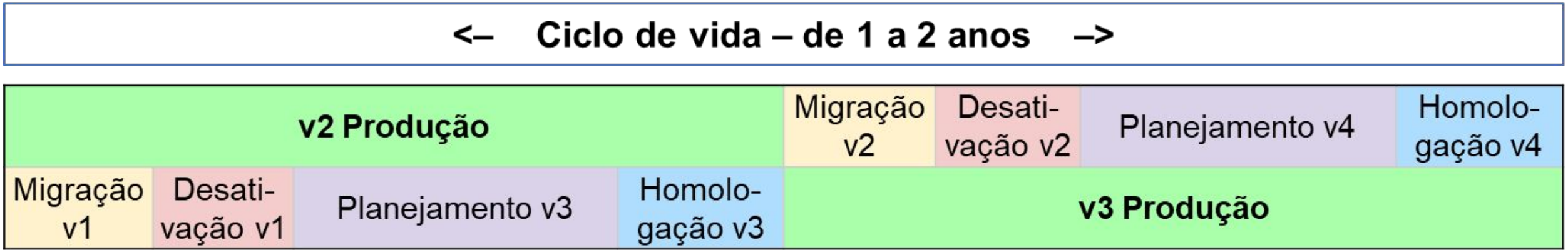
- KV — CNCF GRADUATED
- Vitess — CNCF GRADUATED
- CarbonData
- Ignite
- ArangoDB
- BIGCHAIN
- cassandra
- ClickHouse
- CockroachDB
- Cockroach Labs
- Couchbase
- CRATE.IO
- crunchydata
- CRUX
- Databend
- Dgraph
- DORIS
- Dragonfly
- druid
- EDB
- Epsilla
- FoundationDB
- GraphScope
- GrapheneDB
- IBM DB2
- Iguazio
- infinispan
- InterSystems
- KB
- KUBEBLOCKS
- KubeDB
- MariaDB

Streaming & Messaging

- cloudevents — CNCF GRADUATED
- NATS — CNCF INCUBATING
- STRIMZI — CNCF INCUBATING
- HERON
- nifi
- Spark
- STORM
- Azure Event Hubs

Cluster Nacional RNP

- **Ciclo de Vida**
  - Estratégia Blue/Green
  - SO, dependências
  - K8s, container engine
  - Componentes CNCF, e configs



Cluster Nacional RNP

- **Personalização**
  - Equipamentos - IoT, Switches P4, Sensores
  - Configurações - K8s e componentes CNCF
  - Componentes sob demanda
  - Aplicações externas sob demanda
- **Conetividade**
  - Conectividade entre aplicações via plugins de rede k8s
  - Calico (padrão) e Multus
  - MacVlan + VXLAN ou EVPN sobre a rede IPÊ

Cluster Nacional RNP

- **Ferramentas adicionais:**
  - Monitoramento:
    - Netdata
    - Dashboard K8s
    - Kube-Prometheus-Stack + Grafana
  - Armazenamento centralizado com FTP
  - Repositório privado de imagens de containers
  - DNS externo (.ids.rnp.br)

Cluster Nacional RNP

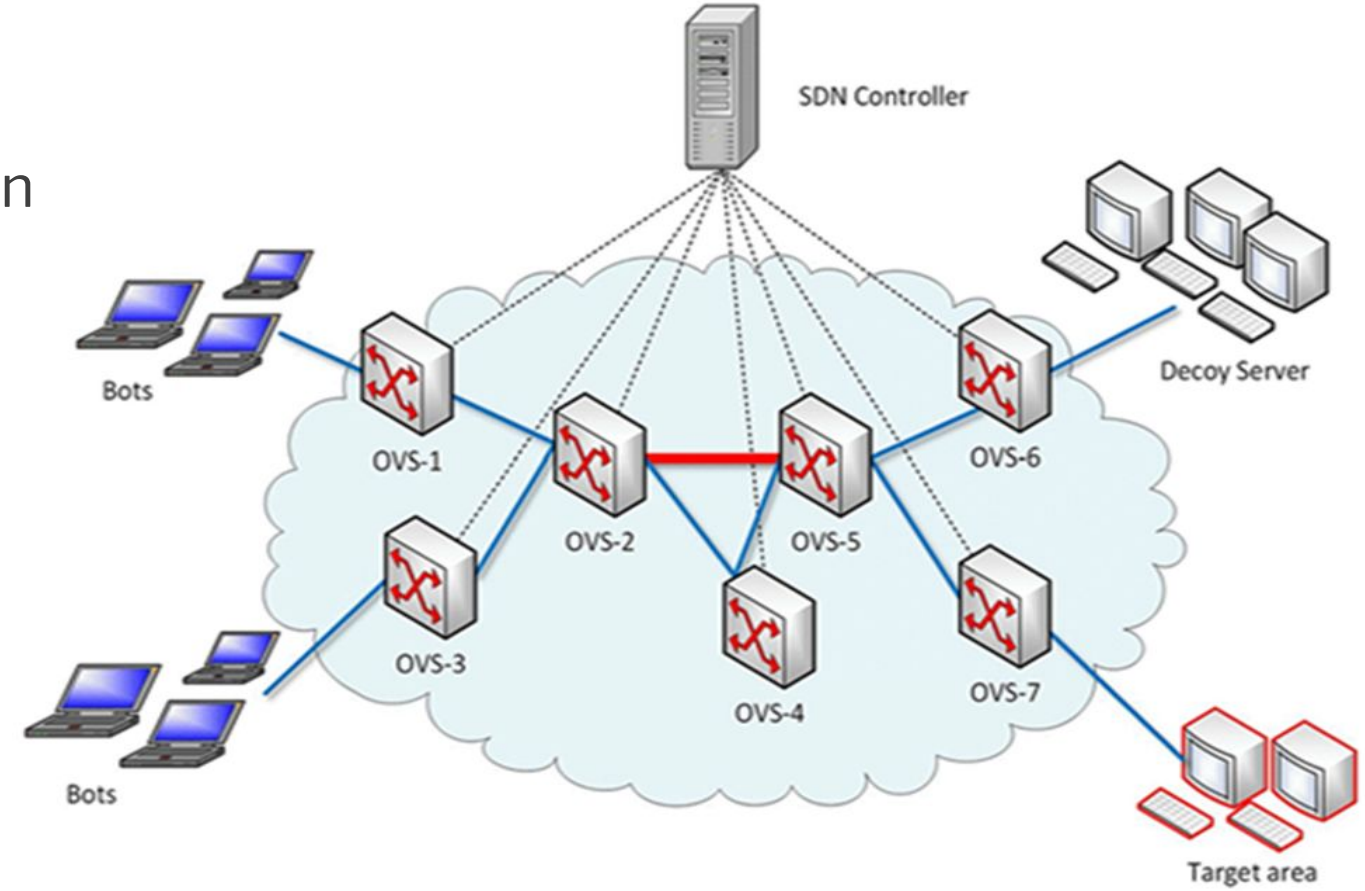
- **Acesso e uso**
  - Testbed “up” 24/7
  - Acesso via Bastion RNP ou diretamente na API
  - Fatia (slice): 1+ namespace por usuário, via credenciais
  - Hierarchical namespaces - subdivisão da fatia
  - Garantia Mínima de recursos dedicados, para disponibilidade
  - Limite Máximo de recursos em utilização, evitando sobrecarga
  - Aplicações publicadas como serviço
  - Implantação Seletiva e uso de Labels K8s

Cluster Nacional RNP

- **Caso de Uso - KCDN**
  - Pesquisa em CDN Cloud-Native
  - Alocação inteligente de recursos
  - Distribuição geográfica real
  - DNS adicional personalizado
  - Resultados aproveitados no eduplay

Cluster Nacional RNP

- **Caso de Uso - Mentored**
  - Pesquisa em Ataques DDoS
  - Conectividade via EVPN/MacVlan
  - Cibersegurança em IoT
  - Boa quantidade de recursos



Testbeds de cibersegurança
DeterLab

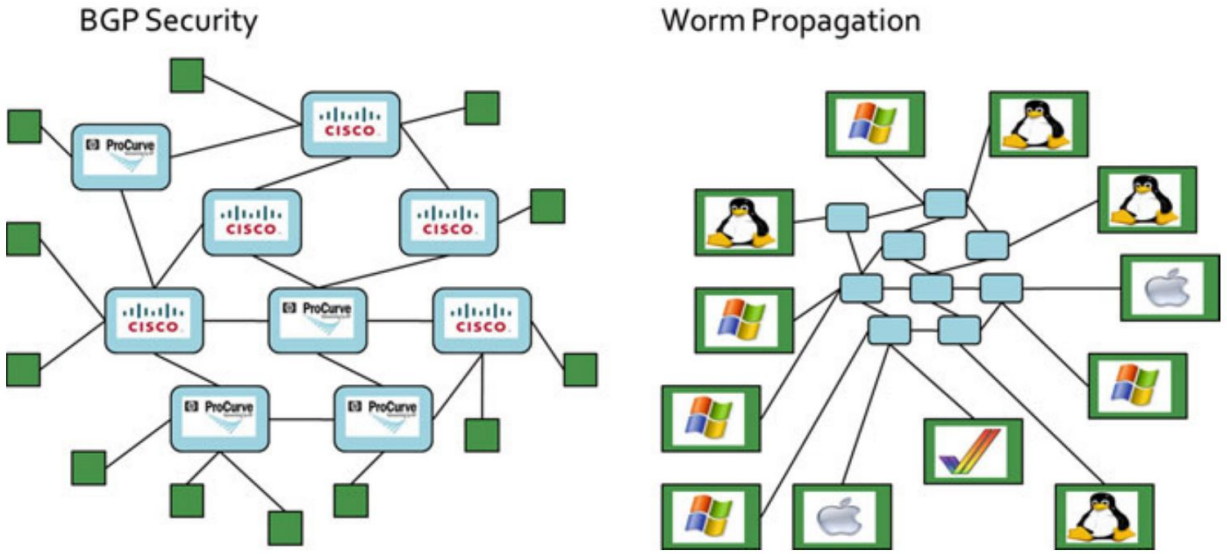
- Em 2004 surge o DeterLab
- **Foco atual**: Uso didático
- **Origem**:
  - Software: baseado no Emulab (modificado)
  - Desenvolvimento: Universidade de Utah, EUA
  - Financiamento:
    - DHS - *US Department of Homeland Security*
    - NSF - *National Science Foundation*
    - DARPA - *Defense Advanced Research Projects Agency*

Testbeds de cibersegurança
DeterLab

- *Testbed* influente
  - +2600 usuários
  - Usado por 47 instituições, em 6 países
- Contêm exercícios prontos
  - Introdução ao Linux e ao *testbed*
  - Ataques de injeção SQL
  - Configuração de *firewalls*
  - Ataques DDoS
  - Interceptação de tráfego (MiTM)

Testbeds de cibersegurança
DeterLab

- **Fidelidade**
  - Representação de dispositivos variável:
    - Dispositivos Físicos
    - Máquinas Virtuais
    - Contêineres (OpenVZ)
    - Processos virtualizados (ViewOS)
    - Co-rotinas/*threads*



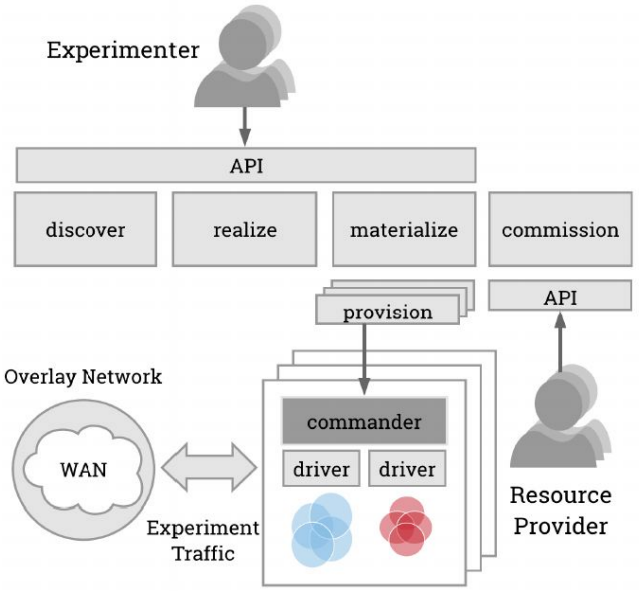
WROCLAWSKI, John et al. DETERLab and the DETER Project. The GENI Book, p. 35-62, 2016.

Testbeds de cibersegurança
DeterLab + MergeTB

- Evolução do DeterLab, adotando a plataforma MergeTB[1]
- Migração para a infraestrutura do projeto SPHERE
- Também financiado pela NSF
- **Foco Atual:** Experimentação

Testbeds de cibersegurança
DeterLab + MergeTB

- **Arquitetura**
  - Conjunto de diversos serviços *stateless*
    - Realizam operações como alocação e instanciação dos recursos solicitados pelo pesquisador
  - '*Drivers*' que realizam manipulações nos recursos, direcionando estes para o estado final desejado
    - Sistema distribuído: utiliza de *locks* para prevenir acesso simultâneo



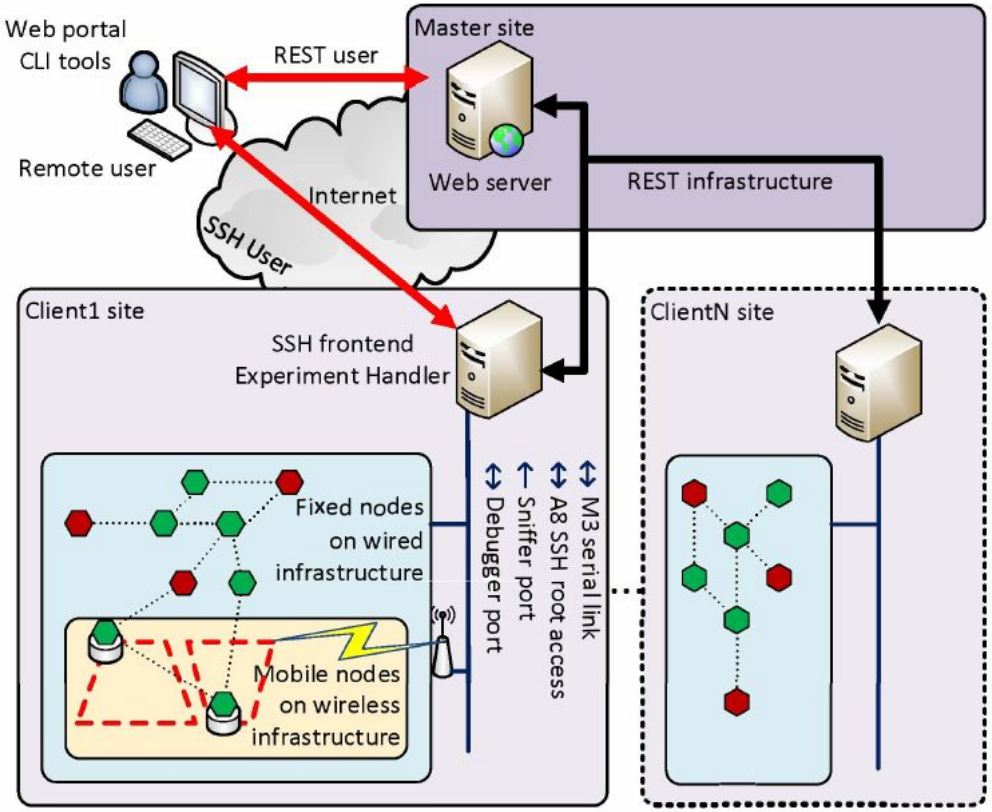
GOODFELLOW, Ryan; THURLOW, Lincoln; RAVI, Srivatsan. Merge: An architecture for interconnected testbed ecosystems. arXiv preprint arXiv:1810.08260, 2018.

Testbeds de cibersegurança
FIT-IoT LAB

- Testbed IoT de larga escala
  - Acesso aberto
  - +1500 dispositivos
  - 6 localidades
- **Foco**: Experimentação IoT
- **Origem**:
  - Universidade de Strasbourg e Universidade de Lyon, França

Testbeds de cibersegurança
FIT-IoT LAB

- Arquitetura com recursos distribuídos
  - Acesso via API REST
  - Acesso via SSH (por intermédio de um *bastion*)
  - Acesso a portas de *debug*
  - *Sniffer* embutido

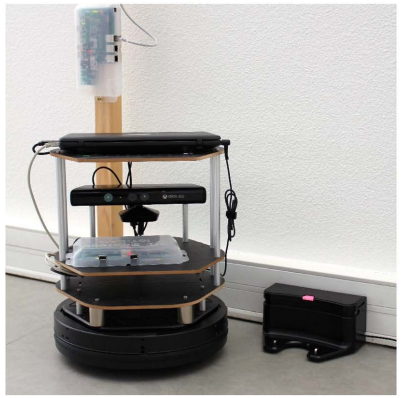


Fonte: ADJIH, Cedric et al. FIT IoT-LAB: A large scale open experimental IoT testbed. In: **2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)**. IEEE, 2015. p. 459-464.

Testbeds de cibersegurança
FIT-IoT LAB

- Dispositivos IoT fixos
  - Em corredores, pilares, etc

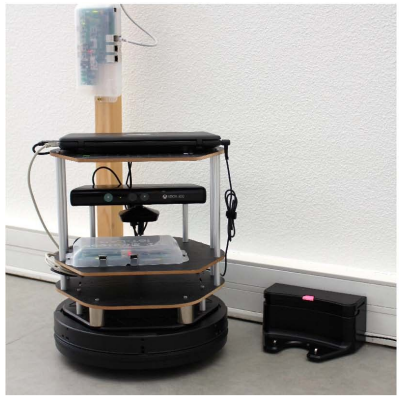
- Dispositivos IoT móveis



ADJIH, Cedric et al. FIT IoT-LAB: A large scale open experimental IoT testbed. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, 2015. p. 459-464.

Testbeds de cibersegurança
FIT-IoT LAB

- Três tipos de dispositivos:
  - ‘**Open Node**’ ⇒ reprogramável pelo usuário
  - **‘Gateway’** ⇒ intermediário para a comunicação entre o Open Node e o Control Node
  - ‘**Control Node’** ⇒ Coordena as atividades de um dispositivo
    - Reprogramação
    - Inicialização, Resets
    - Análise do consumo de energia
    - Inspeção do tráfego de rede
    - Injeção de tráfego de rede



ADJIH, Cedric et al. FIT IoT-LAB: A large scale open experimental IoT testbed. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, 2015. p. 459-464.

Testbeds de cibersegurança
FIT-IoT LAB

- Testbed influente
  - Mais de 500 citações em artigos científicos

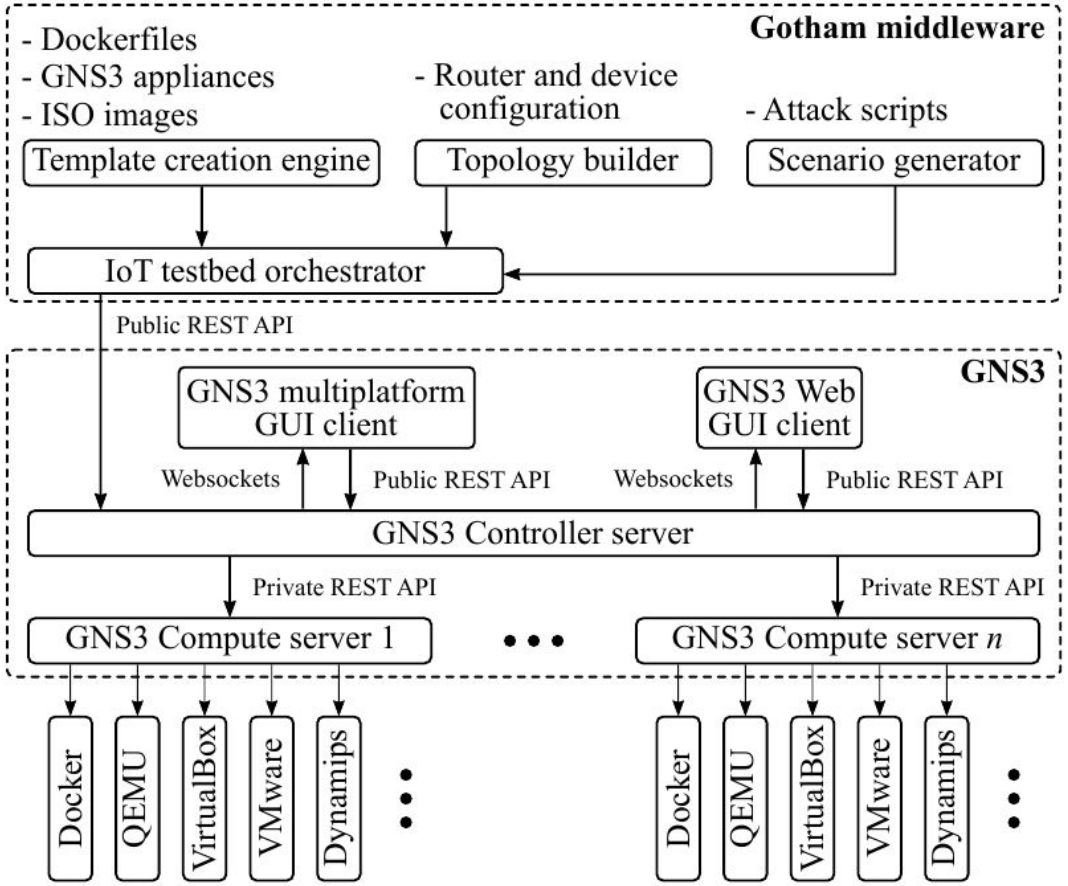
Publications using/citing IoT-LAB **574**

We used Google Scholar to search and list the works that have used IoT-LAB (see our profile).

  - Suporte a diversos protocolos e rádios:
    - IPv6
    - 802.15.4
    - Bluetooth Low Energy
    - Ultra Wide Band (UWB)
    - Sub-GHz

Testbeds de cibersegurança
Gotham Testbed

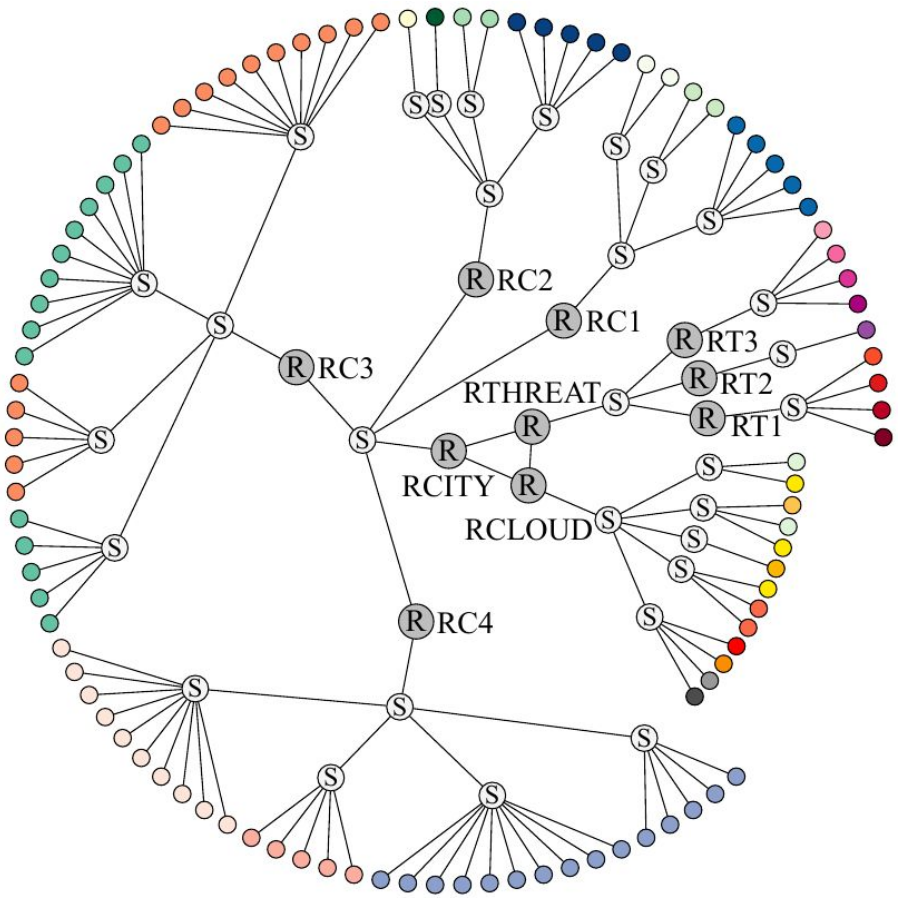
- Proposto em 2023
- **Foco**: Experimentação em segurança, IoT e geração de *datasets*
- **Origem**:
  - Software: Construído sobre o GNS3
  - Universidade de Mondragon, Espanha



Sáez-de-Cámara, X., Flores, J. L., Arellano, C., Urbieta, A., & Zurutuza, U. (2023). Gotham testbed: a reproducible IoT testbed for security experiments and dataset generation

Testbeds de cibersegurança
Gotham Testbed

- Cenário incluso
  - 140 dispositivos, distribuídos em três camadas
    - *Edge* ⇒ Dispositivos IoT e Industrial IoT (100x)
    - *Network* ⇒ Roteadores (10x) e *switches* (30x)
    - *Cloud* ⇒ Serviços auxiliares como DNS e NTP



Sáez-de-Cámara, X., Flores, J. L., Arellano, C., Urbieta, A., & Zurutuza, U. (2023). Gotham testbed: a reproducible IoT testbed for security experiments and dataset generation

Testbeds de cibersegurança
Gotham Testbed

- Aplicações heterogêneas
- Ataques heterogêneos
- 3 *threat actors* com comportamentos distintos

Testbeds de cibersegurança
Gotham Testbed

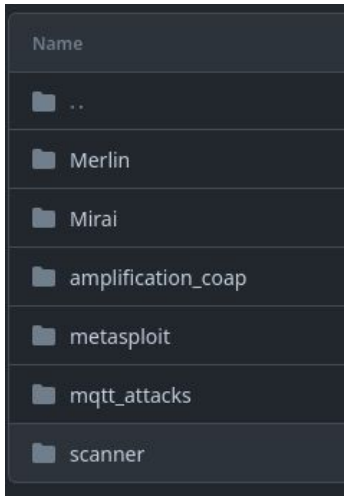
- **Diversos ataques**
  - Tráfego Botnet/C&C (Mirai e Merlin)
  - Varreduras (*Scans*) de rede
  - Ataques de força bruta (usando uma lista de credenciais)
  - Execução de código remoto (RCE)
  - DDoS (10 tipos, incluindo ataques de *flood* UDP, DNS, TCP SYN, TCP ACK, TCP *stomp*, GRE e HTTP)
  - Ataques específicos a protocolos IoT como MQTT e CoAP
  - Transferência de arquivos maliciosos
  - Coleta de dados

Testbeds de cibersegurança
Gotham Testbed

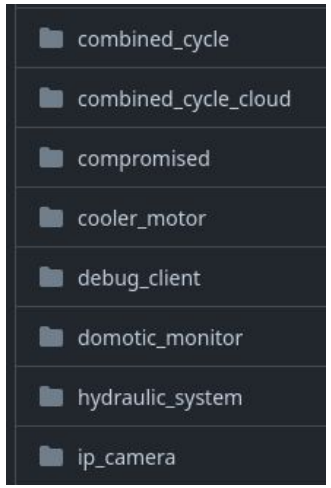
- 4 zonas, com focos em diferentes tipos de dispositivos
  - Museu (Câmeras IP e sensores de monitoramento)
  - *Bristol* (casas com mecanismos de automação residencial)
  - *Rennington* (sensores industriais enviando telemetria para a camada *Cloud*)
  - Central de energia (utilizando outros sensores industriais)

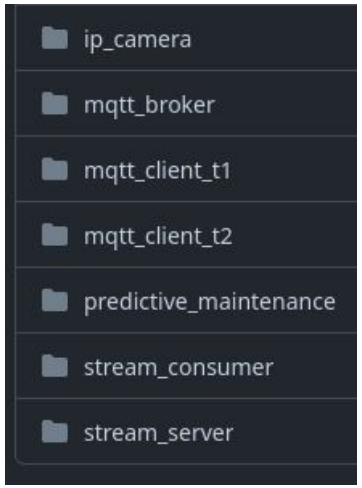
Testbeds de cibersegurança
Gotham Testbed

- Reprodutibilidade:
  - Código fonte disponível
  - Imagens de *containers* (*Dockerfiles*) disponíveis



Botnets e ferramentas de ataque





Dispositivos IoT e IIoT

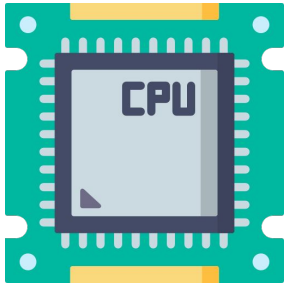
Fonte: https://github.com/xsaga/gotham-iot-testbed/tree/master/

```
FROM fedora:35

RUN dnf install -y \
    python \
#    masscan \
    git \
    gcc \
    make \
    libpcap-devel \
    && dnf clean all \
    && rm -rf /var/cache/yum

RUN rpm -vhU https://nmap.org/dist/nmap-7.92-1.x86_64.rpm

# masscan binary in /masscan/bin/masscan
RUN git clone https://github.com/robertdavidgraham/masscan.git &&\
    cd masscan &&\
    make

CMD ["/bin/bash"]
```

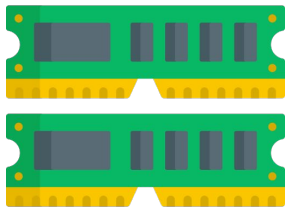
Dockerfile exemplo

Testbeds de cibersegurança
Gotham Testbed

- Fidelidade e flexibilidade
  - Emulação de enlaces
  - Limitação de recursos por dispositivo



Processamento



Memória

Vazão

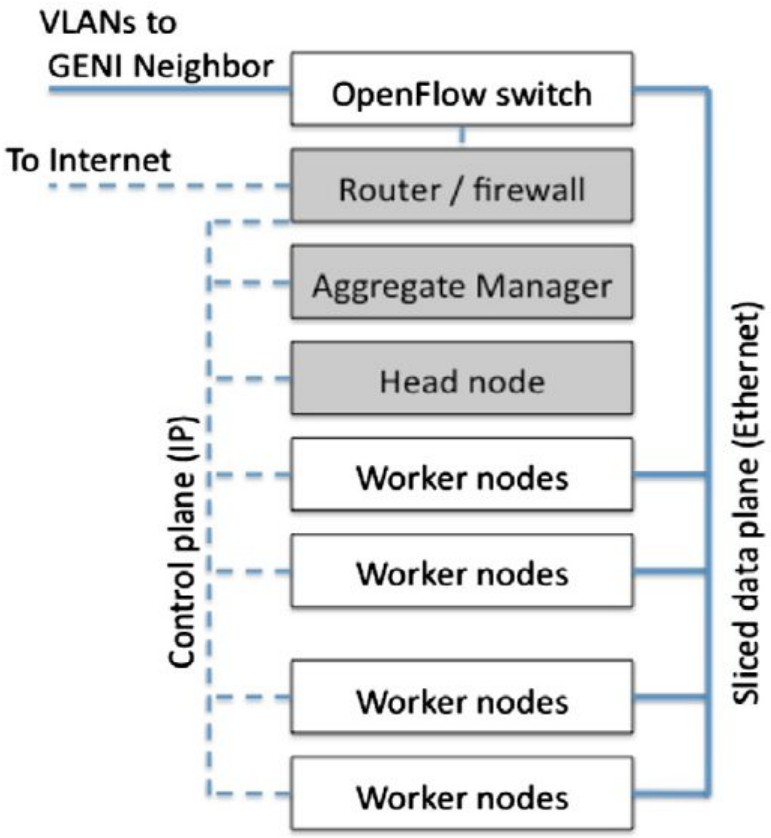
Latência

Testbeds de cibersegurança
GENI e FABRIC

- Foi um *testbed* influente na literatura (servido a comunidade acadêmica por mais de 10 anos)
- 2023: descontinuado e sucedido pelo FABRIC
- Arquitetura GENI:
  - Virtualização e *containers* (Linux VServer, KVM, OpenVZ)
  - Dispositivos físicos
  - SDN utilizando o padrão OpenFlow + VLANs
  - Federação
  - APIs, ferramentas da comunidade

geni
Exploring Networks of the Future

Testbeds de cibersegurança
GENI e FABRIC



BERMAN, Mark et al. GENI: A federated testbed for innovative network experiments. Computer Networks, v. 61, p. 5-23, 2014.

Testbeds de cibersegurança
GENI e FABRIC

FABRIC

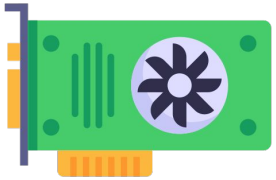
- FABRIC é o novo *testbed* de escala nacional (EUA)
- Objetivo: fornecer infraestrutura programável para experimentos
  - Não somente em dispositivos *edge*, mas também na malha da rede
  - Utilização de ativos de rede com tecnologia P4

Testbeds de cibersegurança
GENI e FABRIC

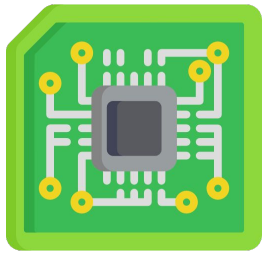
- TeraCore
  - Rede em topologia de anel
  - 1.2Tbps
  - Fibra ótica

Testbeds de cibersegurança
GENI e FABRIC

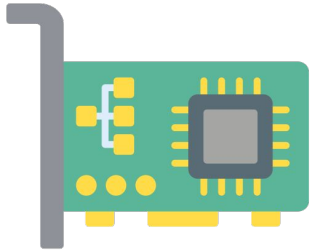
- Recursos disponíveis:
  - Centenas de núcleos
  - Terabytes de RAM



GPUs



FPGAs



SmartNICs

Testbeds de cibersegurança
FED4FIRE+

- O Fed4FIRE+ é um *testbed* europeu que representou uma significativa iniciativa na pesquisa
- **Objetivo**: Aprimorar a integração e federação dos *testbeds* estabelecidos no Fed4FIRE
  - Concluído em 2021

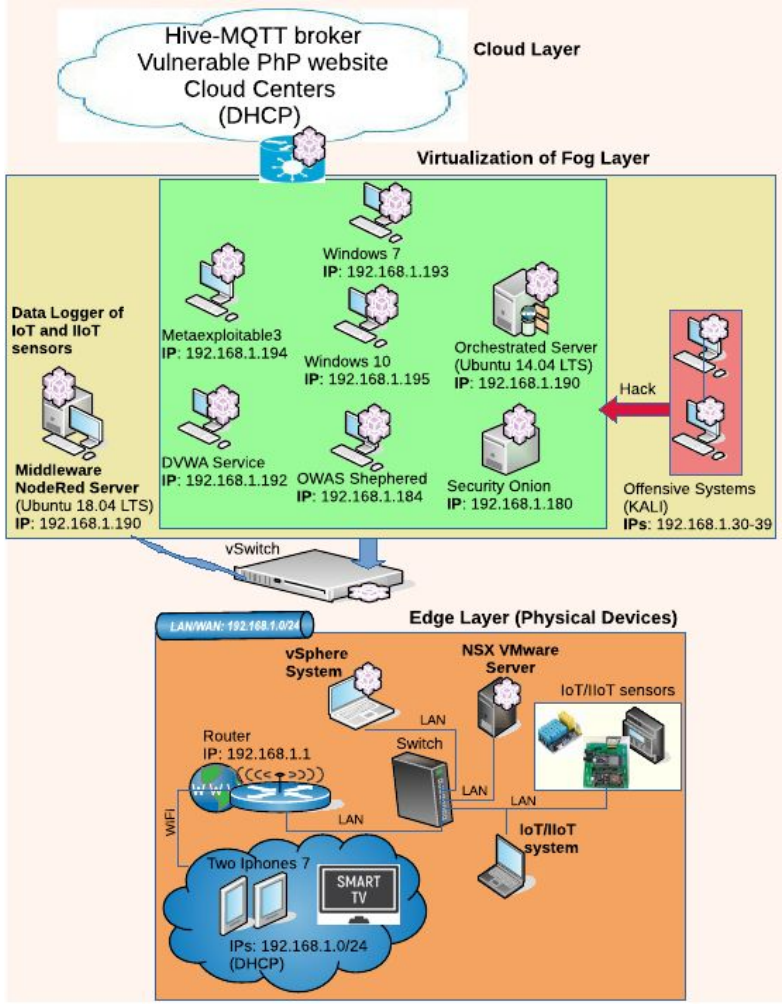
FED4FIRE
FEDERATION FOR FIRE PLUS

Testbeds de cibersegurança
FED4FIRE+

- Apresenta uma gama de tecnologias
  - Redes cabeadas e sem fio
  - IoT, SDN, Cloud
  - Big Data, IA
  - Dentre outras
- O **portal Fed4FIRE+** continua disponível: https://portal.fed4fire.eu/
  - Mantido pelo instituto de pesquisa belga IMEC
  - Oferece acesso a recursos na federação de *testbeds*
    - Recursos computacionais, armazenamento, redes
    - Ferramentas de gestão e monitoramento

Testbeds de cibersegurança
TON_IoT

- **Testbed dedicado para a criação de *datasets***
- Arquitetura organizada em três camadas:
  - *Edge* ⇒ Dispositivos físicos como sensores, smartphones, *workstations* e *laptops*
  - *Fog* ⇒ Diversos recursos virtualizados (Windows, Metasploitable, DVWA, etc)
  - *Cloud* ⇒ *Dashboard* MQTT, *Website* PHP vulnerável

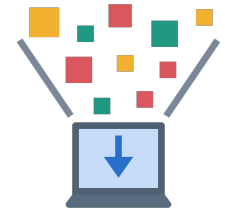


Testbeds de cibersegurança
TON_IoT

- O *dataset* contém:
  - Telemetria de sensores
  - Capturas de pacotes
- Vários tipos de tráfego:
  - *Scans* de rede (Nessus & Nmap)
  - DoS/DDoS (utilizando *scripts* Python com biblioteca Scapy)
  - Ataques *ransomware,* Instalação de *backdoors*
  - XSS, Injeções SQL
  - Interceptação de tráfego (MiTM)

Testbeds de cibersegurança
TON_IoT

- Extração de atributos a partir da ferramenta Zeek



Captura de rede

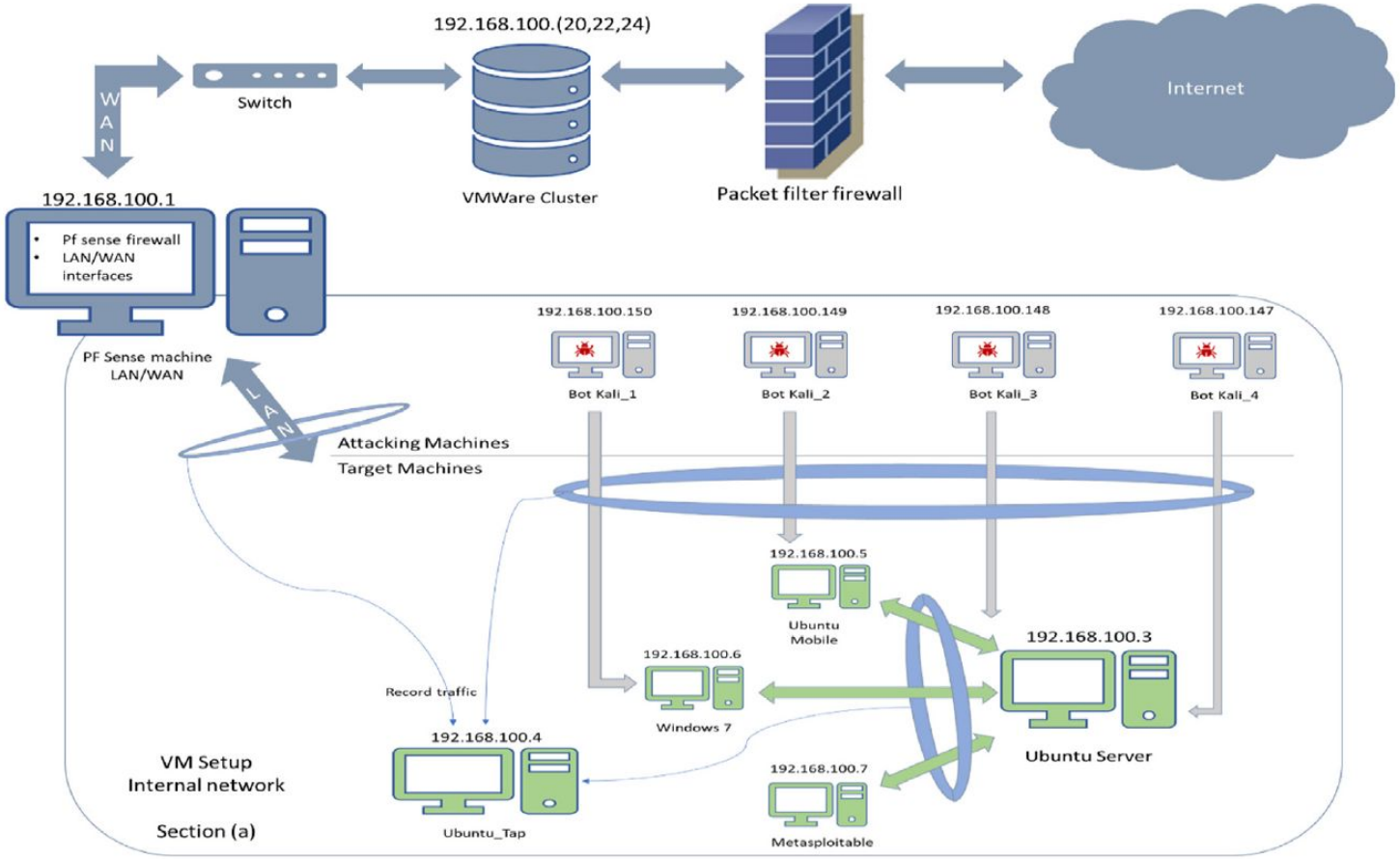
zeek

44 atributos

timestamp	dns_query	http_method
src_ip	ssl_version	http_uri
service	ssl_subject	http_referrer

Testbeds de cibersegurança
Bot-IoT

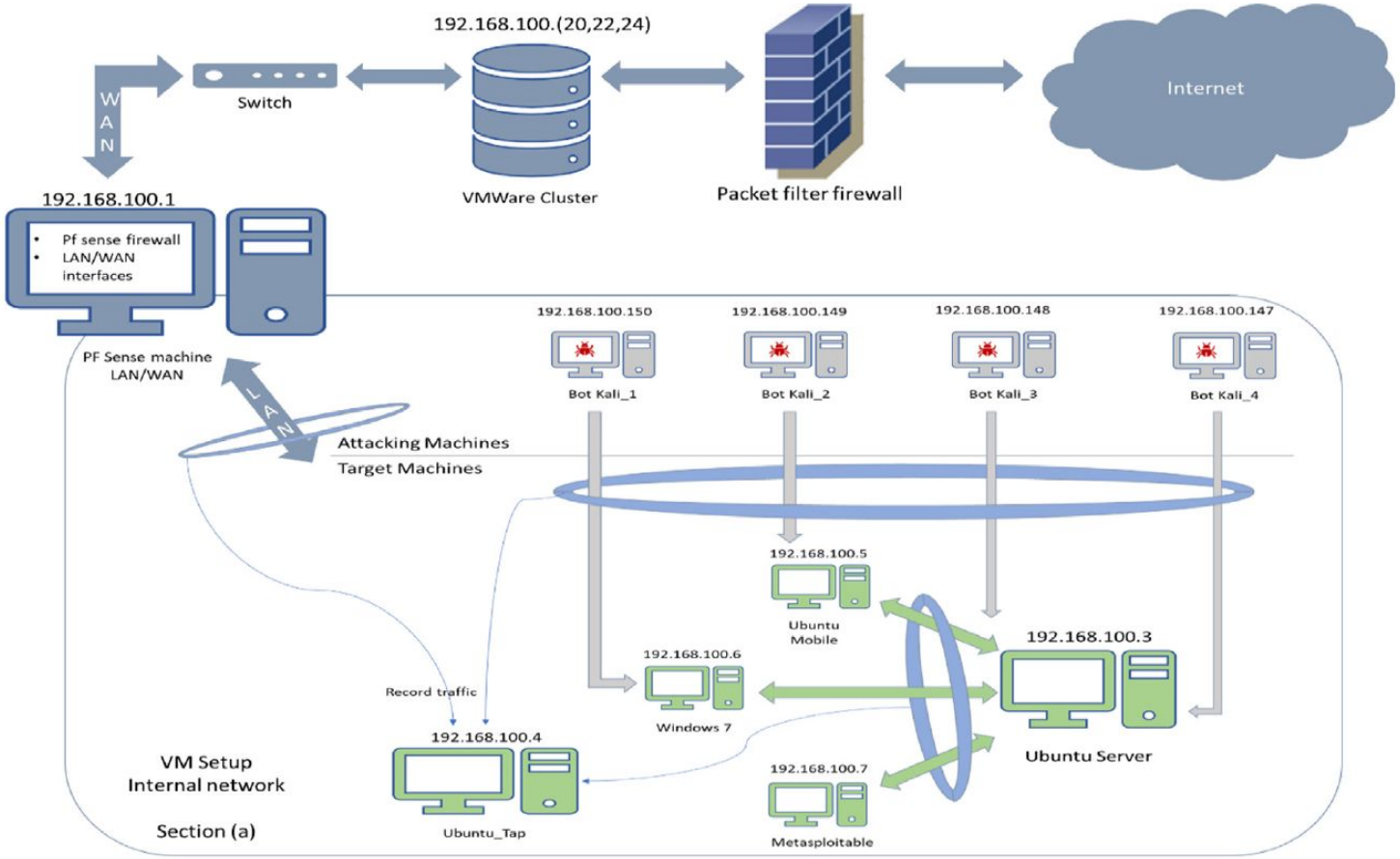
- **Testbed para geração de *datasets***
- Infraestrutura baseada em virtualização



KORONIOTIS, Nickolaos et al. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Generation Computer Systems, v. 100, p. 779-796, 2019.

Testbeds de cibersegurança
Bot-IoT

- Diversas plataformas
  - Windows, Metasploitable, Ubuntu
- Diversos protocolos
  - DNS, FTP, HTTP, SSH
- Dispositivos IoT emulados
  - Javascript + NodeRED



KORONIOTIS, Nickolaos et al. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Generation Computer Systems, v. 100, p. 779-796, 2019.

Testbeds de cibersegurança
Bot-IoT

- O *dataset* contém capturas de pacotes
  - Tráfego de sensores MQTT
  - Tráfego malicioso
    - Varreduras de portas
    - Ataques *botnet*

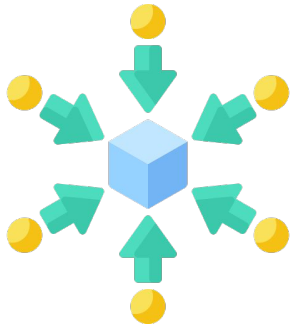
Testbeds de cibersegurança
Resumo - Tabela comparativa

Testbed	**Recursos**	**Flexibilidade**	**Escala**	**Execução Segura**	**Disponibilidade**
Deterlab (antigo)	CT, VM, Phy*	Alta	Alta	Sim	Educação apenas
DeterLab (MergeTB)	VMs, Phy	Alta	ND	Sim	Sim
FIT-IoT LAB	**Phy**	**Alta**	**Alta**	**ND**	**Sim**
Gotham	**CT e VM**	**Alta**	**Média**	**Sim**	**Sim (código-fonte)**
GENI	VM, CT, Phy	Alta	Alta	Sim	Descontinuado
FABRIC	VM	Alta	Alta	Sim	Sim
Fed4FIRE+	Misto ‡	Misto ‡	Misto ‡	Misto ‡	Sim
TON_IoT	**Phy e VM**	**Baixa**	**Baixa**	**ND**	**Apenas *dataset***
Bot-IoT	VM	Baixa	Baixa	ND	Apenas *dataset*

Phy Dispositivos físicos; *VM* Máquinas Virtuais; *CT* Containers; ‡ Dependente do testbed federado selecionado; *ND* Não detalhado; ∗ Dentre outros

Testbeds de cibersegurança
Considerações sobre *testbeds*

- Tendo em vista os *testbeds* apresentados, observa-se
  - Variedade de escalas
  - Arquiteturas distintas



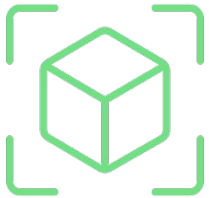
Centralizada

Distribuída

Testbeds de cibersegurança
Considerações sobre *testbeds*

- Tendo em vista os *testbeds* apresentados, observa-se
  - Programabilidade em múltiplos níveis (nó & rede)
    - Tendências como tecnologias SDN
  - Diferentes abordagens para a representação de dispositivos
    - Impacta no isolamento dos experimentos e do *testbed*
    - Também afeta a alocação e compartilhamento de recursos

Dispositivos Físicos

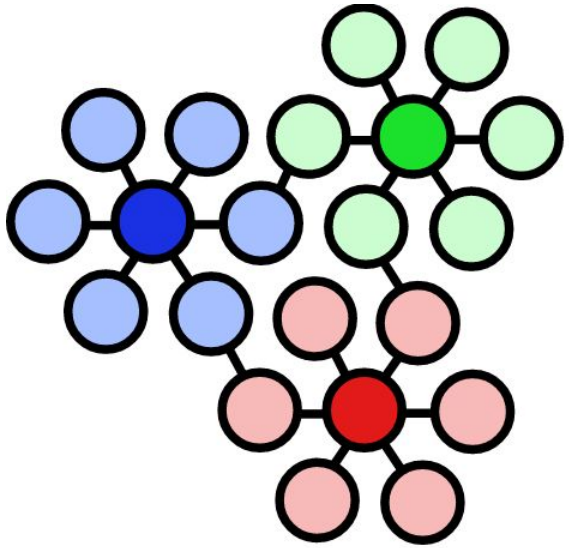


Máquinas Virtuais

Containers

Testbeds de cibersegurança
Considerações sobre *testbeds*

- Além destes, há outros testbeds na literatura!



emulab

PLANETLAB Europe

An open platform for developing, deploying, and accessing planetary-scale services

MENTORED

Testbed

Projeto MENTORED

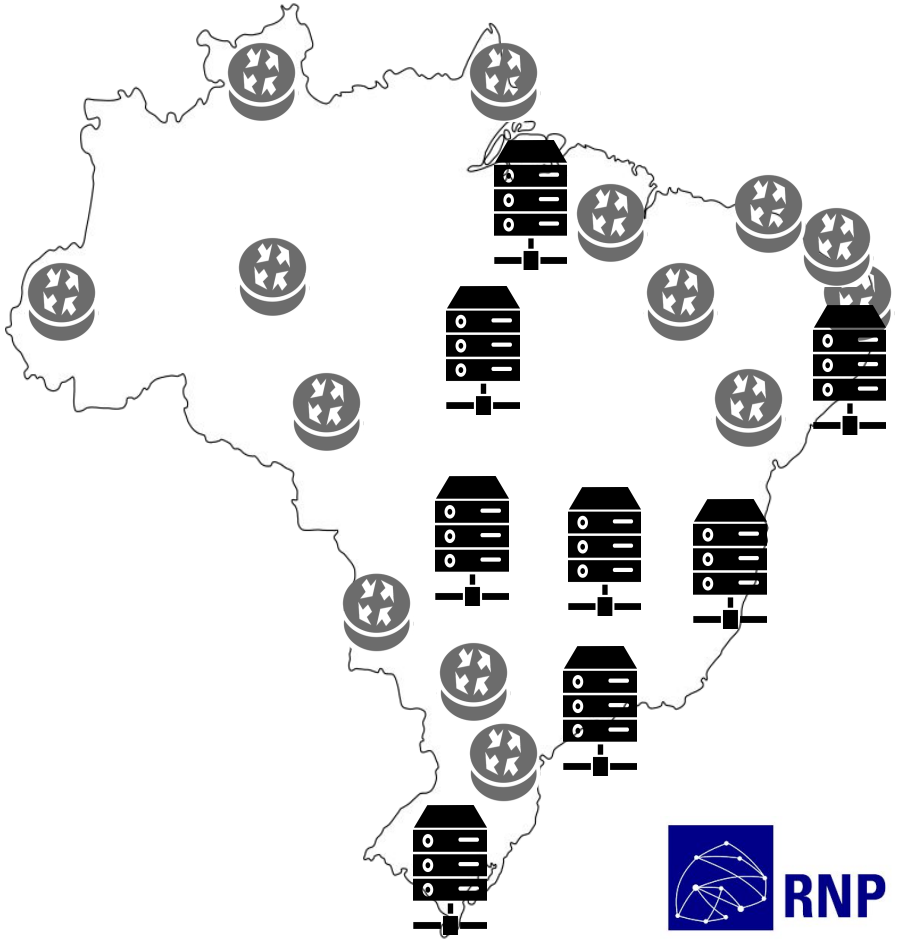
- Identificar, modelar e avaliar comportamentos maliciosos relacionados à IoT;

- 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*

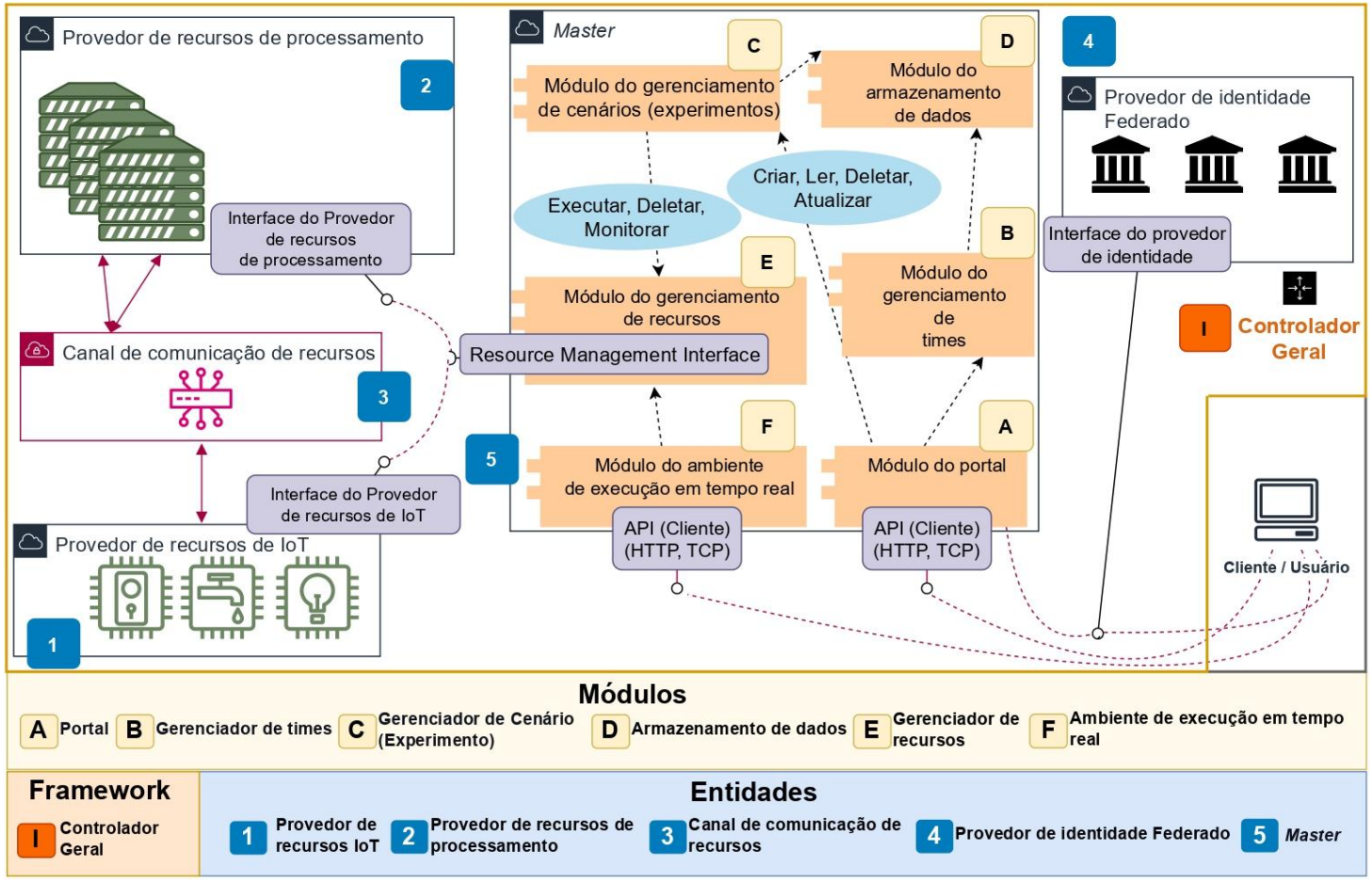
- Prover um ambiente controlado para experimentação em cibersegurança;
- Utiliza a Infraestrutura Definida por Software da Rede Nacional de Ensino e Pesquisa (IDS-RNP):
  - Oferece escala realista e alto volume de tráfego de rede;
  - É baseado no **Kubernetes** e possui suporte a diferentes tecnologias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



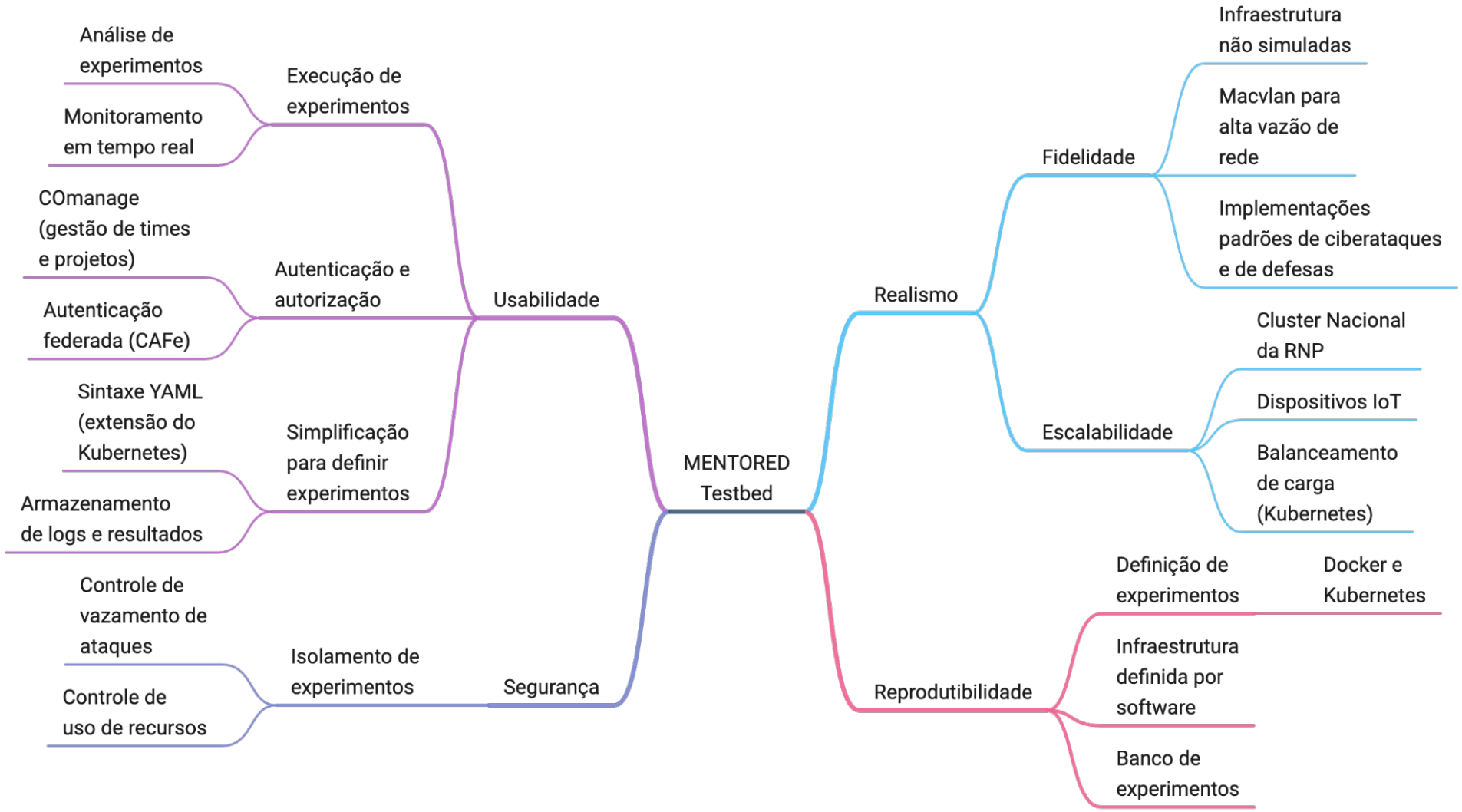
Framework Mentored
Atributos

Framework Mentored

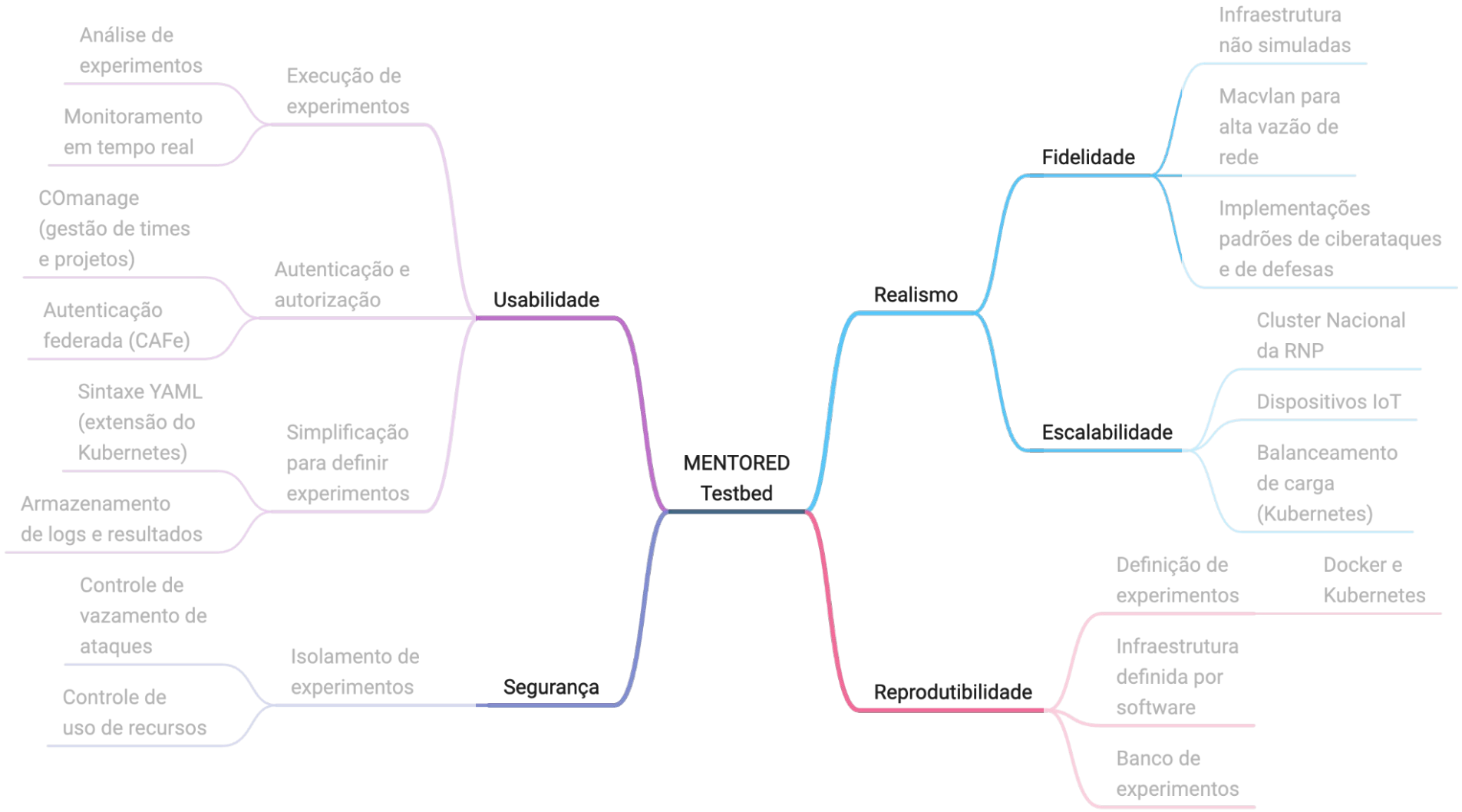
- Independente de tecnologia
- Recursos de processamento e IoT
- Softwares para **“simplificar” experimentação**



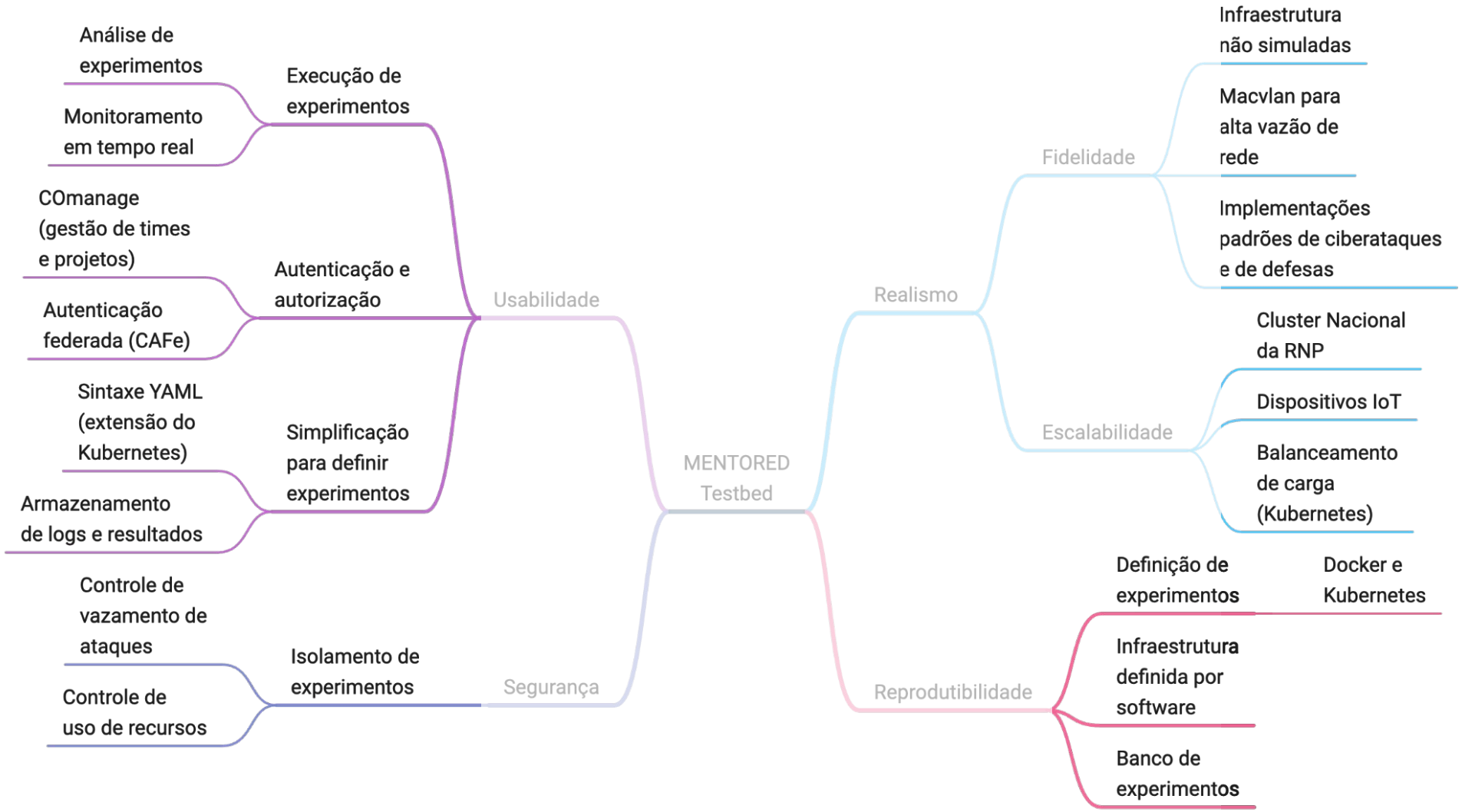
Framework Mentored
Requisitos e Características



Framework Mentored
Requisitos e Características



Framework Mentored
Requisitos e Características

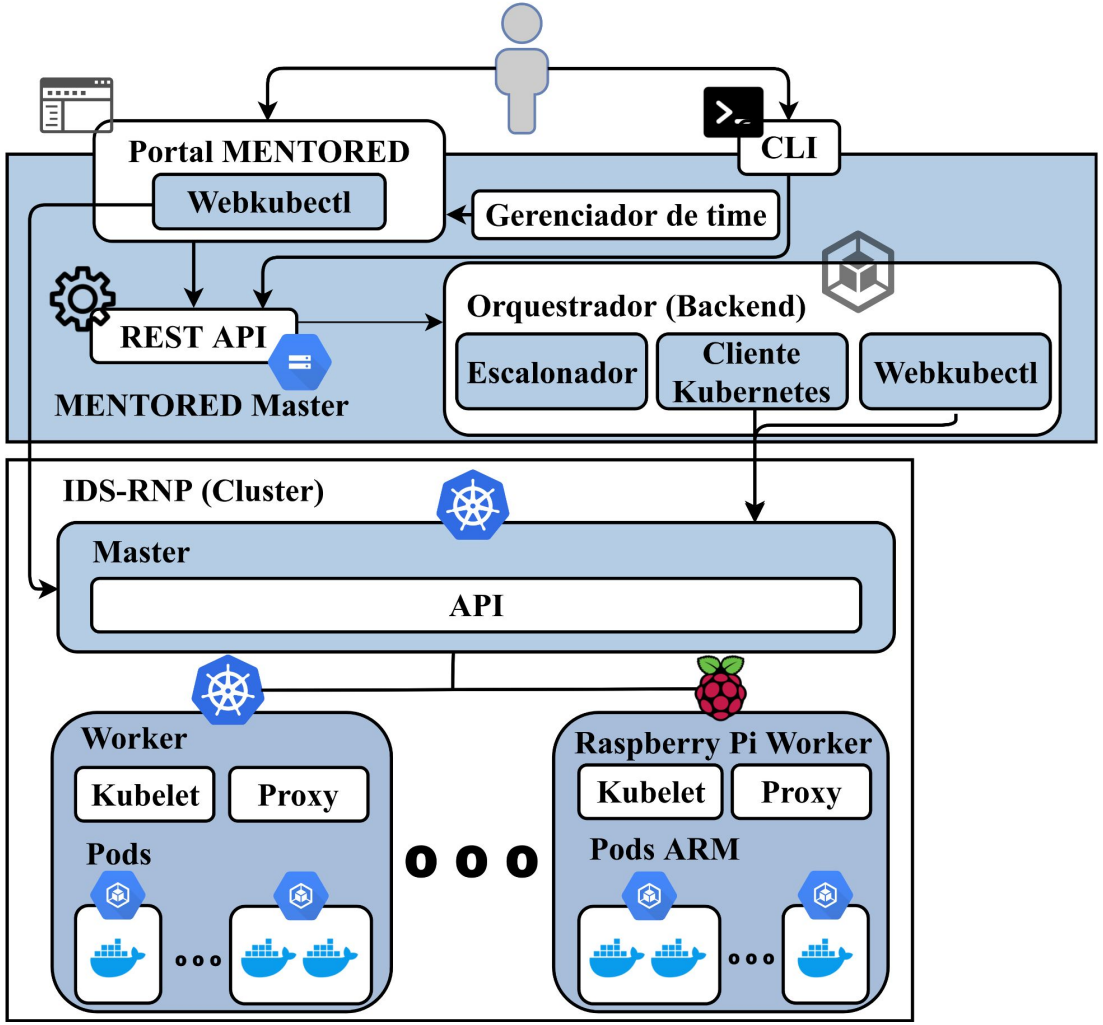


Coffee-break | Q&A

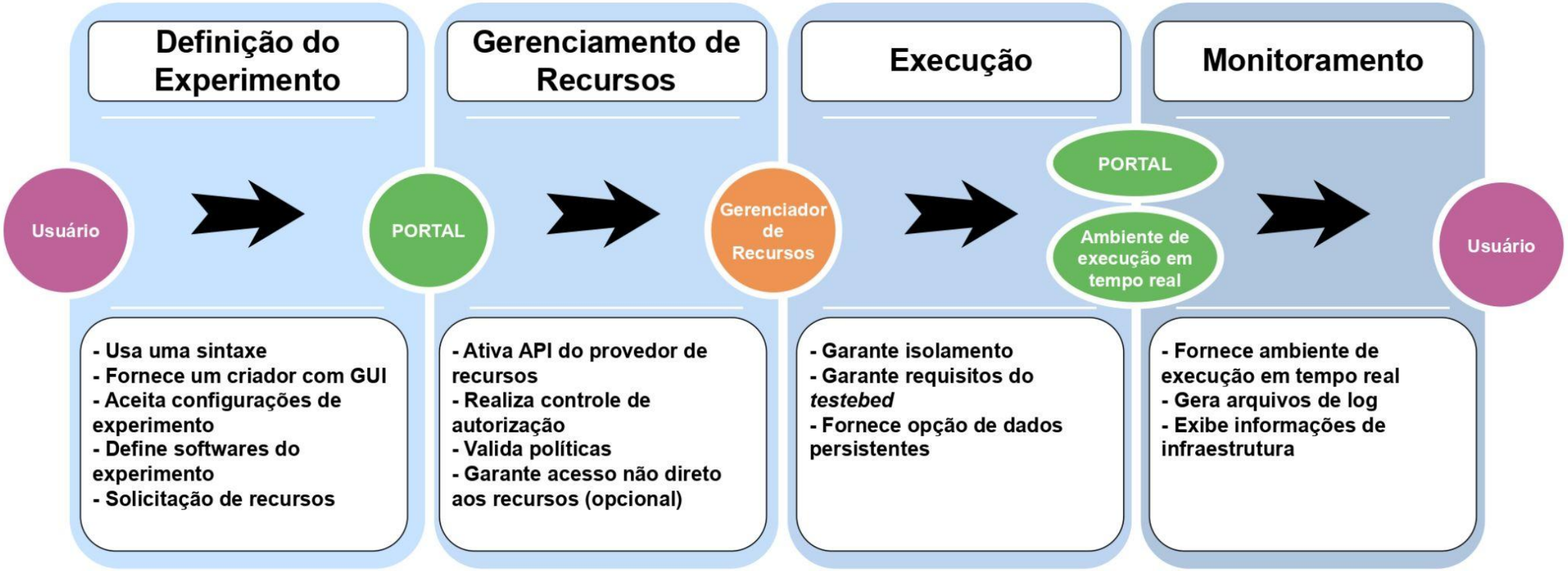
Github

github.com/mentoredtestbed/minicurso-sbrc-2024-testbeds

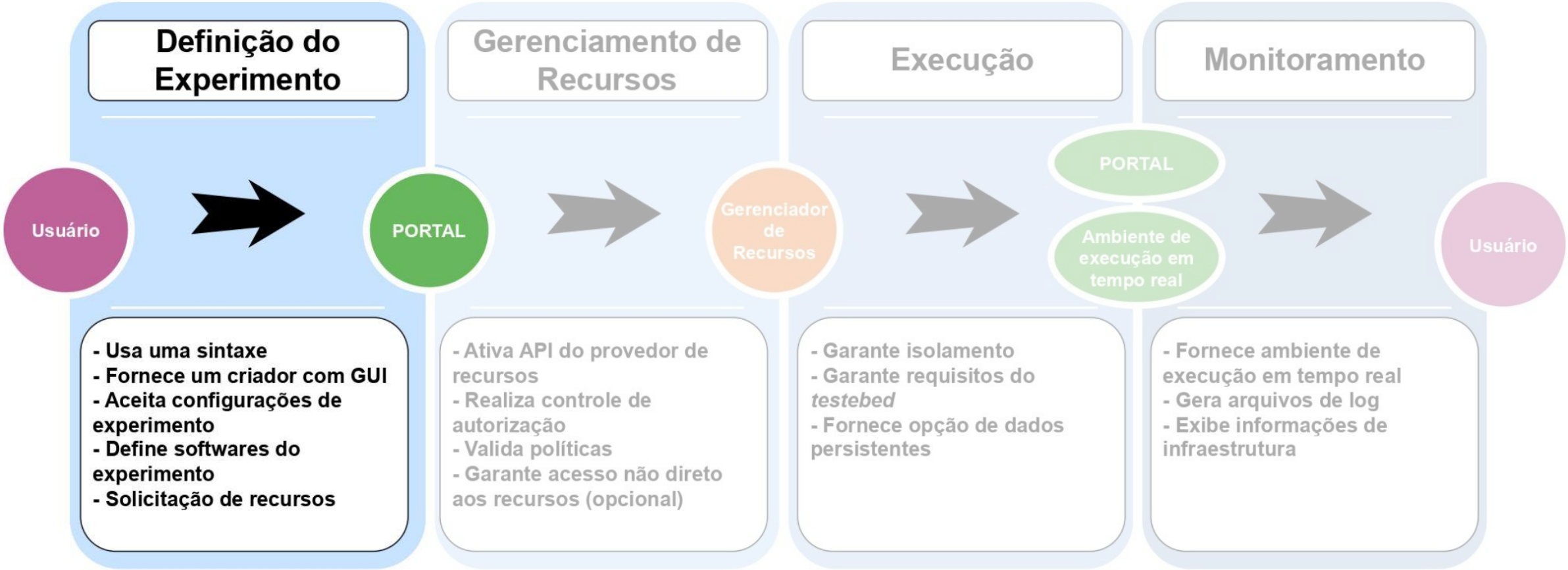
Mentored Testbed
Arquitetura da implementação



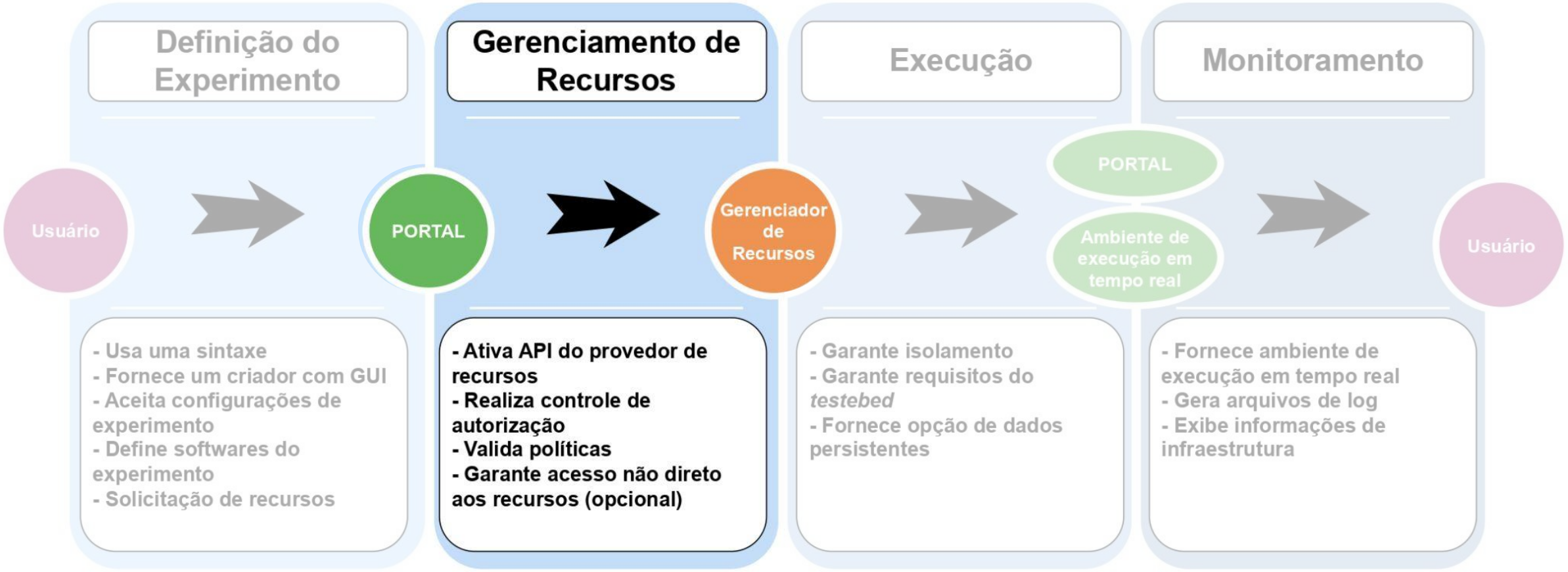
Mentored Testbed
Fluxo de execução de experimento



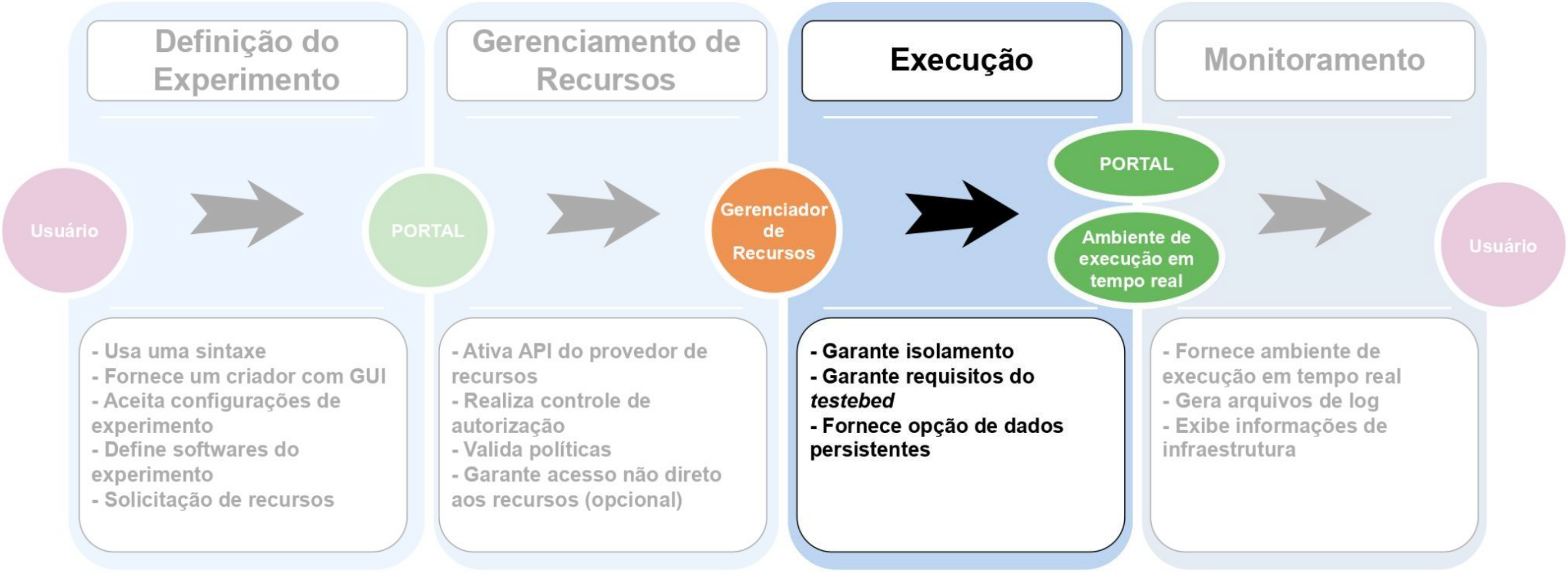
Mentored Testbed
Definição do experimento



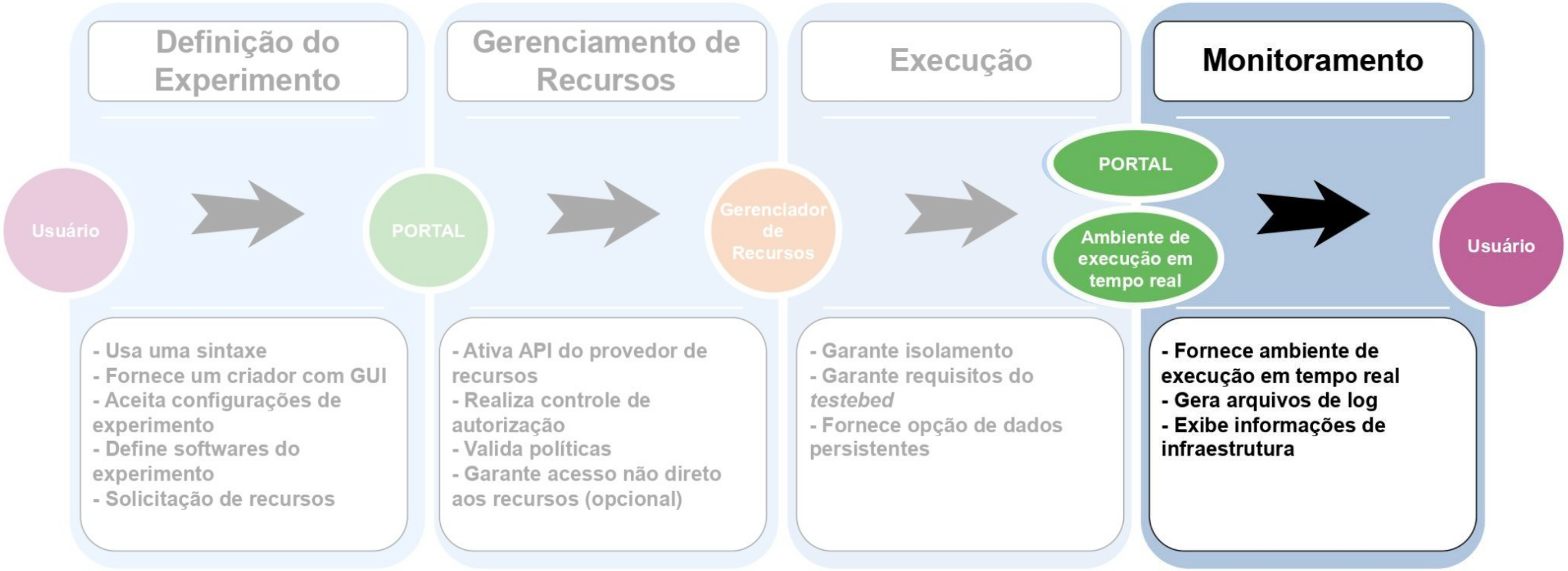
Mentored Testbed
Gerenciamento de recursos



Mentored Testbed
Execução

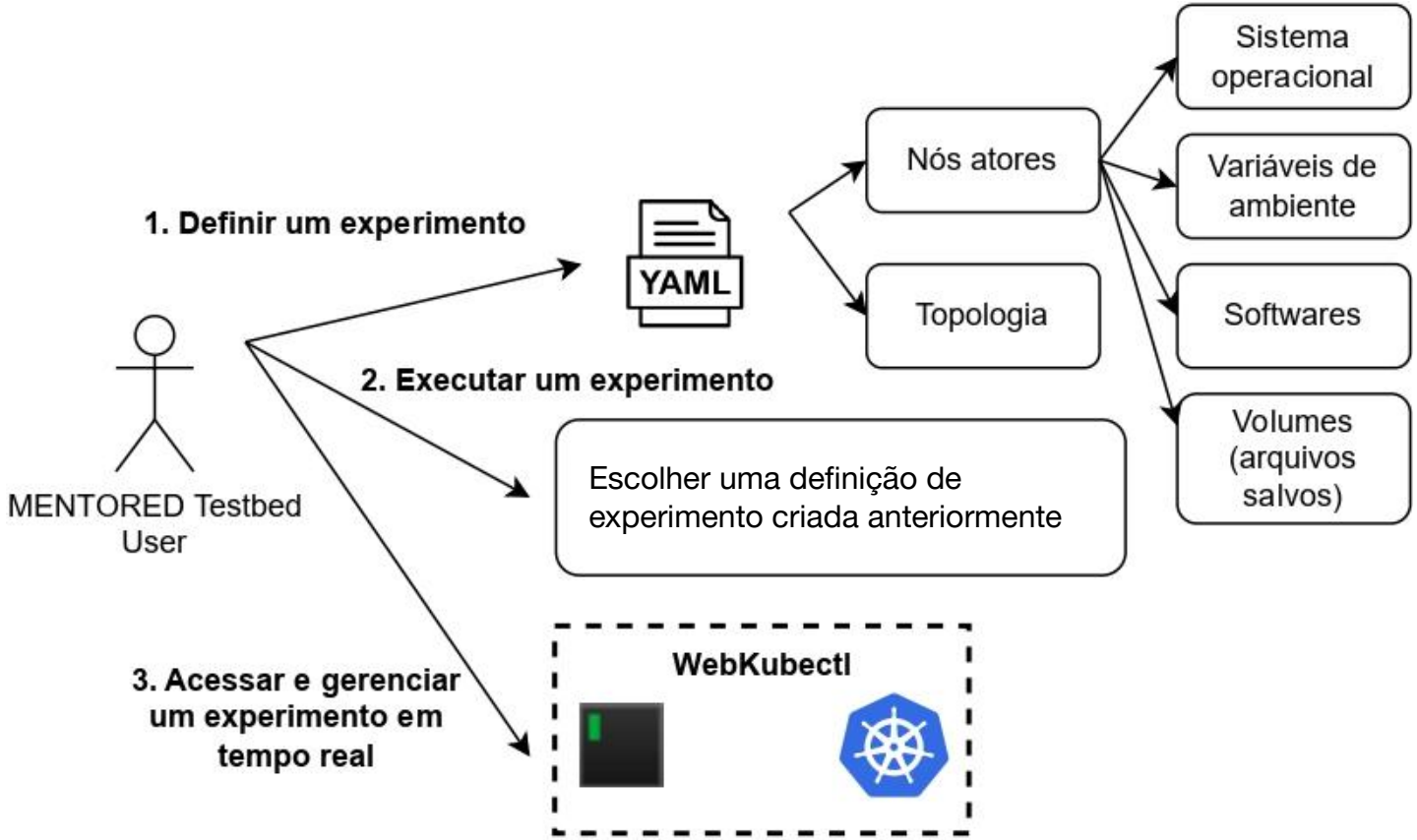


Mentored Testbed
Monitoramento



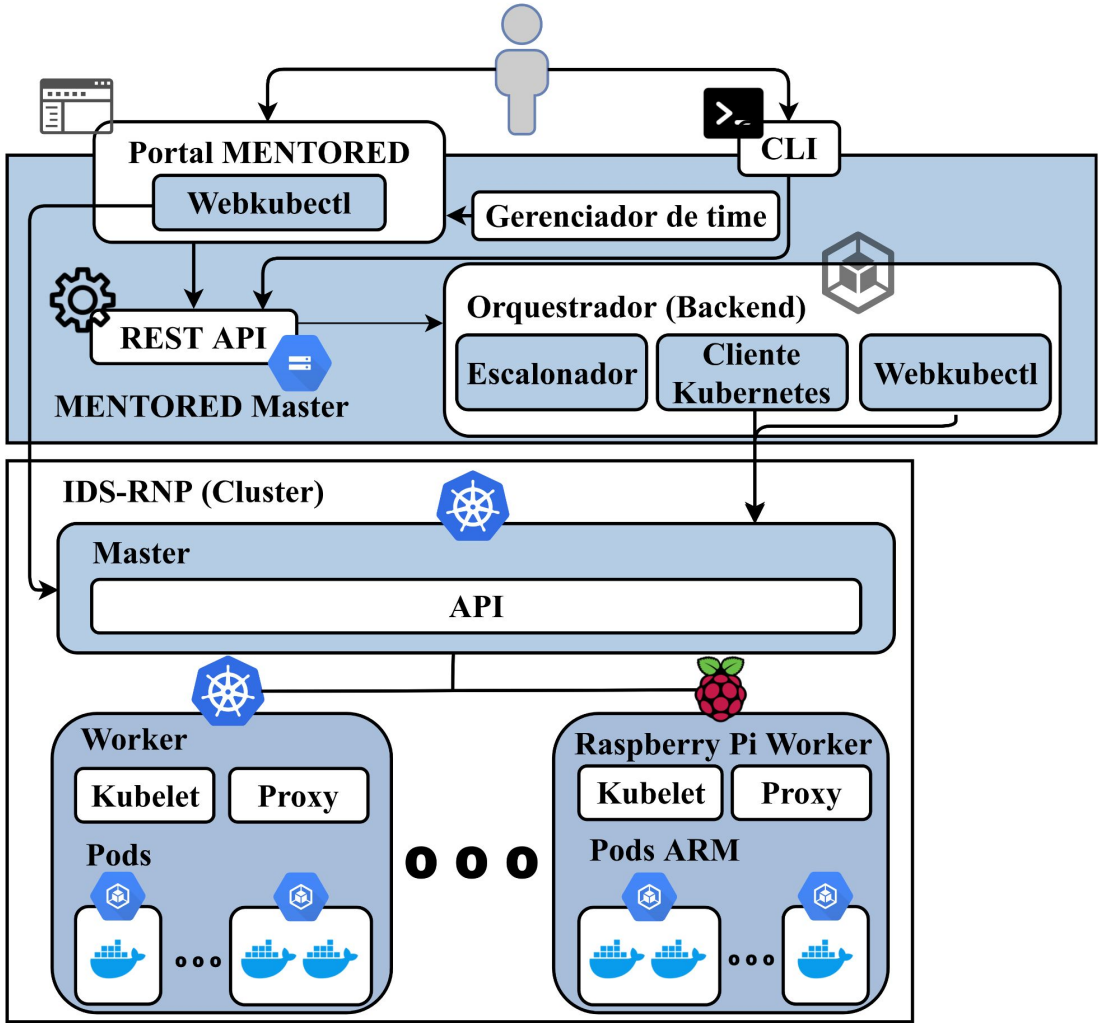
Mentored Testbed
Ponto de vista do experimentador

- 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



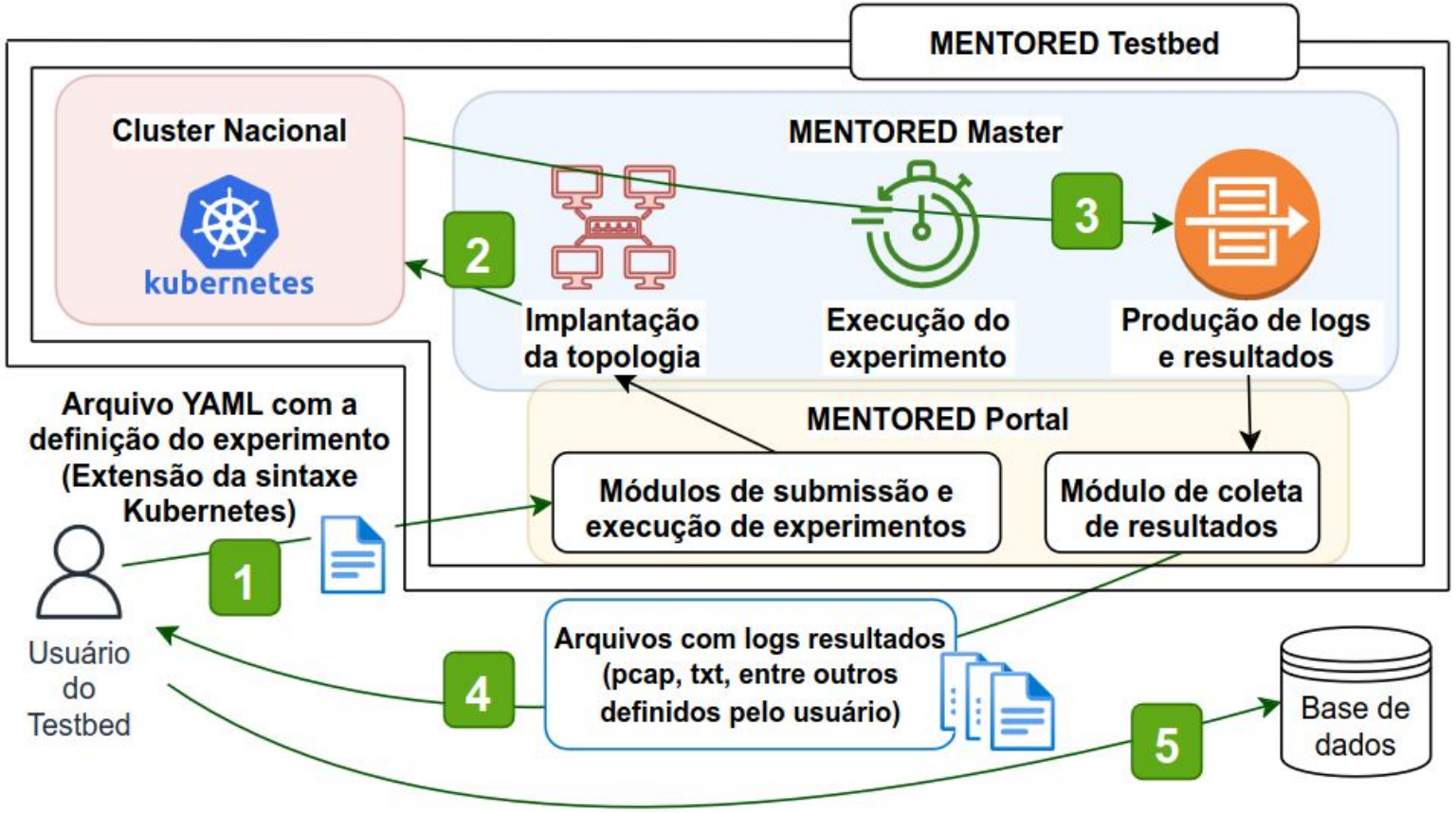
Mentored Testbed
Arquitetura da implementação

- 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**



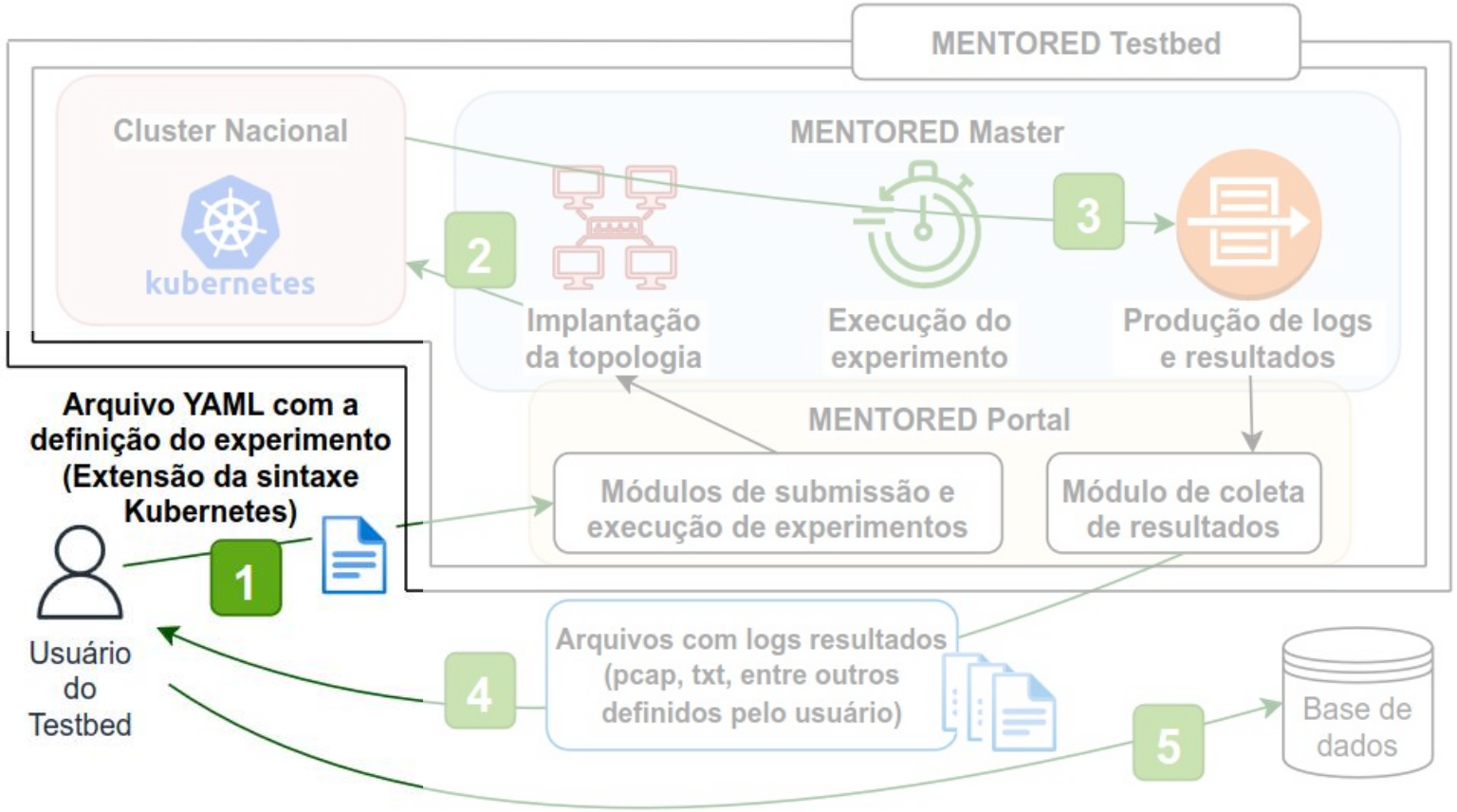
Mentored Testbed
Criando bases de dados

- TODO: Mencionar Publicação



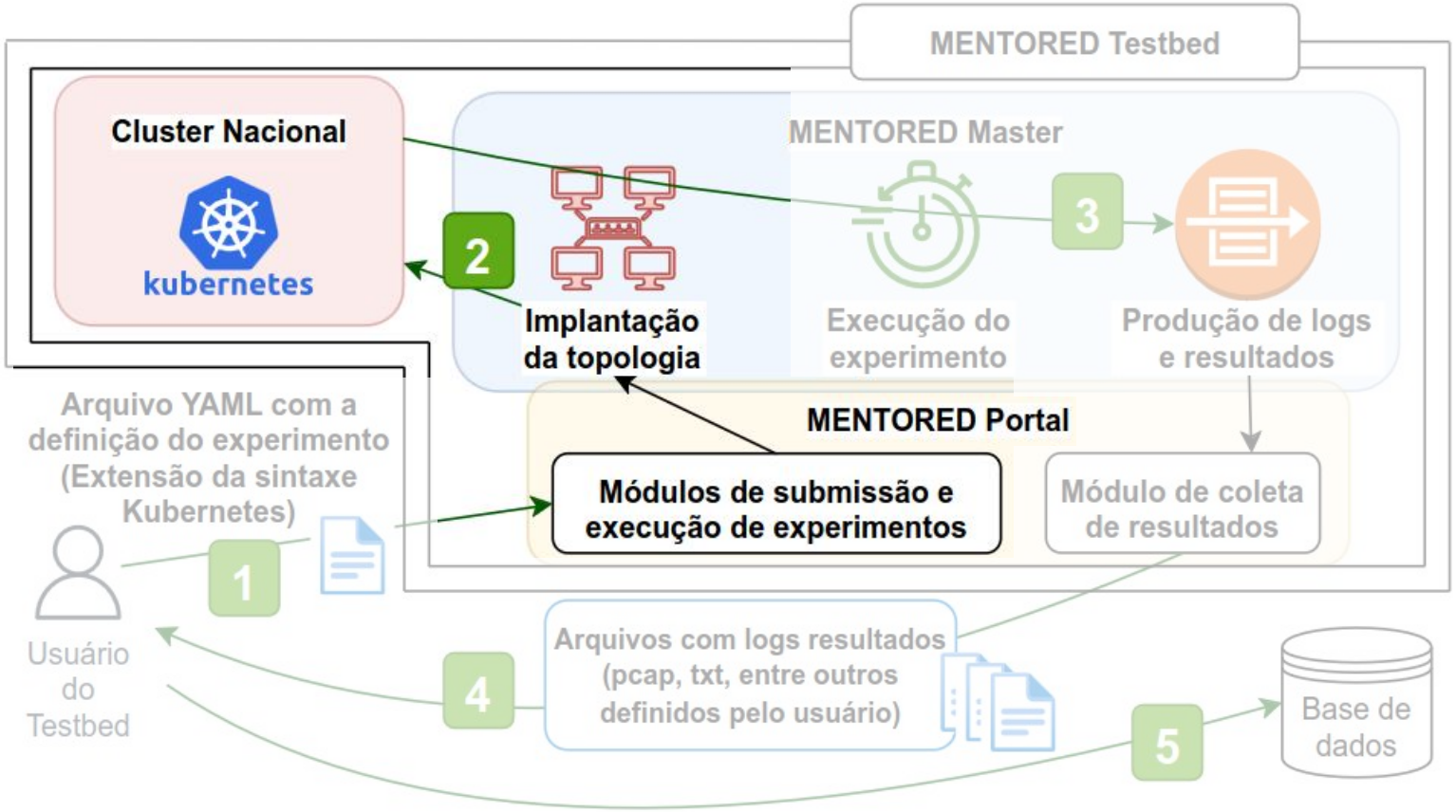
1. Definição do experimento (número de nós, topologia, softwares, parâmetros, etc.)
2. Alocação do experimento definido nos recursos do testbed
3. Execução do experimento com monitoramento e acesso de recursos em tempo real
4. Coleta dos resultados do experimento, incluindo os arquivos definidos pelo 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.)

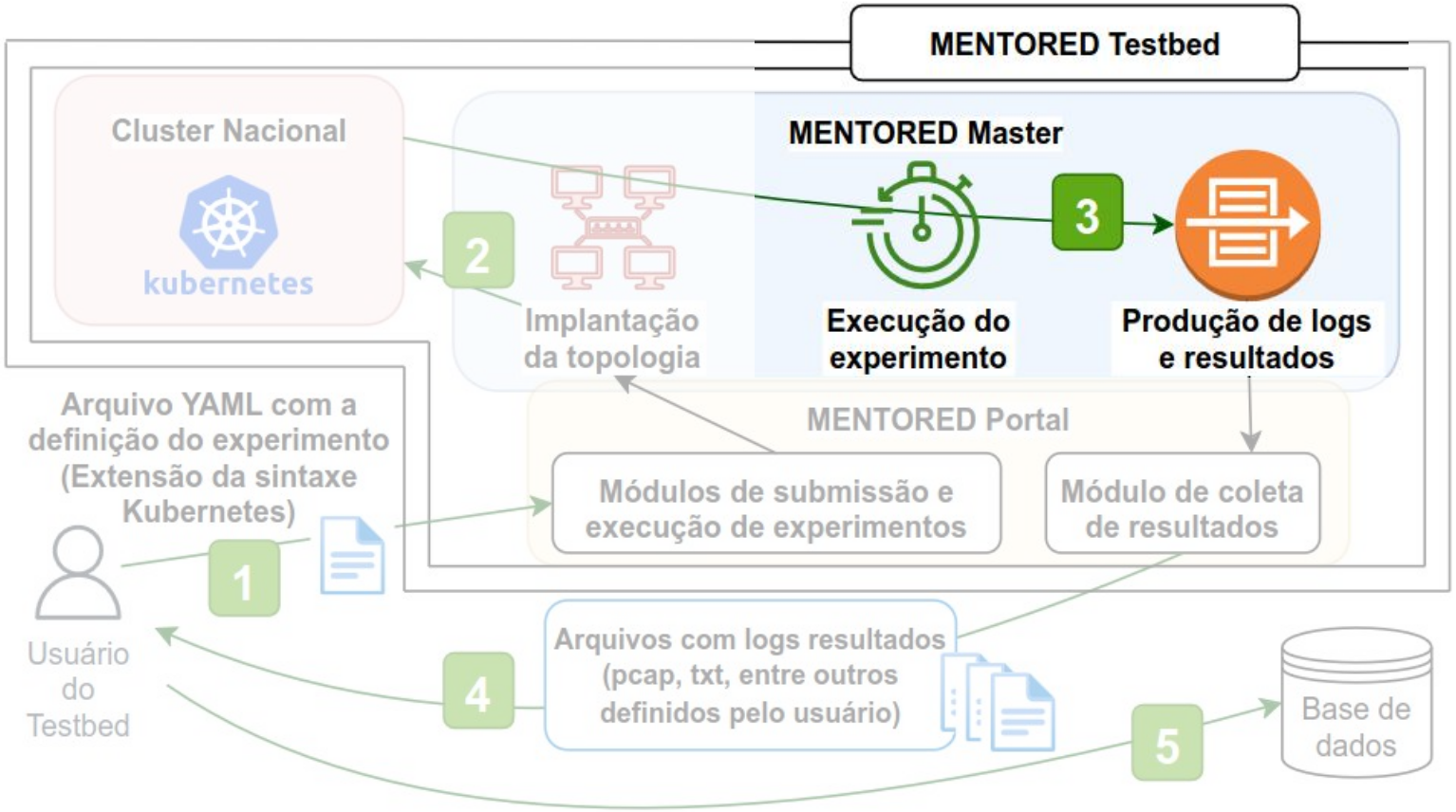
2 Alocação do experimento definido nos recursos do testbed

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.)

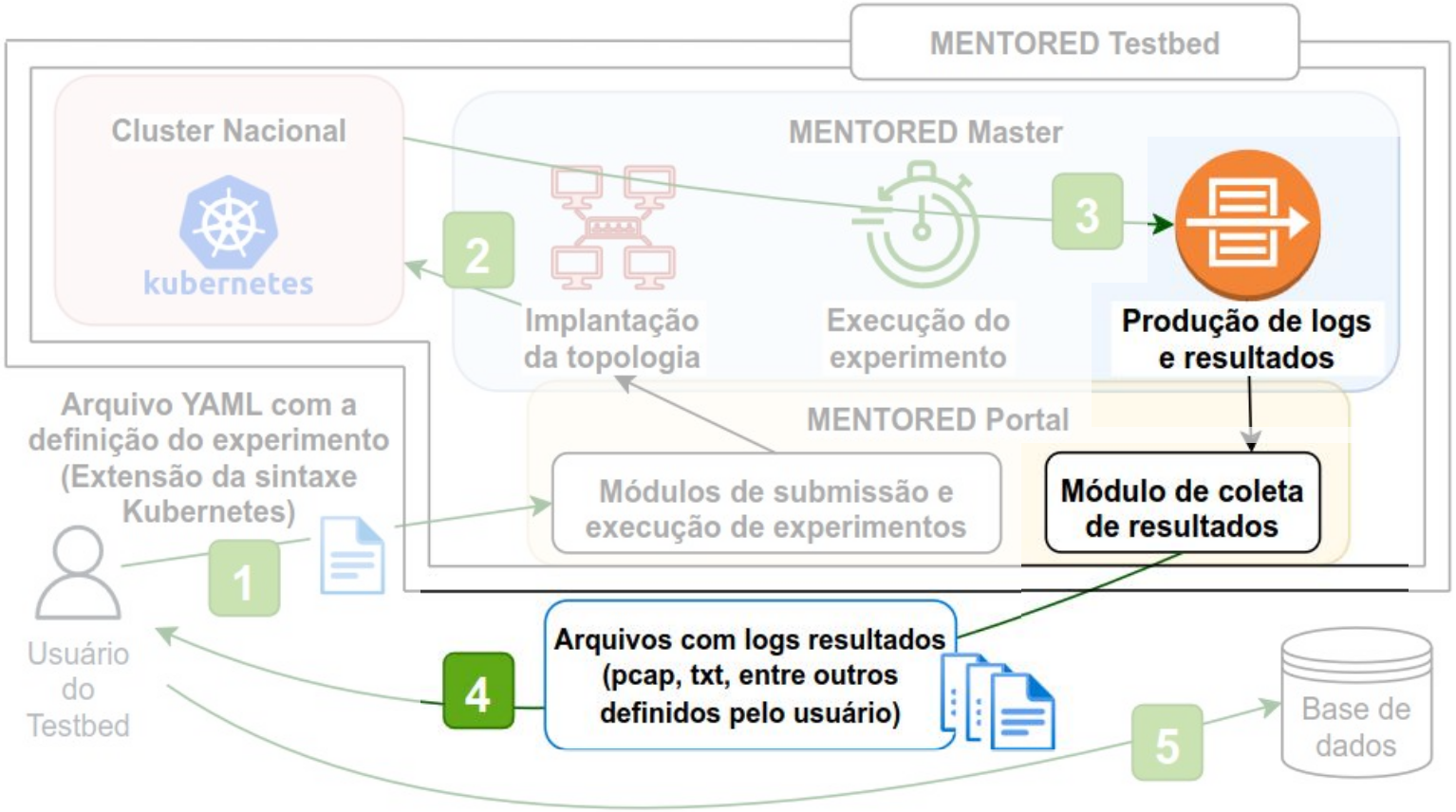
2 Alocação do experimento definido nos recursos do testbed

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

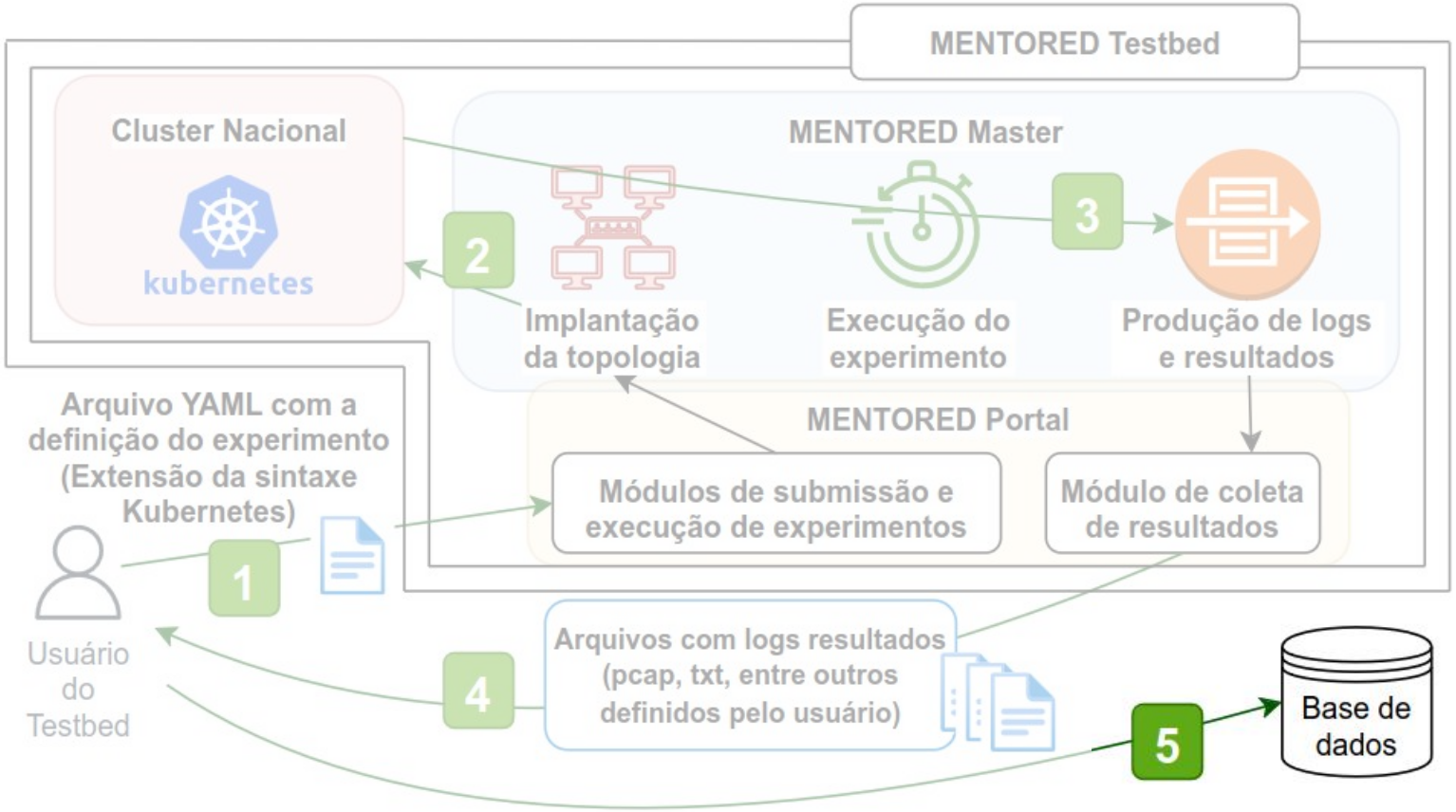
5 Processamento de dados usando ferramentas de análise de segurança e tráfego de rede. Definição de bases de dados usadas para avaliação e validação de técnicas de segurança

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



1 Definição do experimento (número de nós, topologia, softwares, parâmetros, etc.)

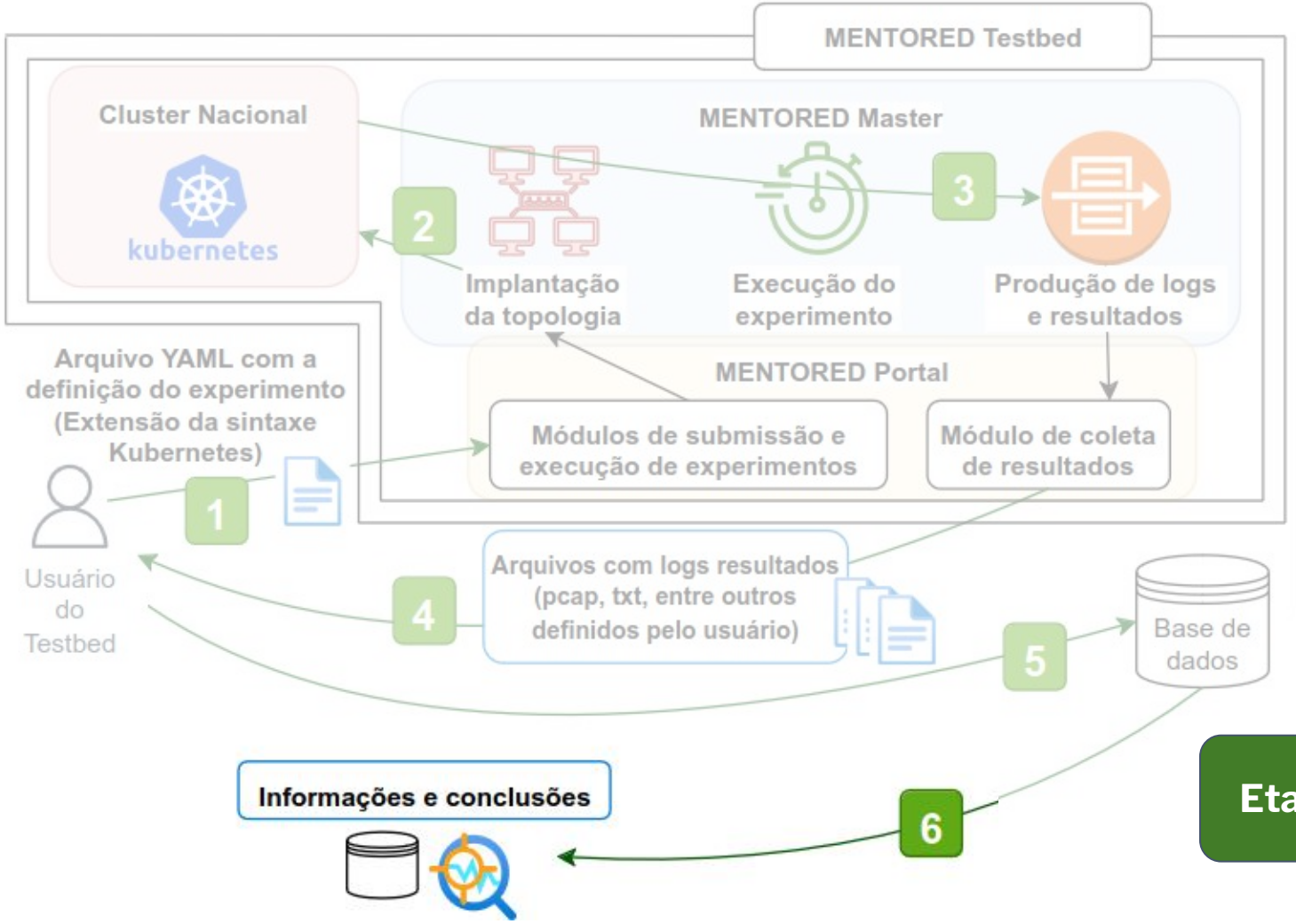
2 Alocação do experimento definido nos recursos do testbed

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

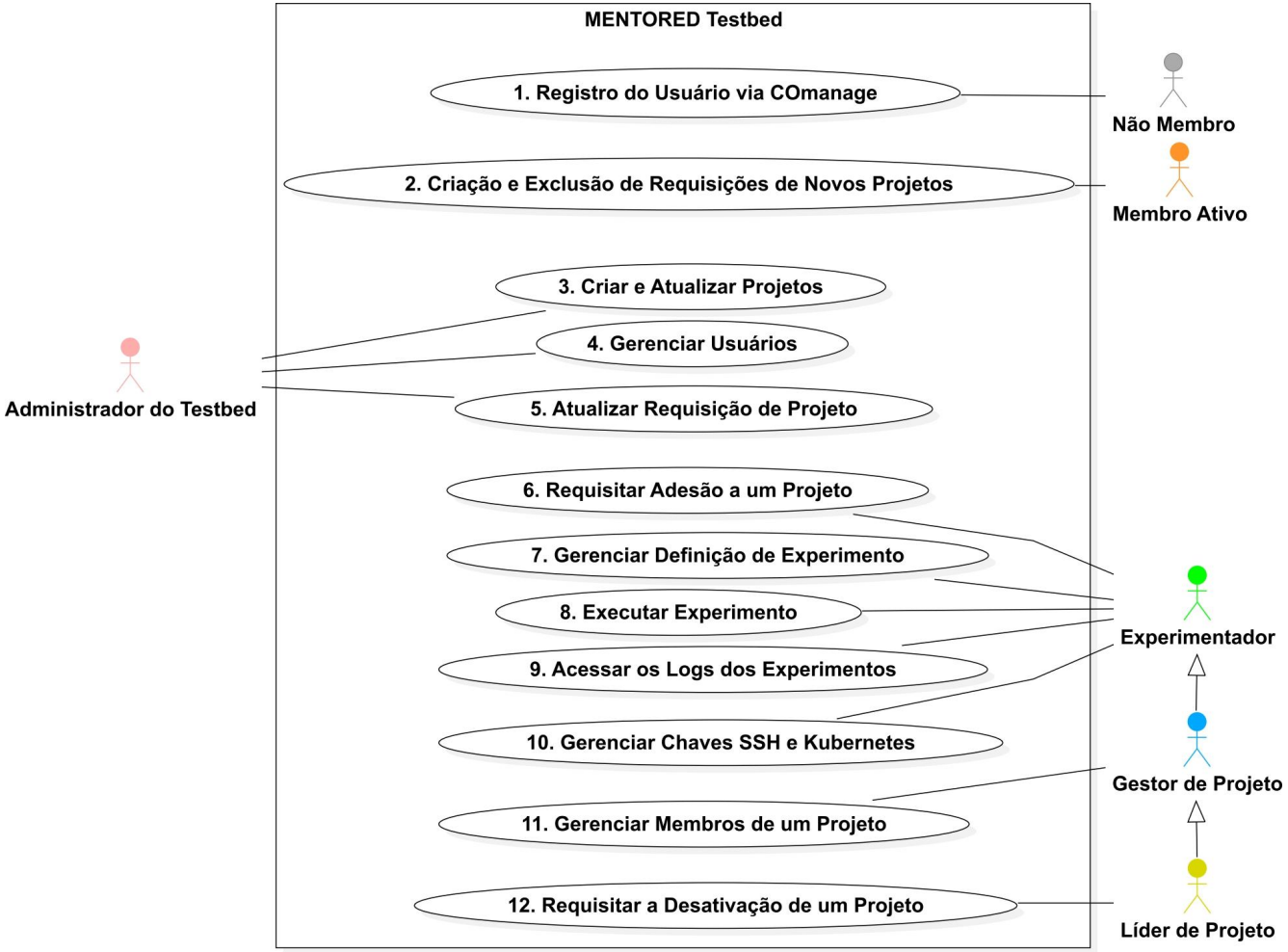
Mentored Testbed
Criando bases de dados



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.
6. **Análise de dados: Informações e conclusões do cenário usado no experimento.**

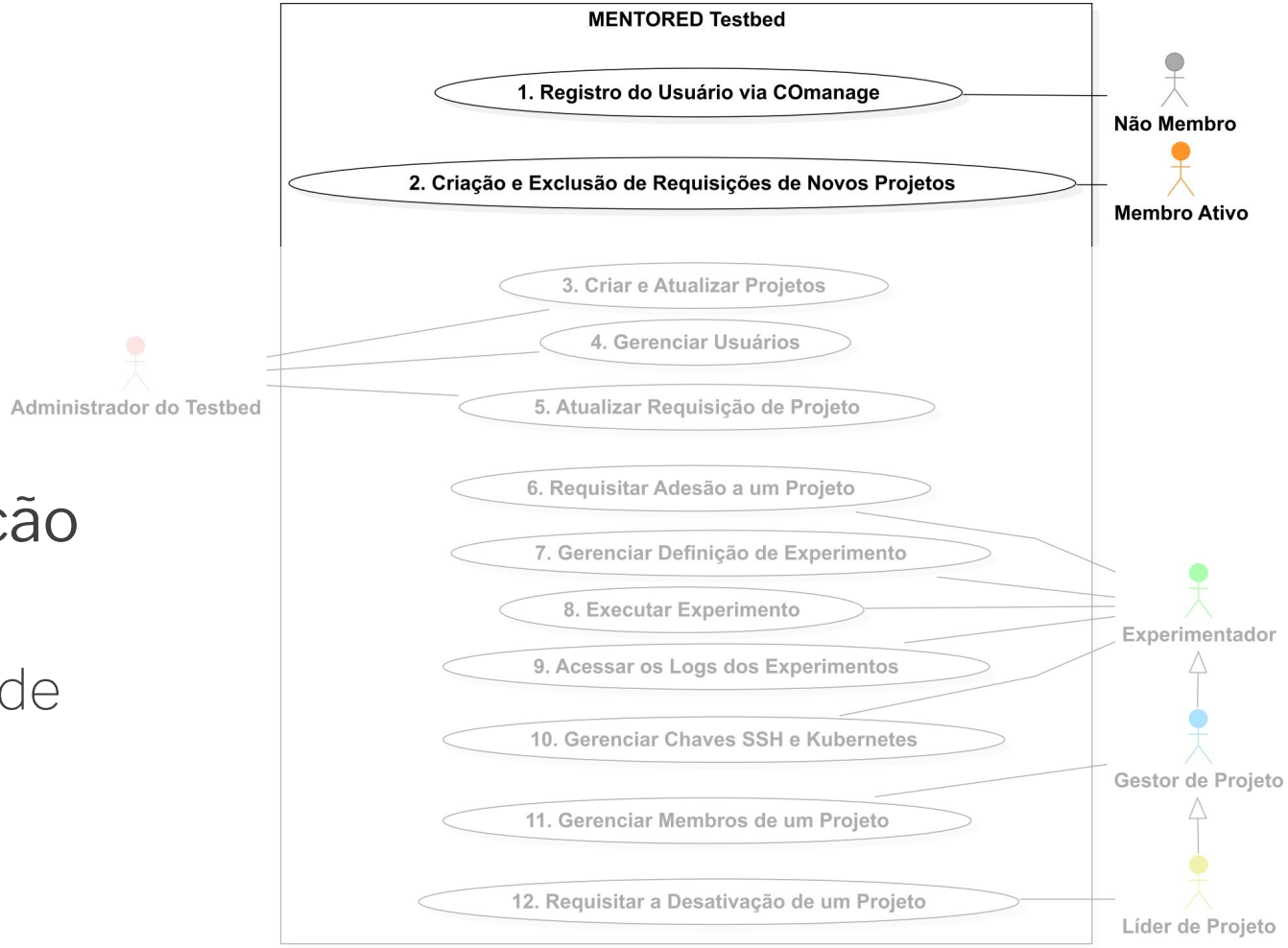
Etapa planejada pelo experimentador

Mentored Testbed
Gestão de Projetos e Times



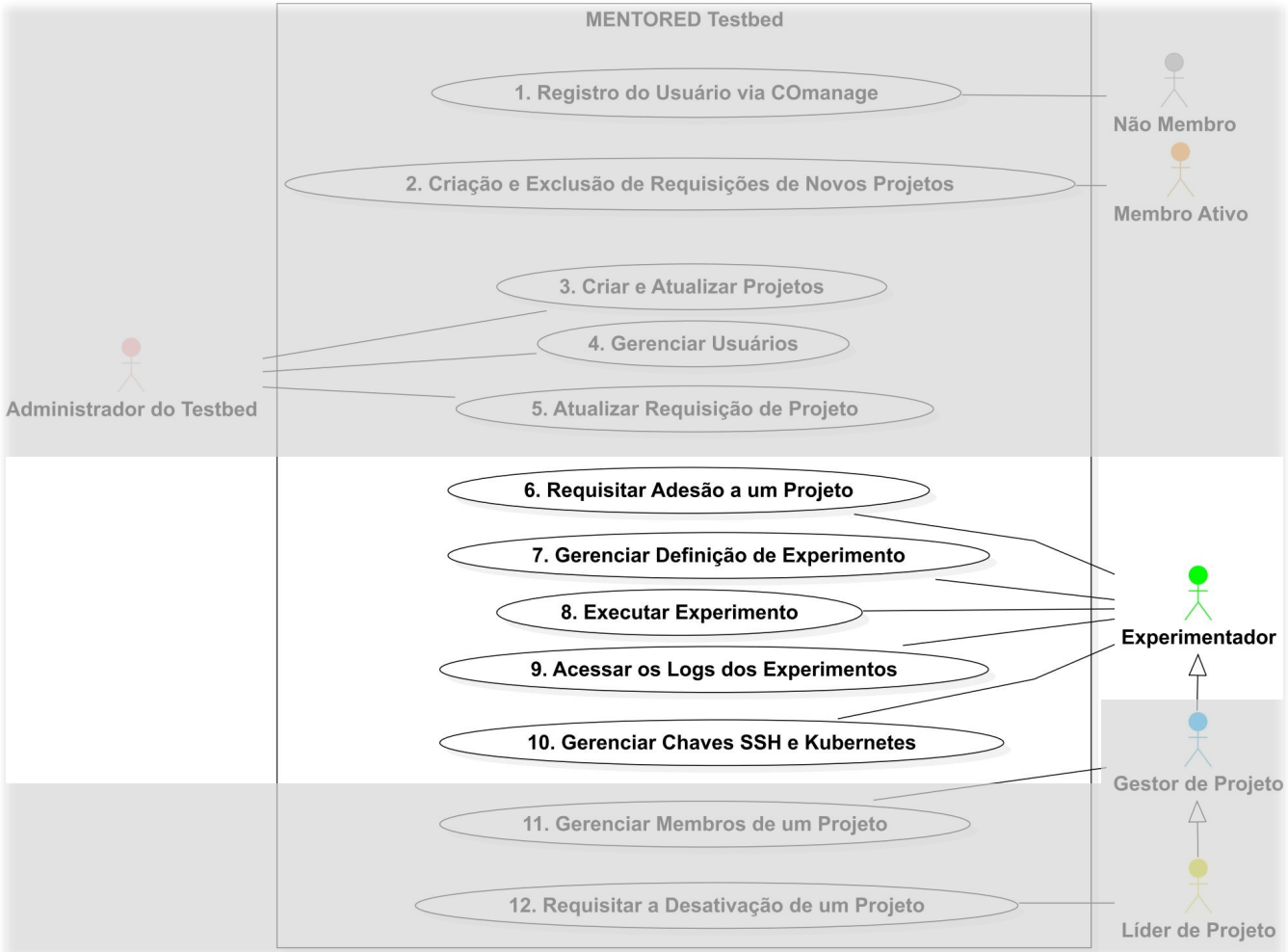
Mentored Testbed
Gestão de Projetos e Times

- **Não Membro**: usuários não cadastrados no sistema.
  - Registra-se no sistema via COmanage.
- **Membro ativo**: após cadastro, usuários podem requisitar a criação de novos projetos.
  - Pode criar ou excluir requisições de novos projetos.



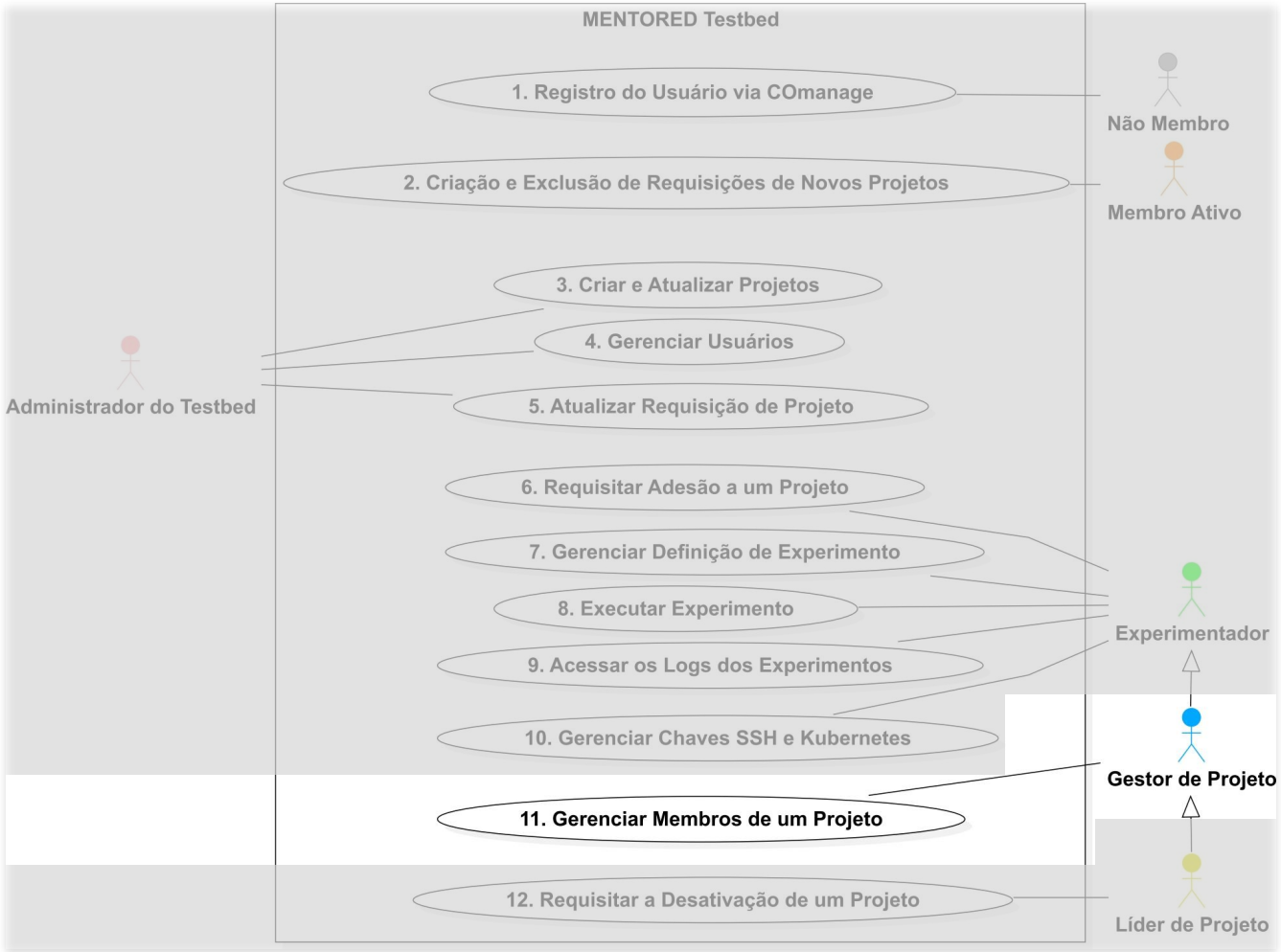
Mentored Testbed
Gestão de Projetos e Times

- **Experimentador**: possui a capacidade de realizar experimentos dentro de um projeto associado.
  - Pode entrar em projetos
  - Gerencia e acessa logs dos experimentos.
  - Gerencia chaves SSH e Kubernetes.



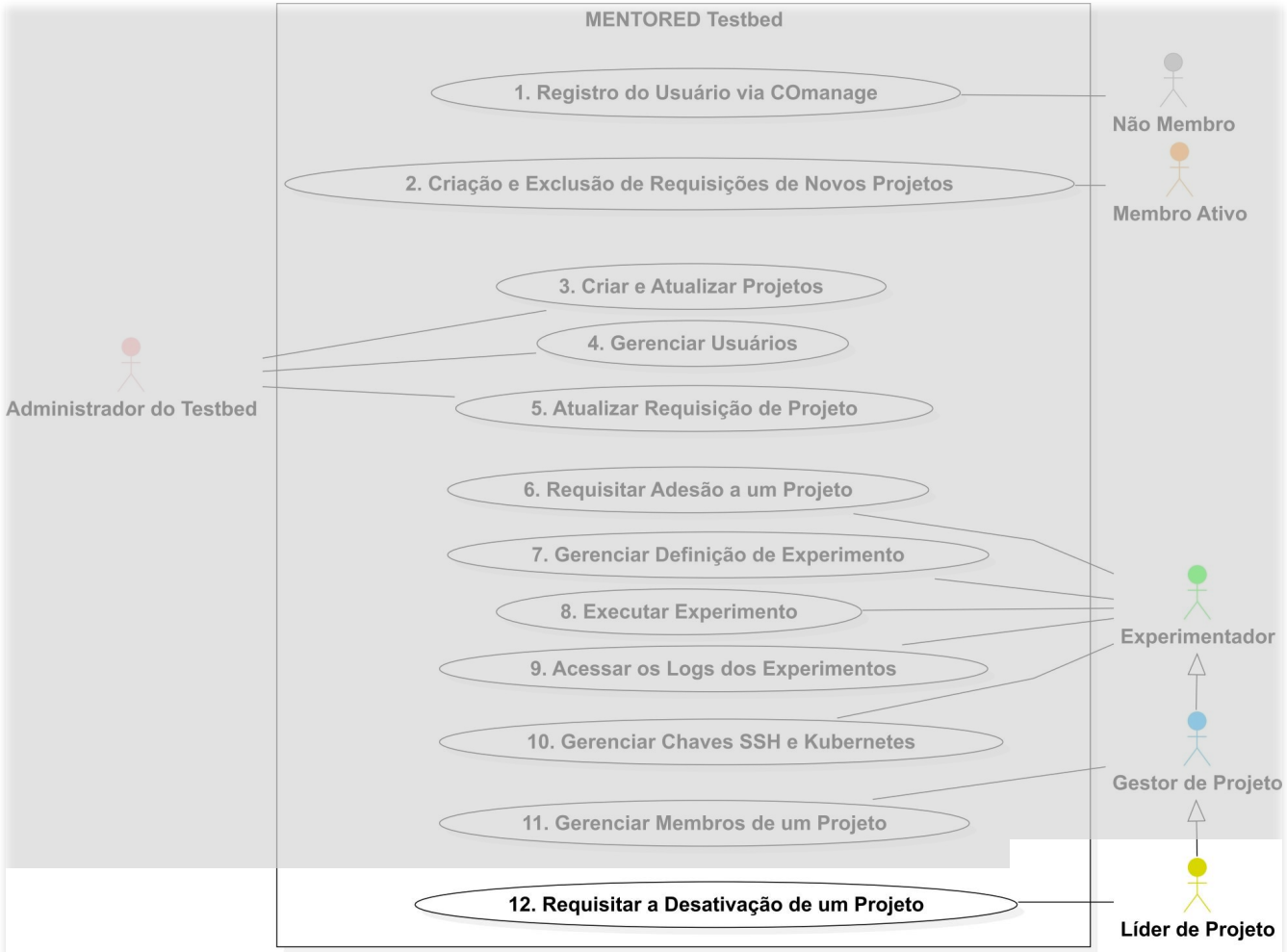
Mentored Testbed
Gestão de Projetos e Times

- **Gestor de Projeto**: responsável por administrar os usuários e experimentos dentro de um projeto.
  - Pode realizar as mesmas funções do Experimentador
  - Tem permissão para adicionar e remover membros do projeto



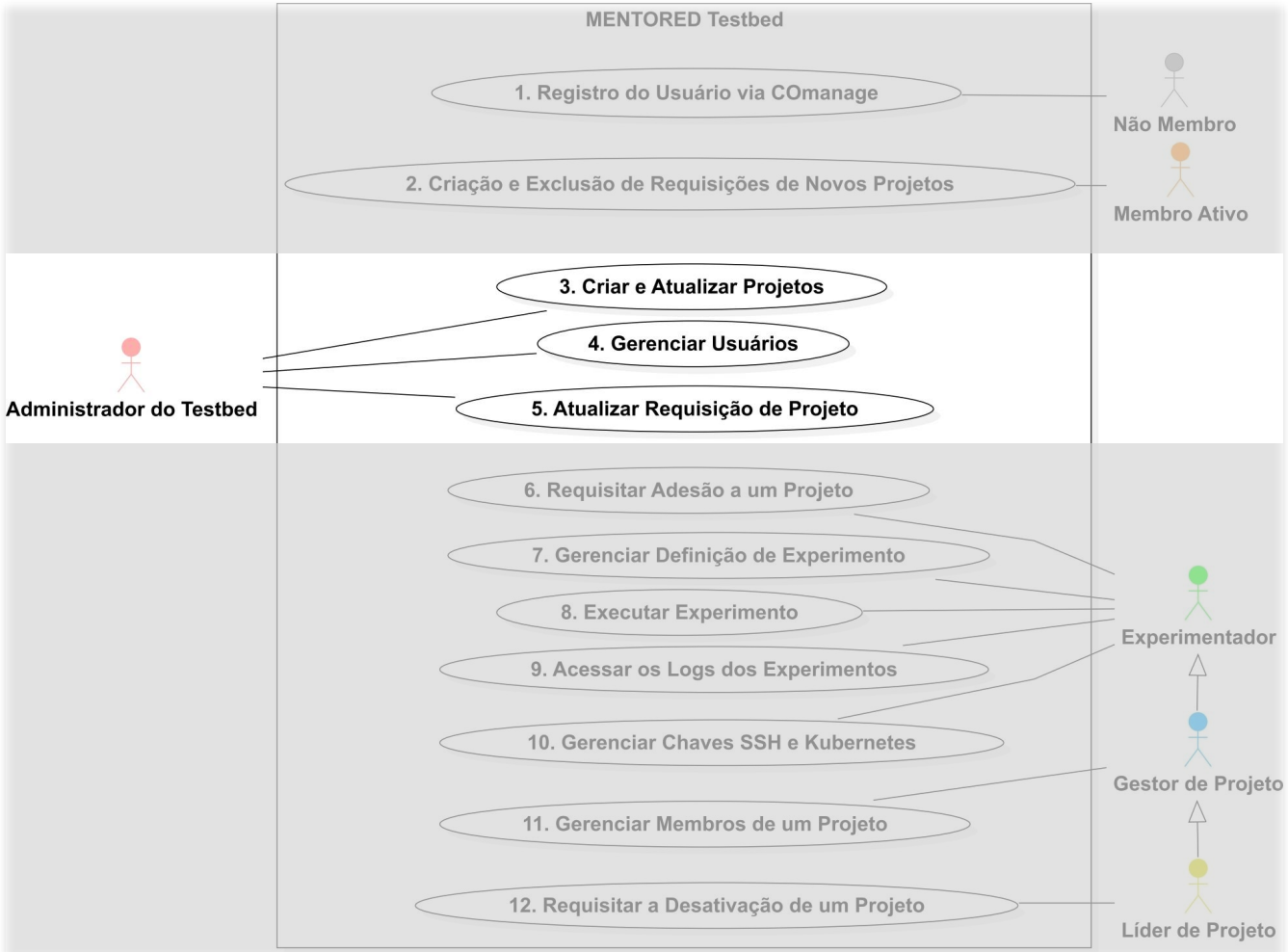
Mentored Testbed
Gestão de Projetos e Times

- **Líder de Projeto**: papel designado ao usuário após ter um projeto aceito.
  - Maior privilégio dentro de um projeto.
  - Possui os mesmos direitos concedidos aos papéis Gestor de Projeto e Experimentador.
  - Pode delegar os papéis Gestor de Projeto e Experimentador aos usuários.



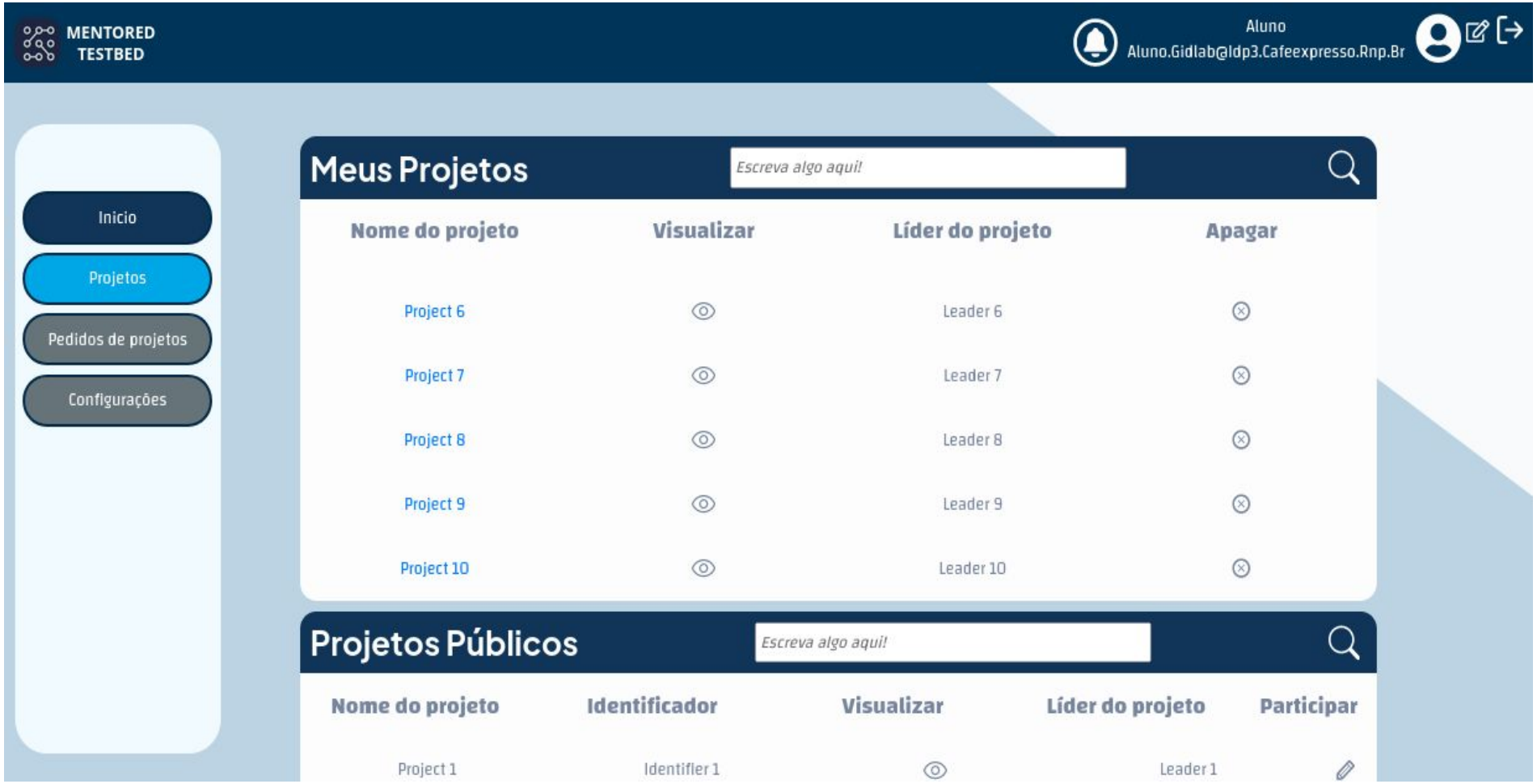
Mentored Testbed
Gestão de Projetos e Times

- **Administrador do Testbed**: Responsável por administrar as requisições de projetos e registros de usuários.



Mentored Testbed
Telas - *Dashboard*

Mentored Testbed
Telas - Projetos

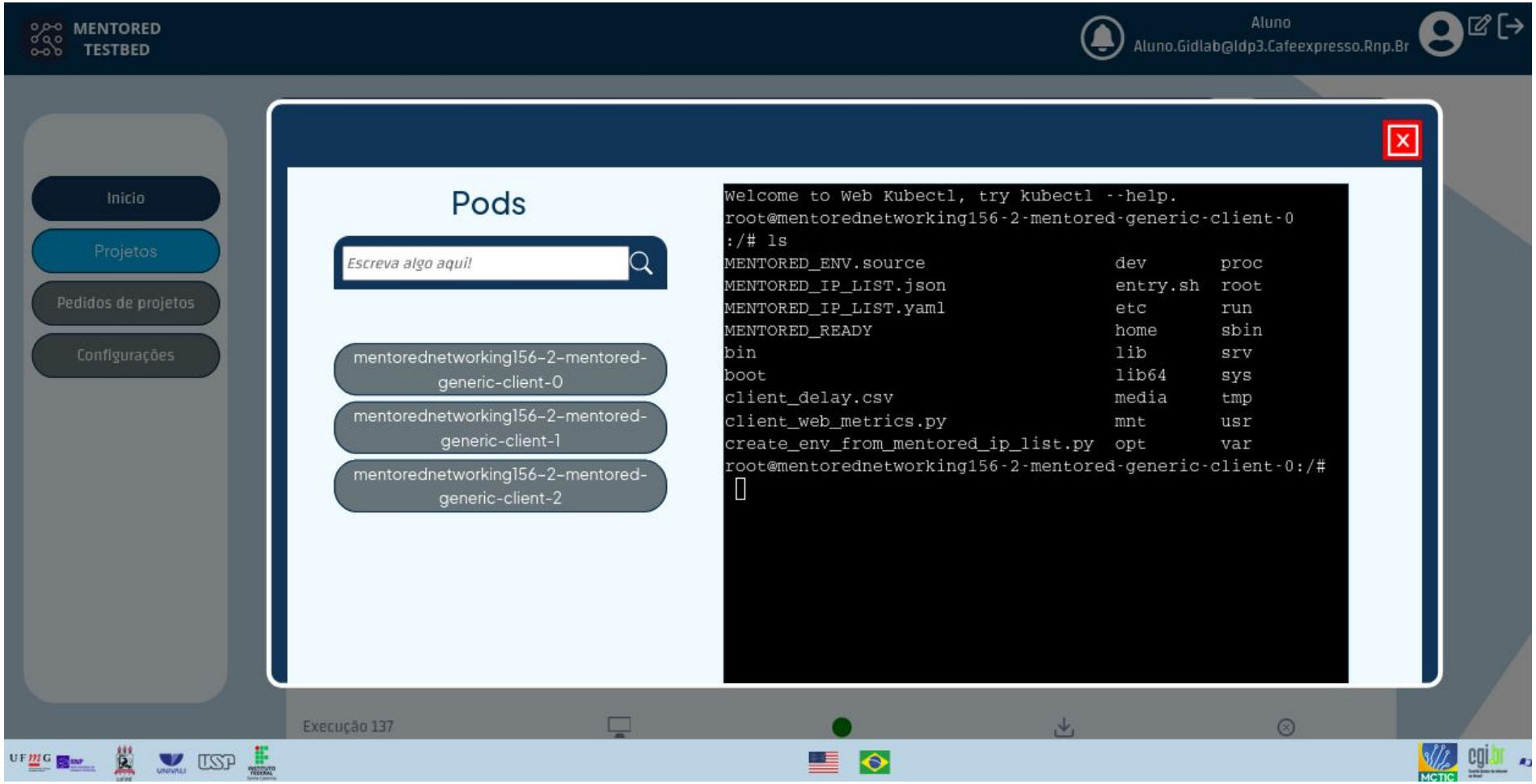


Mentored Testbed

Telas - Definição de Experimentos

Mentored Testbed

Telas - Monitoramento em Tempo Real



Atividades Práticas

Prática
Tipos de ataques

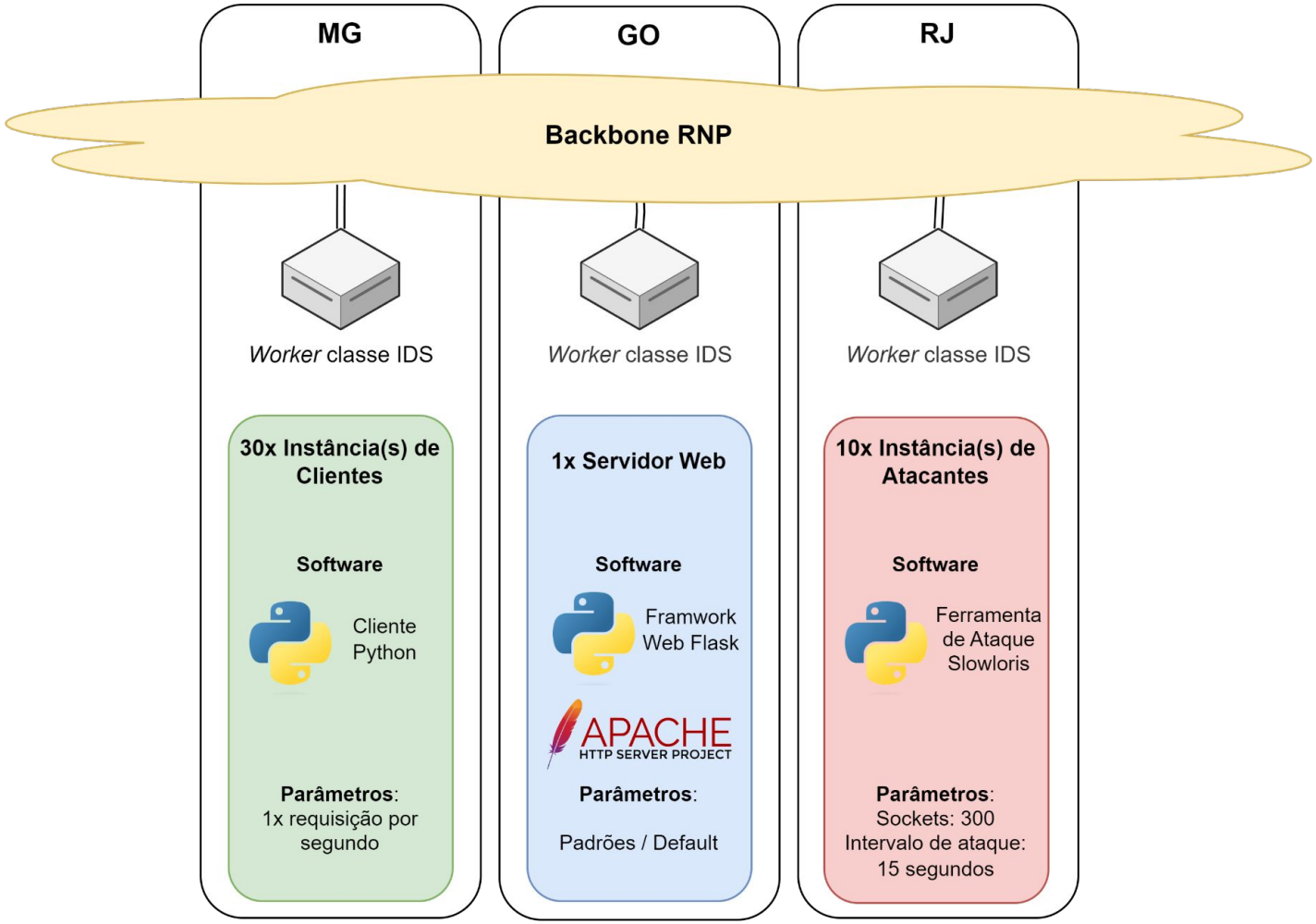
- Grupo-1
  - Ataque com Slowloris
    - *Um ataque "low and slow" é um tipo de ataque DoS ou DDoS que depende de um pequeno streaming de tráfego muito lento visando recursos de aplicativos ou servidores.*
- Grupo-2
  - Ataque com Hping3
    - Um ataque com hping envia uma grande quantidade de tráfego de rede para um sistema-alvo, visando sobrecarregá-lo e torná-lo inacessível para usuários legítimos.

Diferença entre ataques
Hping3 vs Slowloris

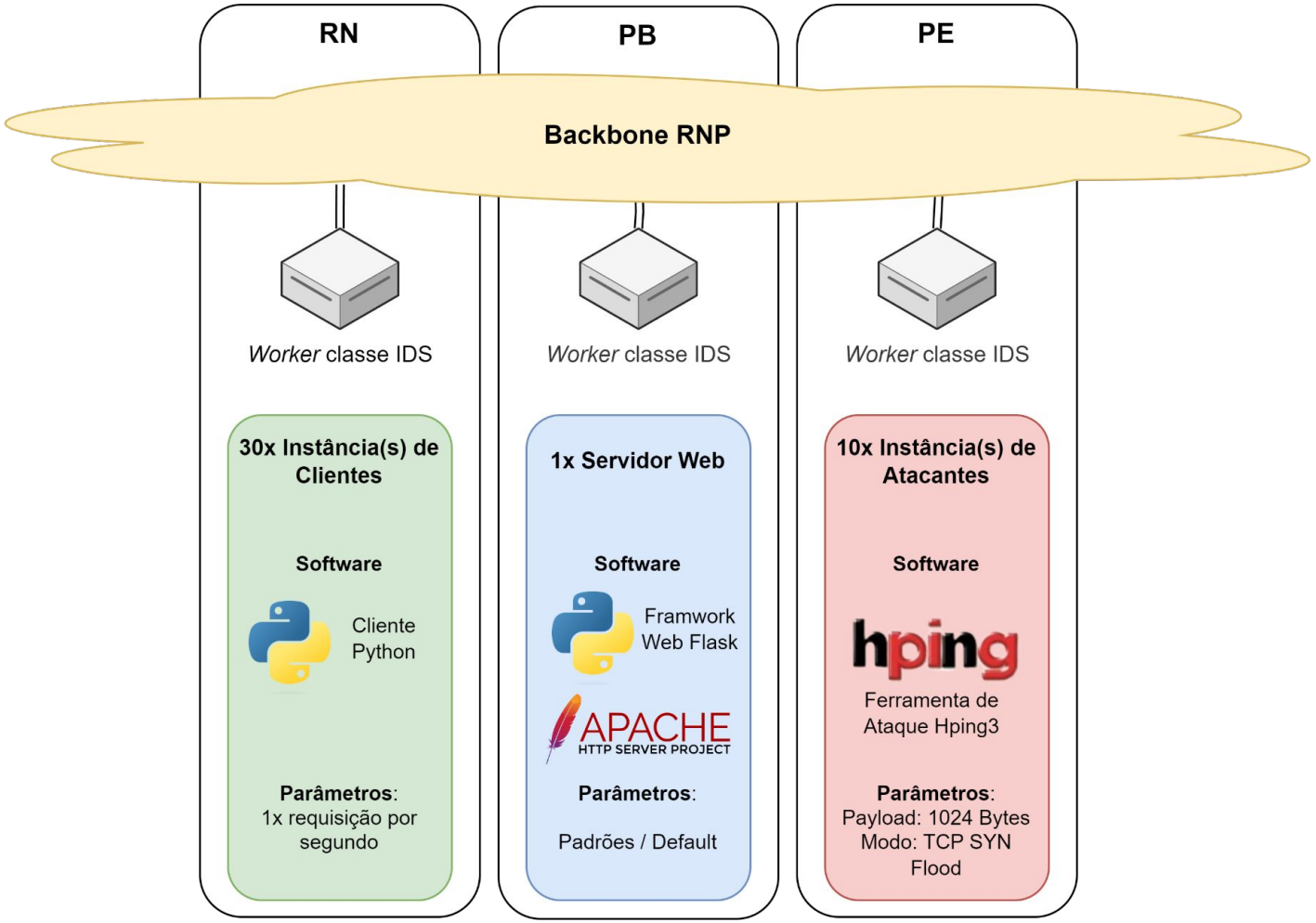
Ataque	**Camada de operação**	**Consumo de banda**
Hping3	Layer 3 (ex: TCP SYN Flood, etc)	Alto
SlowLoris	Layer 7 - Aplicações como servidores *Web*	Baixo

Experimentos
Comportamento do ataque

Grupo 1
Configuração do ataque com Slowloris



Grupo 2
Configuração do ataque com Hping3



Vítima

Parte do código responsável pelo servidor

```yaml
name: mentored_experiment
nodeactors:
  - name: 'na-server'
    persitent_volume_path: "/app/packets.pcap"
    replicas: 1
    containers:
      - name: tshark
        image: ghcr.io/mentoredtestbed/mentored-tshark
        command: ["/entry.sh"]
        args: ["tshark", "-i", "net1", "-x", "-w", "packets.pcap"]
        env:
          - name: TIMEOUT_CMD
            value: "300"
      - name: 'server'
        image: ghcr.io/mentoredtestbed/generic-apache-flask-webserver:latest
        ports:
          - containerPort: 80
        resources:
          requests:
            memory: "1G"
            cpu: "1"
          limits:
            memory: "2G"
            cpu: "2"
    region: 'ids-pe'
```

Clientes

Parte do código responsável pelos clientes

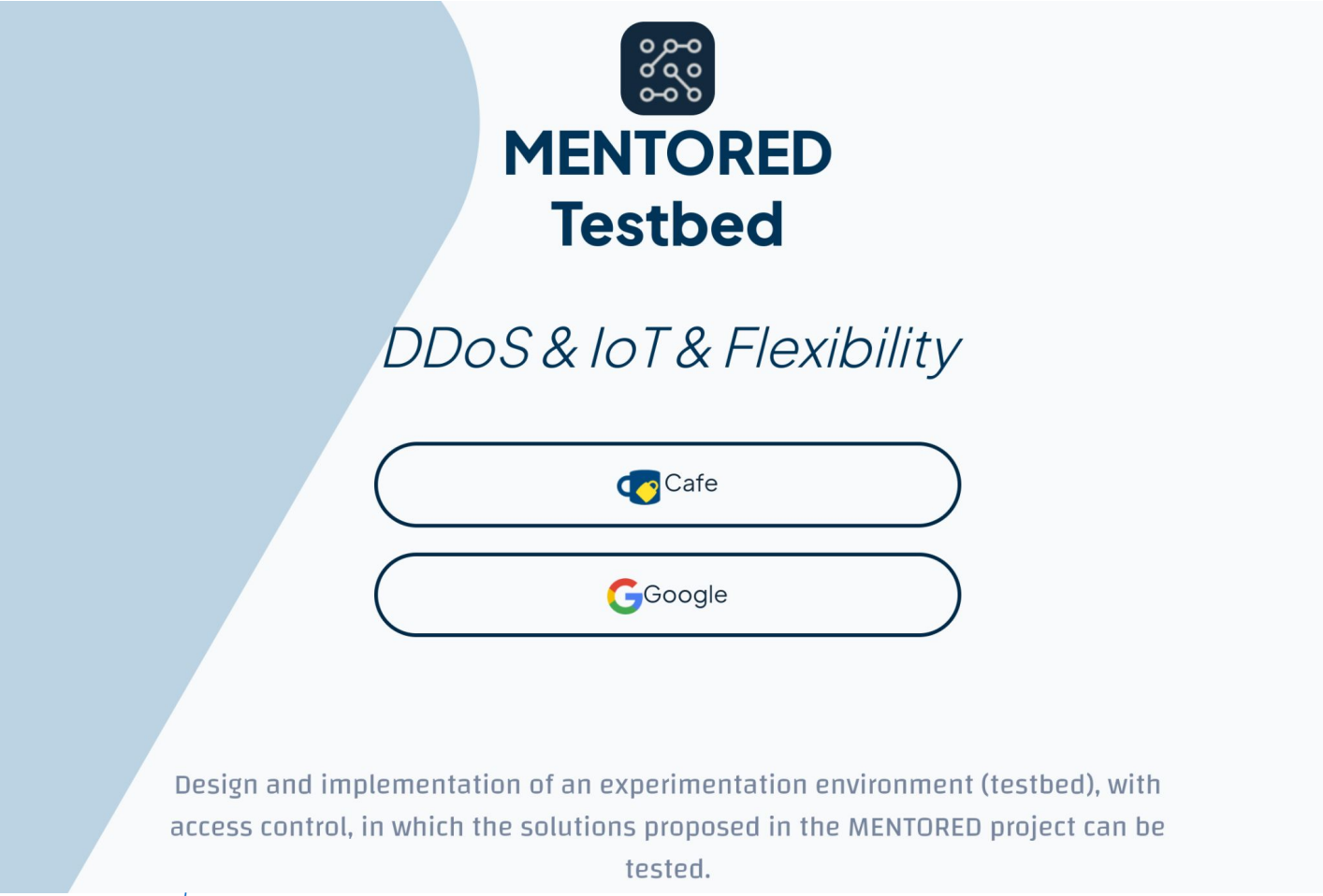
```yaml
- name: 'generic-client-pb'
  persitent_volume_path: "/client_delay.csv"
  replicas: 10
  containers:
    - name: 'client-pb'
      image: ghcr.io/mentoredtestbed/generic-client:latest
      command: ["/entry.sh"]
      args: ['python3', 'client_web_metrics.py', "1", "1"]
      env:
        - name: TIMEOUT_CMD
          value: "300"
        - name: ADD_SERVER_IP_TO_COMMAND
          value: "true"
      resources:
        requests:
          memory: "64Mi"
          cpu: "100m"
        limits:
          memory: "128M"
          cpu: "200m"
  region: 'ids-pb'
```

Atacante

Parte do código responsável pelos atacantes

```yaml
- name: 'generic-botnet-go'
  persitent_volume_path: "/MENTORED_IP_LIST.yaml"
  replicas: 4
  containers:
    - name: 'botnet-go'
      image: ghcr.io/mentoredtestbed/generic-botnet:latest
      command: ["/entry.sh"]
      args: ["slowloris", "-p", "80"]
      #args: ["hping3", "-S", "--faster", "-p", "80"]
      #args: ["hping3", "-S", "--flood", "-S", "-d 1024", "-p", "80"]
      env:
        - name: PROTOCOL
          value: "ICMP"
        - name: TIMEOUT_CMD
          value: "180"
        - name: TIME_WAIT_START
          value: "60"
        - name: ADD_SERVER_IP_TO_COMMAND
          value: "true"
      resources:
        requests:
          memory: "64Mi"
          cpu: "100m"
        limits:
          memory: "128M"
          cpu: "200m"
  region: 'ids-go'
```

Atividade Prática
Login no portal do MENTORED *Testbed*

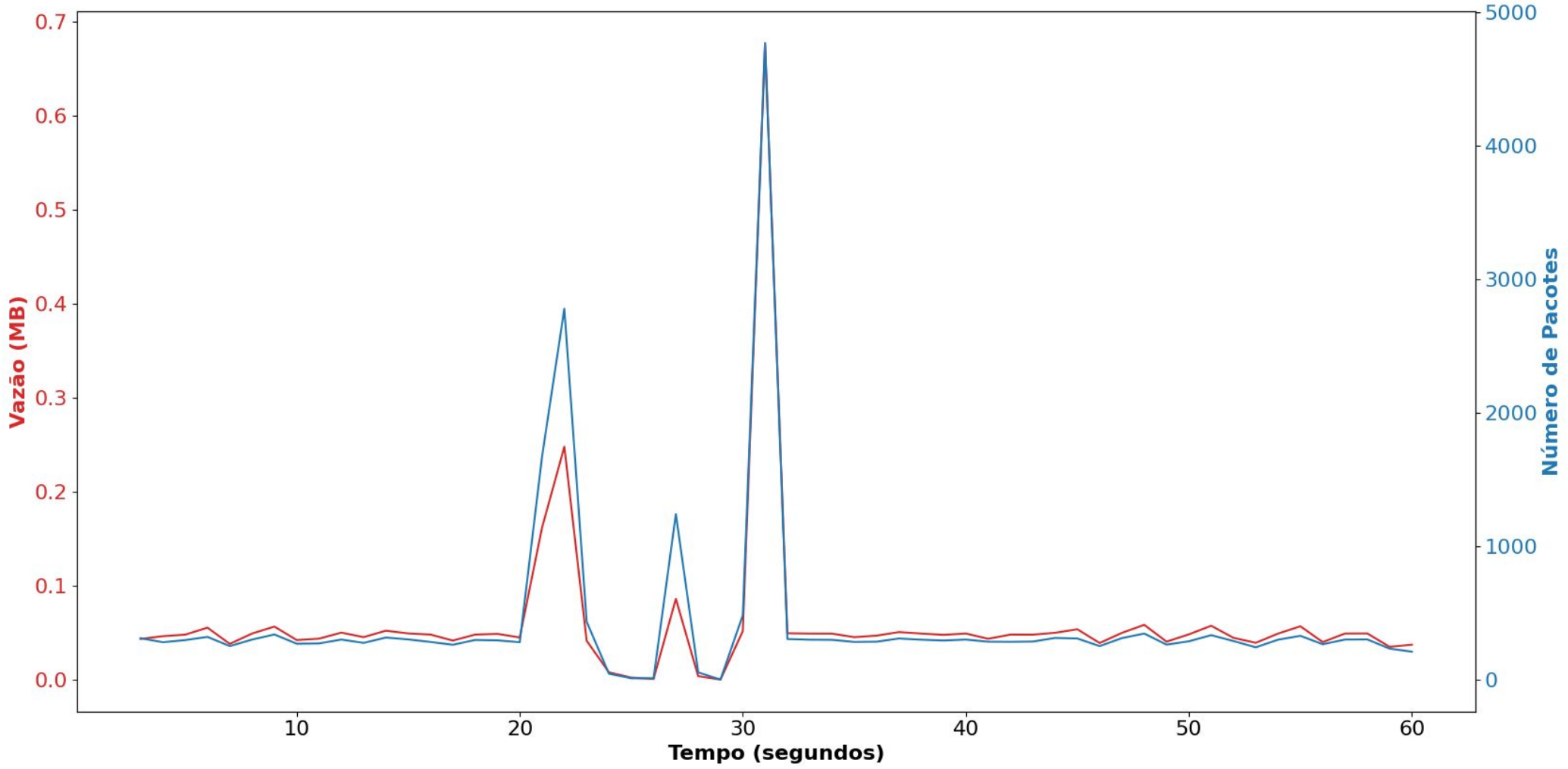


*https://portal.mentored.ccsc-research.org
*https://github.com/mentoredtestbed/minicurso-sbrc-2024-testbeds

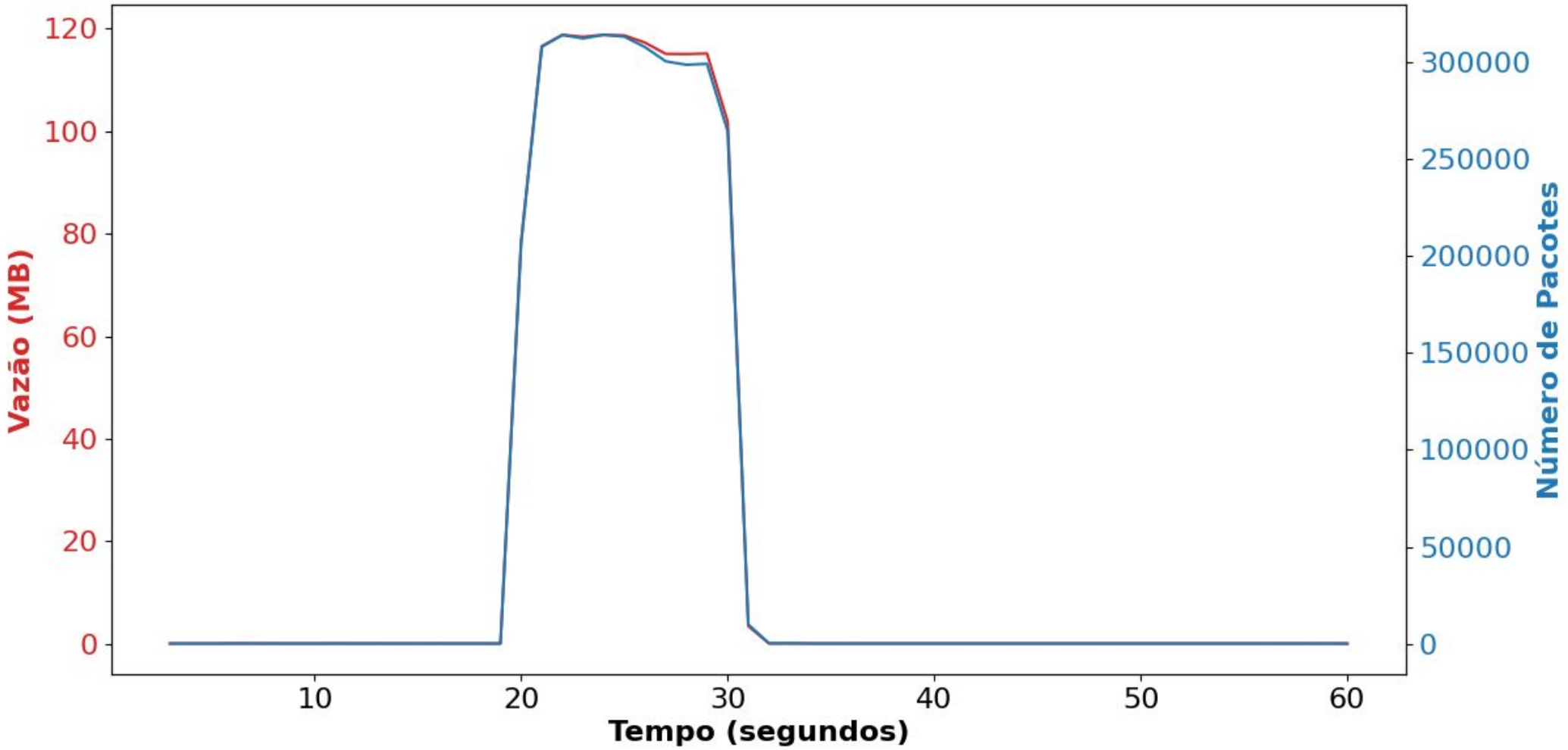
Resultado
Arquivos resultantes do ataque

- Arquivo com a captura de tráfego da vítima;
  - *packets.pcap*
- Arquivos com o tempo de respostas das requisições GET dos clientes;
  - *client_delay.csv*
- Arquivo contendo a lista de todos os IPs classificados por tipo e região;
  - *MENTORED_IP_LIST.yaml*
- Arquivo contendo os *logs* do experimento;
  - *experiment_logs.tar*
- Ferramentas utilizadas na criação dos gráficos;
  - *https://github.com/mentoredtestbed/minicurso-sbrc-2024-testbeds*

Grupo 1
Resultado do ataque com Slowloris

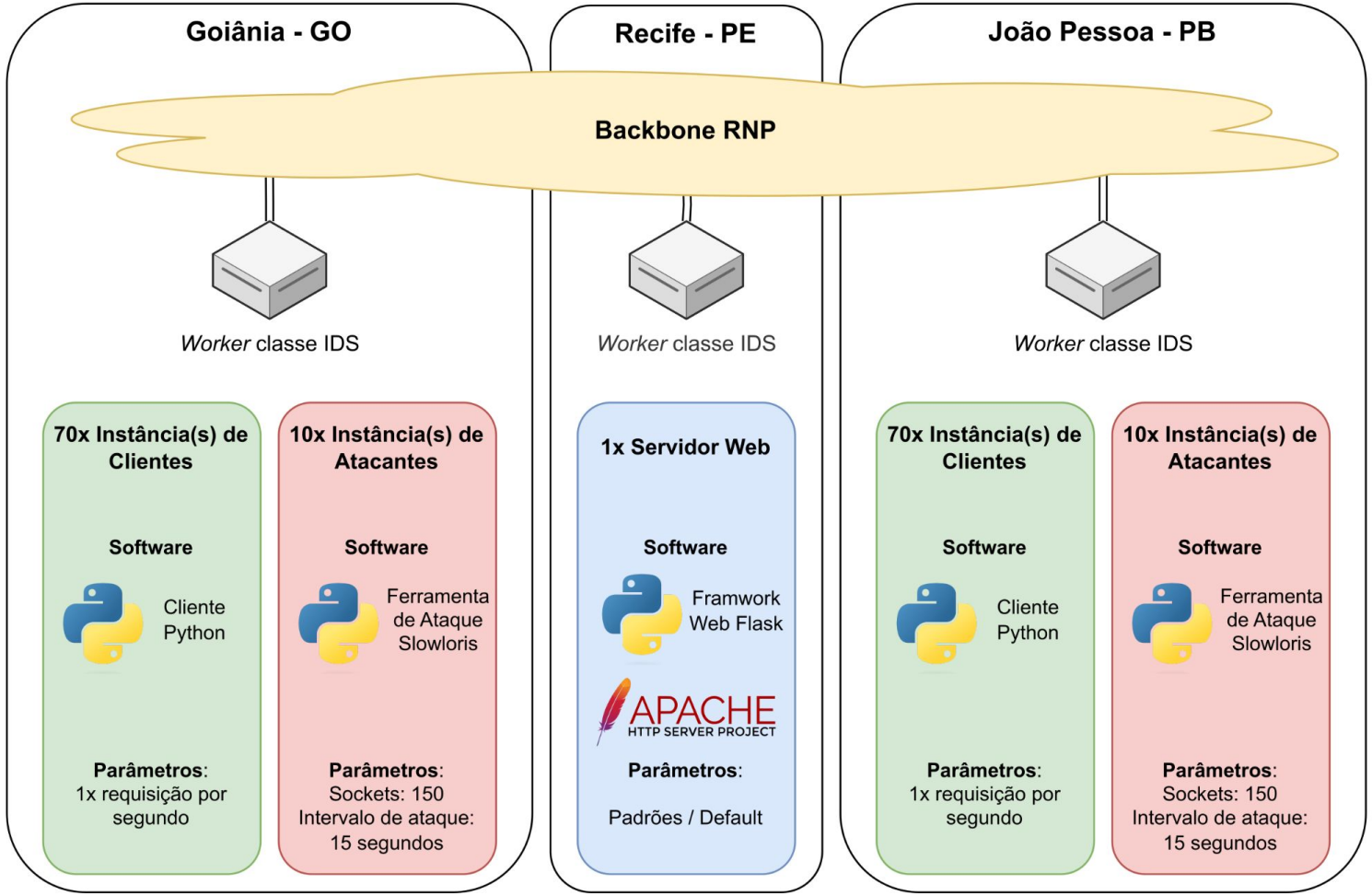


Grupo 2
Resultado do ataque com Hping3



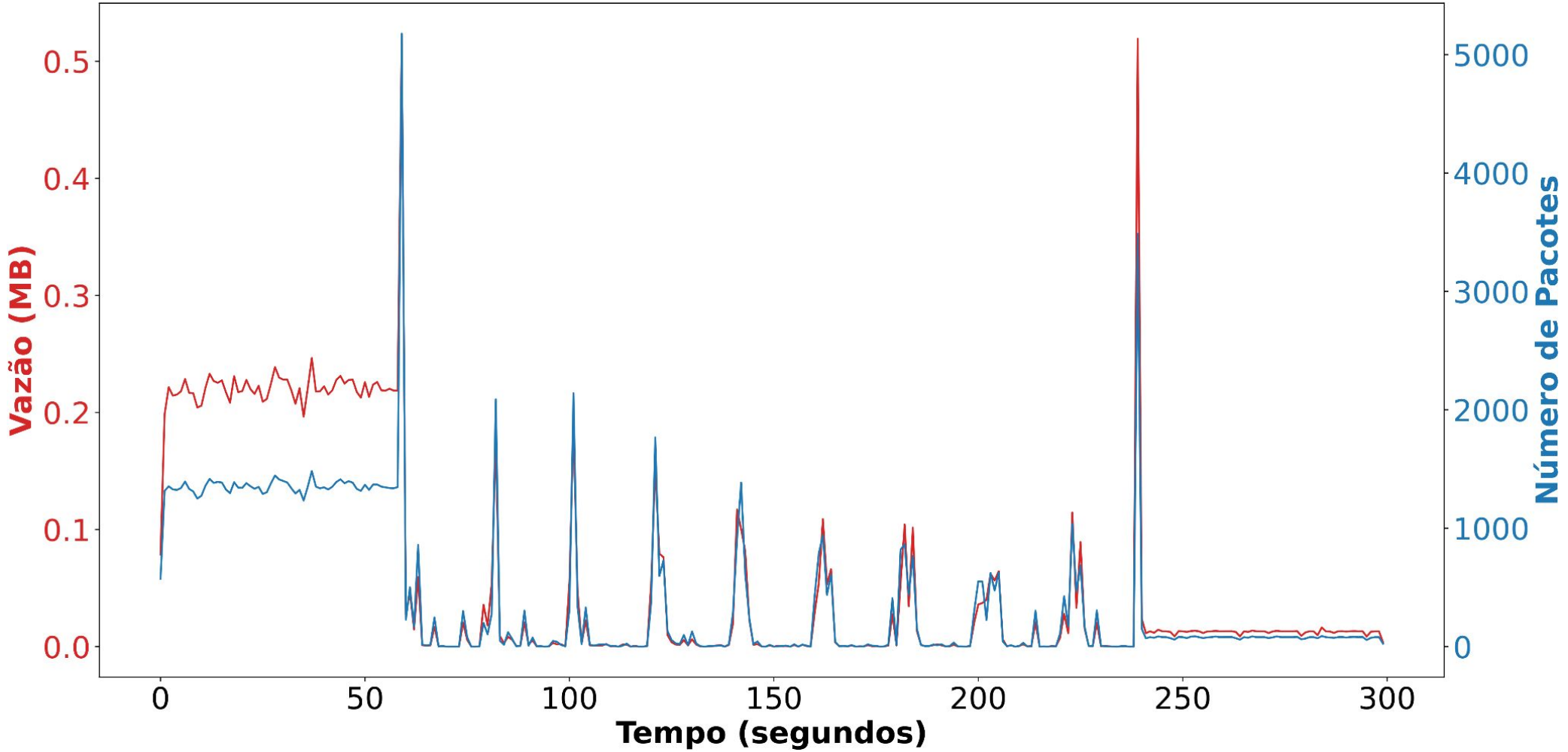
Experimentos
Comportamento do ataque

Capítulo do Livro
Configuração do ataque com Slowloris

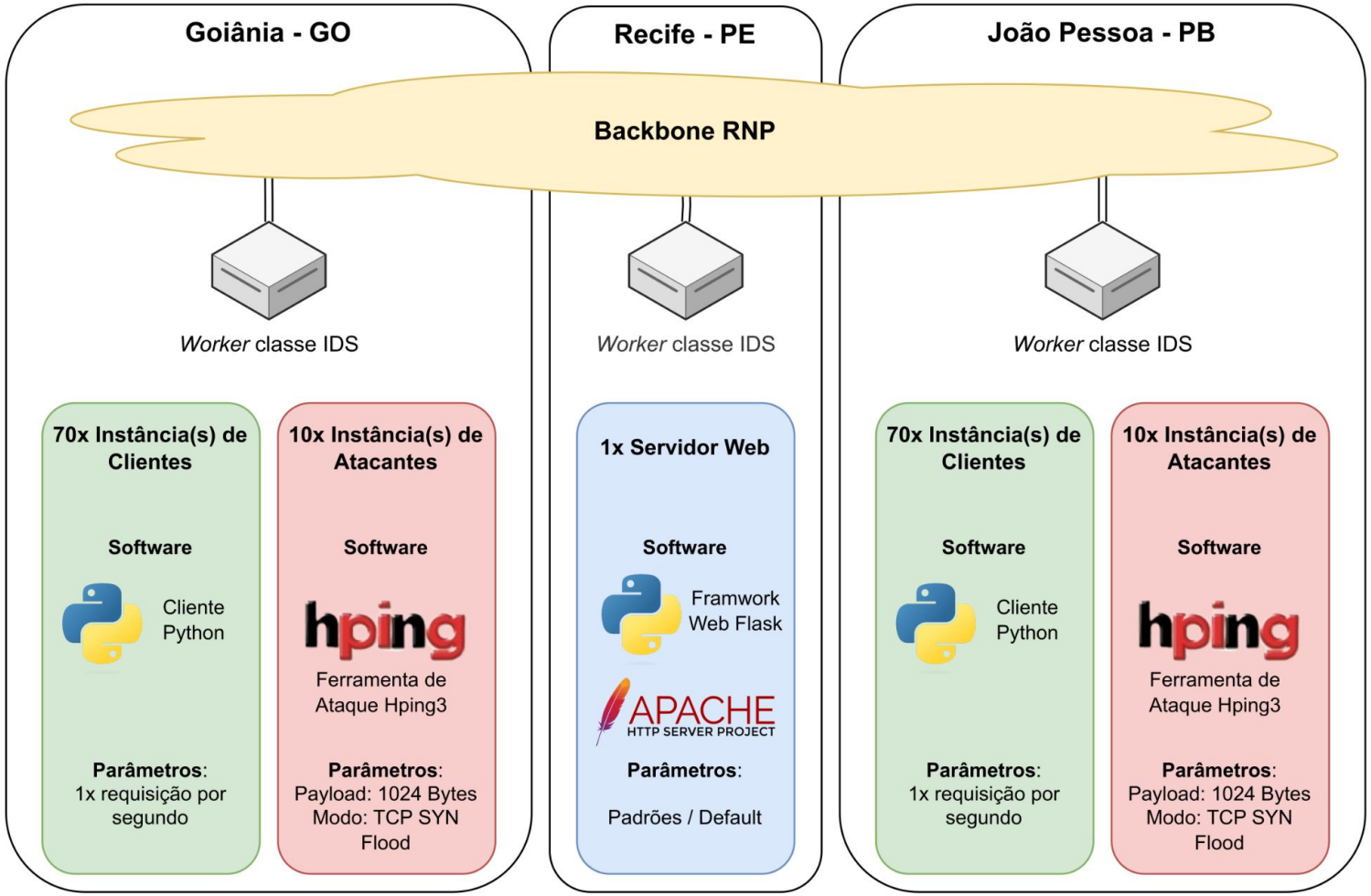


Slowloris

Gráfico com o ataque utilizando o Slowloris

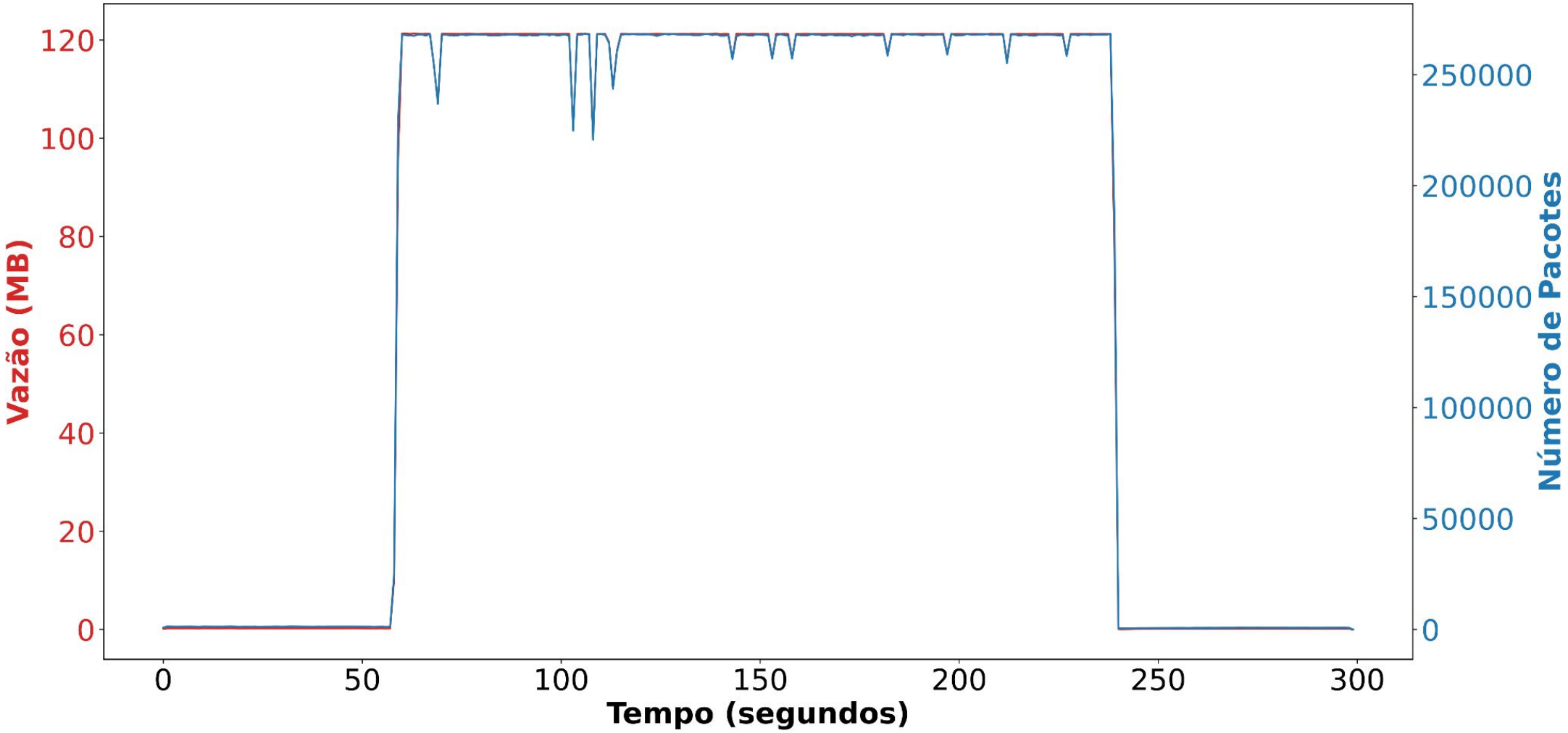


Capítulo do Livro
Configuração do ataque com Hping3



Hping3

Gráfico com o ataque utilizando o Hping3



Considerações Finais

Considerações finais

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

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

Github

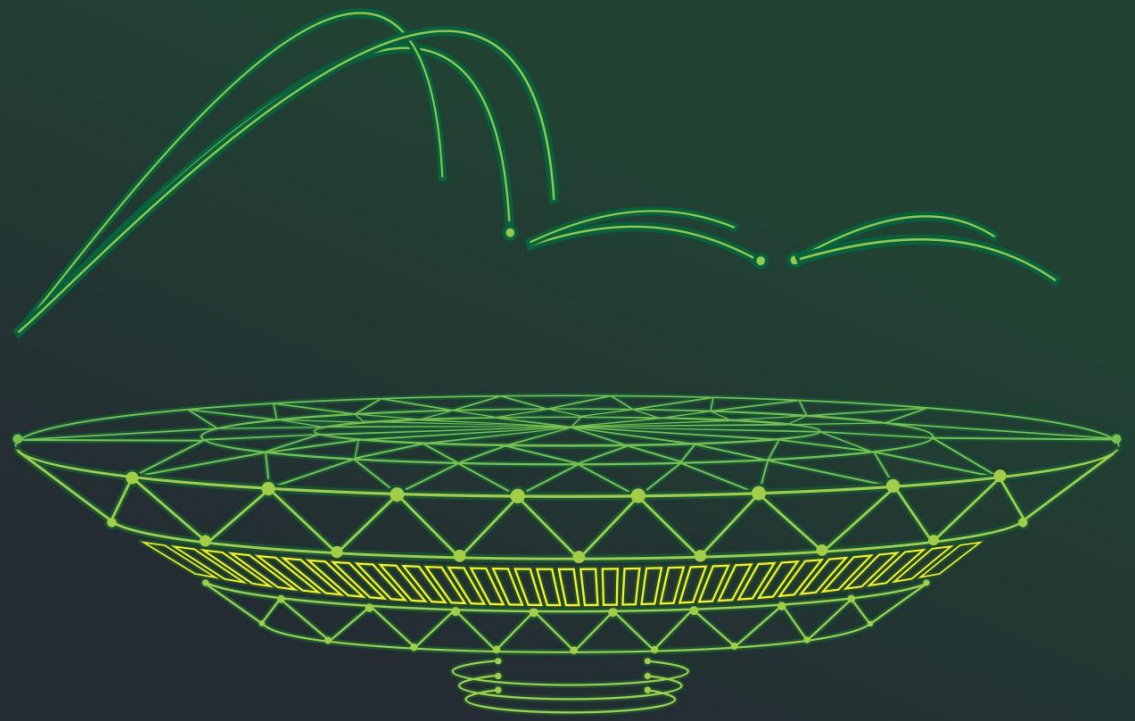
Fontes & Leitura Complementar

- Fontes
  - Em algumas imagens autorais foi feito uso de ícones providos por https://uxwing.com e https://www.flaticon.com

Testbeds para Pesquisa Experimental em Cibersegurança: Da Teoria à Prática

Apresentadores:

- Michelle S. Wangham
- Bruno H. Meyer
- Davi D. Gemmer
- Khalil G. Q. de Santana
- Luiz Eduardo Folly de Campos
- Emerson Ribeiro de Mello



SBRC'24

Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos.