



# DA MODELAGEM À EXPERIMENTAÇÃO PREDIZENDO E DETECTANDO ATAQUES DDOS E ZERO-DAY

Michele Nogueira, D.Sc.  
Pesquisadora Responsável  
michele@dcc.ufmg.br

23 de Maio de 2022



23<sup>o</sup> WRNP  
Workshop RNP



# Panorama do Projeto

## Parceiros



MENTORED



# Panorama do Projeto

## Equipe de Concepção



MENTORED



Michele Nogueira  
**Pesquisadora Responsável/  
Líder WP2**



José Suruagy  
**Pesquisador Principal e  
Líder WP1**



Aldri Santos  
**Pesquisador Principal e  
Líder WP3**



Michelle Wangham  
**Pesquisadora Associada e  
Líder WP4**



Paulo Gonçalves  
**Pesquisador Associado**



Daniel Batista  
**Pesquisador Associado**



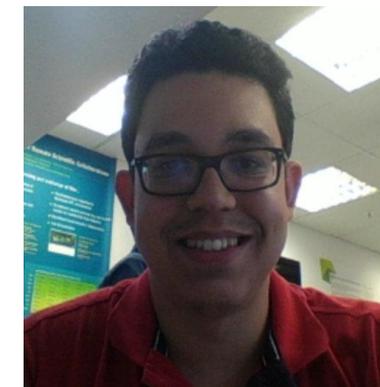
Emerson Melo  
**Pesquisador Associado**



Iara Machado  
**Apoio**



André Marins  
**Apoio**



Clayton Reis  
**Apoio**



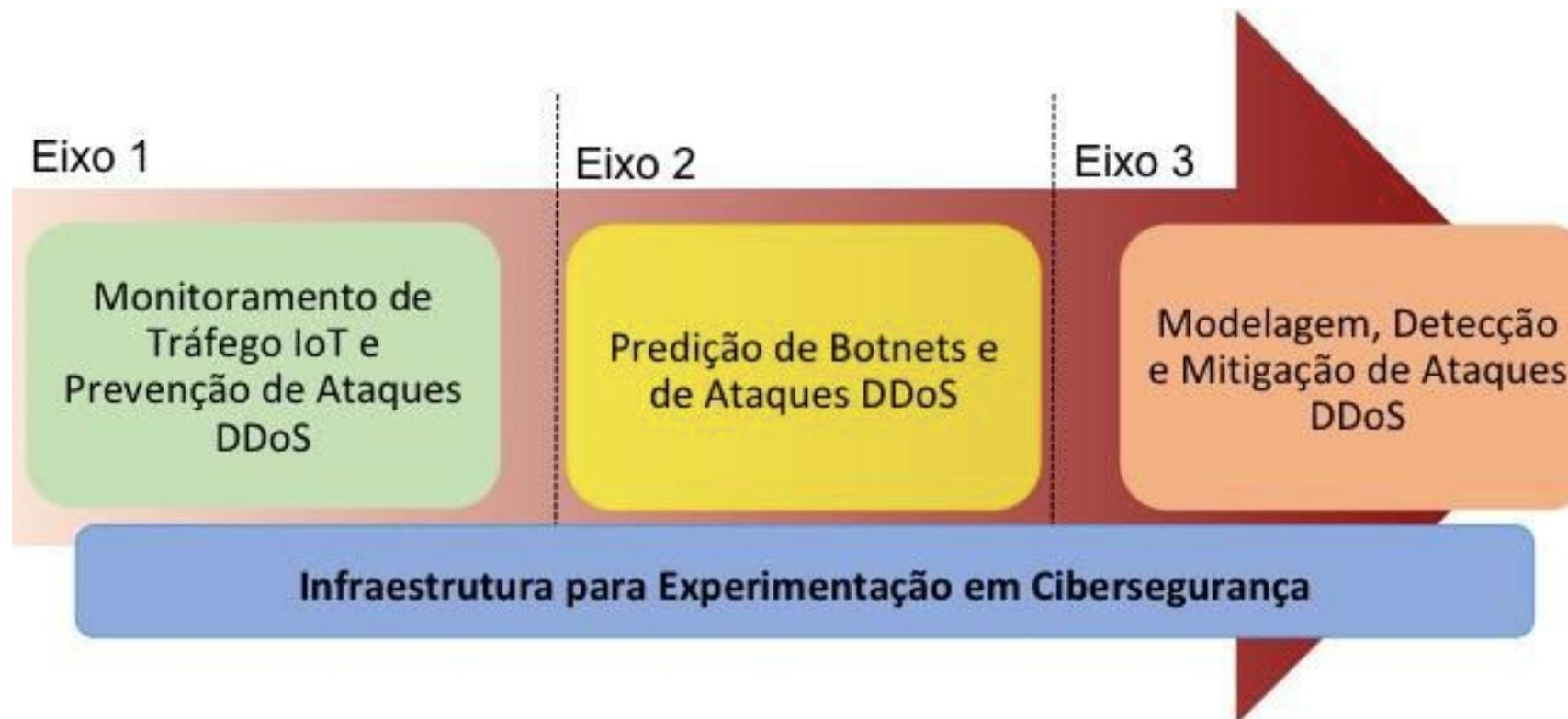
**Identificar, modelar e avaliar** comportamentos maliciosos associados à IoT de forma a auxiliar na construção de soluções avançadas e coordenadas para possibilitar:  
**prevenção, predição, detecção e mitigação**  
de ataques DDoS e Zero-Day

# Visão Geral

## Arcabouço de Soluções



MENTORED



# Visão Geral

## Pacotes de Trabalho



MENTORED

WP1

José Suruagy  
(líder)

Paulo  
Gonçalves

Edilson Lima

WP2

Michele  
Nogueira (líder)

Daniel Batista

Wagner  
Monteverde

WP3

Aldri Santos  
(líder)

Michele  
Nogueira

Edilson Lima

WP4

Michelle  
Wangham (líder)

Emerson Mello

Iara Machado

André Marins

Clayton Reis

# Pacote de Trabalho 4

## Ambiente Experimental - Cibersegurança



MENTORED



Prover um ambiente controlado para experimentação (*testbed*) com cenários da IoT para avaliar propostas de cibersegurança

Quem?

1º Pesquisadores dos WPs

2º Comunidade de Segurança



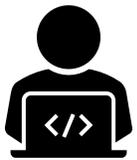
# Pacote de Trabalho 4

## Objetivos Específicos



MENTORED

- Oferecer recursos para experimentação em cenários realistas



**Avaliar soluções contra ataques DDoS e de botnets baseados na IoT**



**Desenvolver metodologias avançadas para prover pesquisa experimental em cibersegurança sob demanda**



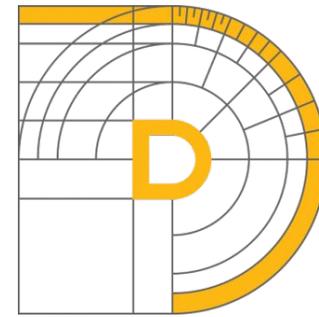
**Apoiar - EaD, capacitações e disseminação (ataques e soluções de segurança)**

# Pacote de Trabalho 4

## Testbeds de Referência



MENTORED



The **DETER** Project

- Metodologia de experimentação em cibersegurança
  - Experimentação replicável, escalável e verificável
  - Redução da complexidade ao criar experimentos de cibersegurança
- Acesso aos recursos físico como servidores e dispositivos IoT

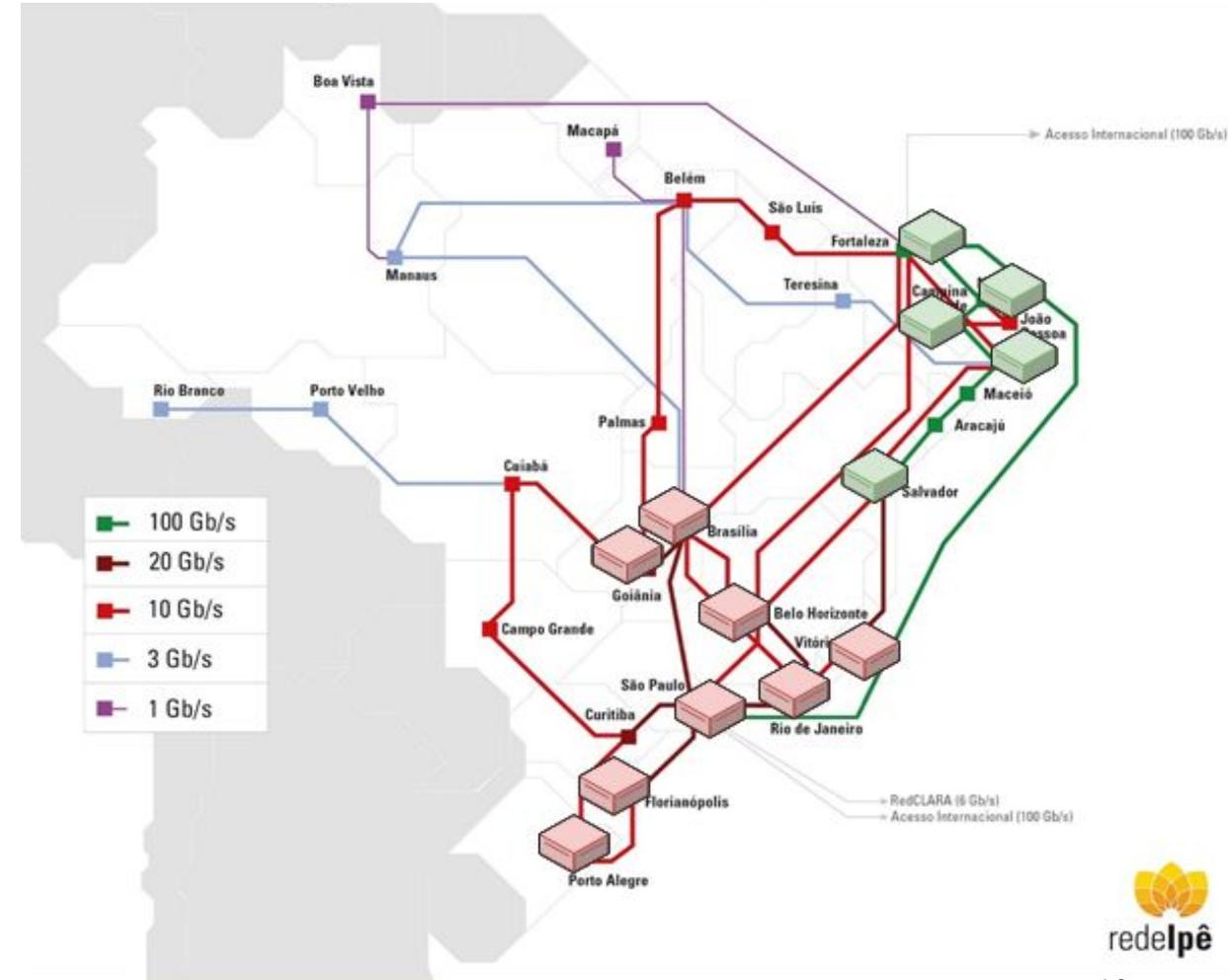
# Infraestrutura Definida por Software

## Alicerce



MENTORED

- **RNP**
- **Recursos**
  - Servidores *bare metal*
  - Links de alta velocidade - 1 a 100Gbps
- **Modelo de Uso**
  - Sob demanda (requer setup inicial)
- **Propósito**
  - Infraestrutura virtualizável e programável
  - Orquestração de recursos em paradigma Cloud-Native



# Infraestrutura Definida por Software (IDS-RNP)

## Vantagens

- Processamento e de armazenamento
- Rede customizável e de longa distância
- Software Livre
- Configurações sob-demanda
- Suporta a inclusão de redes de borda
- Equipe de apoio da RNP



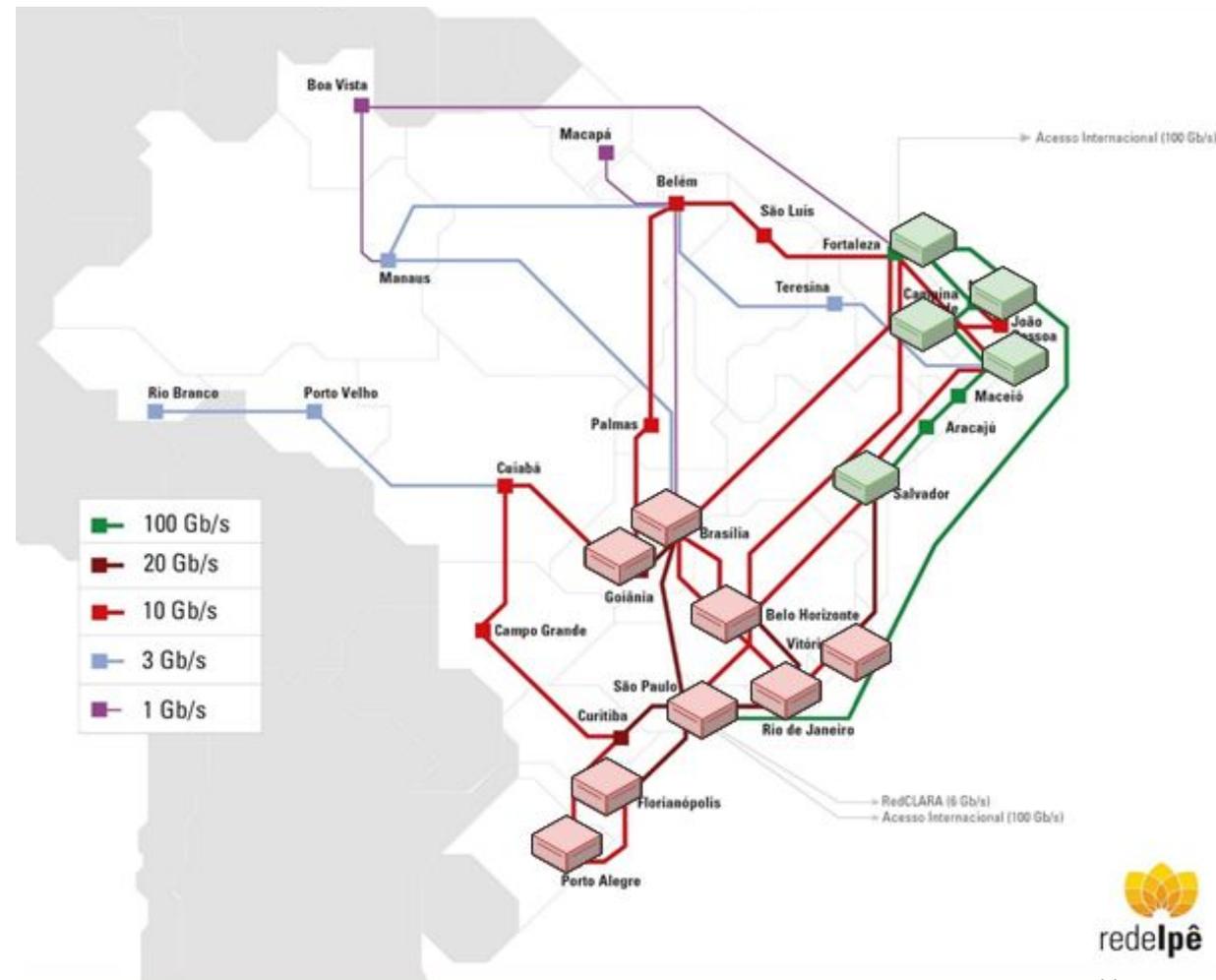
kubernetes



docker



MENTORED

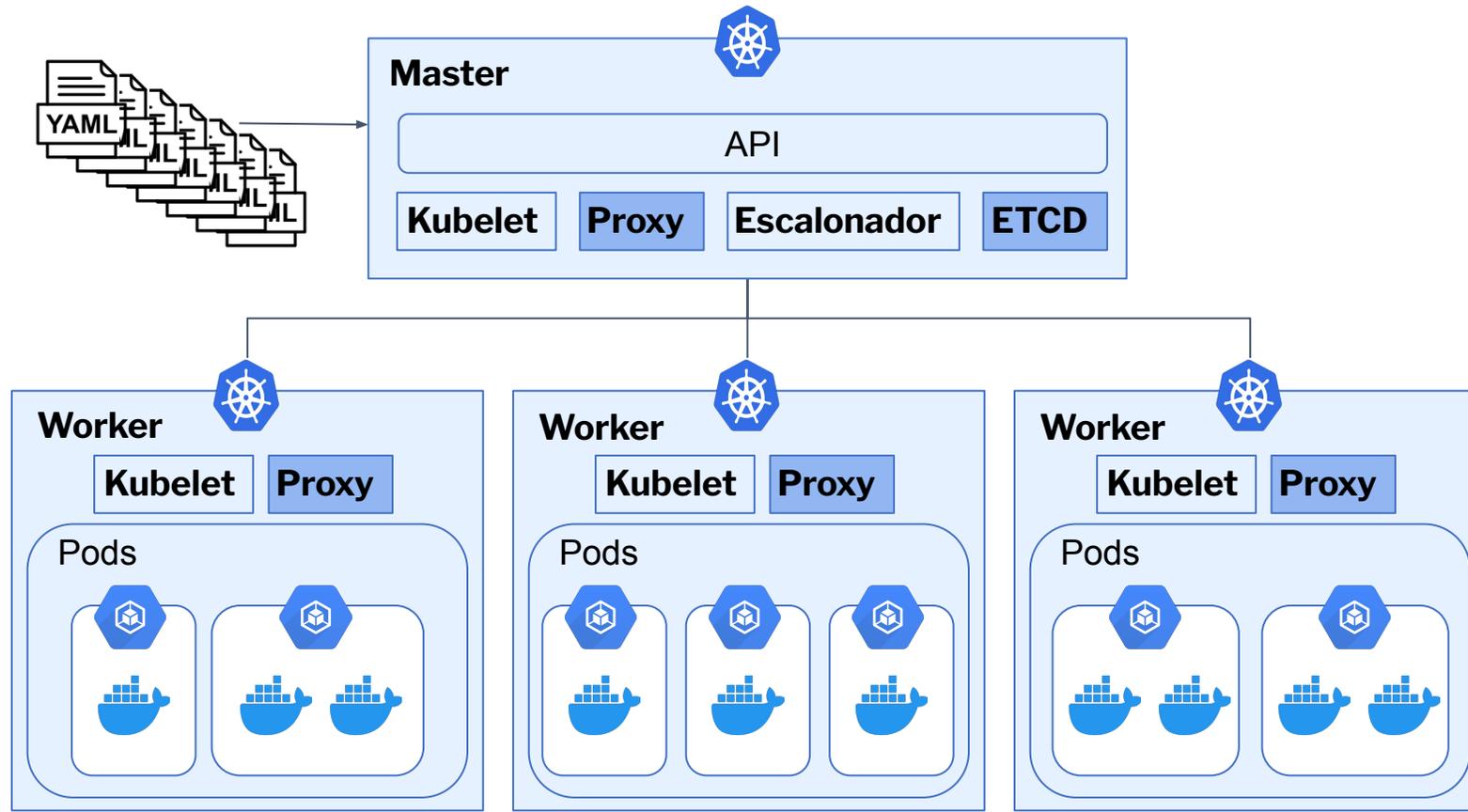


# Infraestructura Definida por Software

## Kubernetes



MENTORED

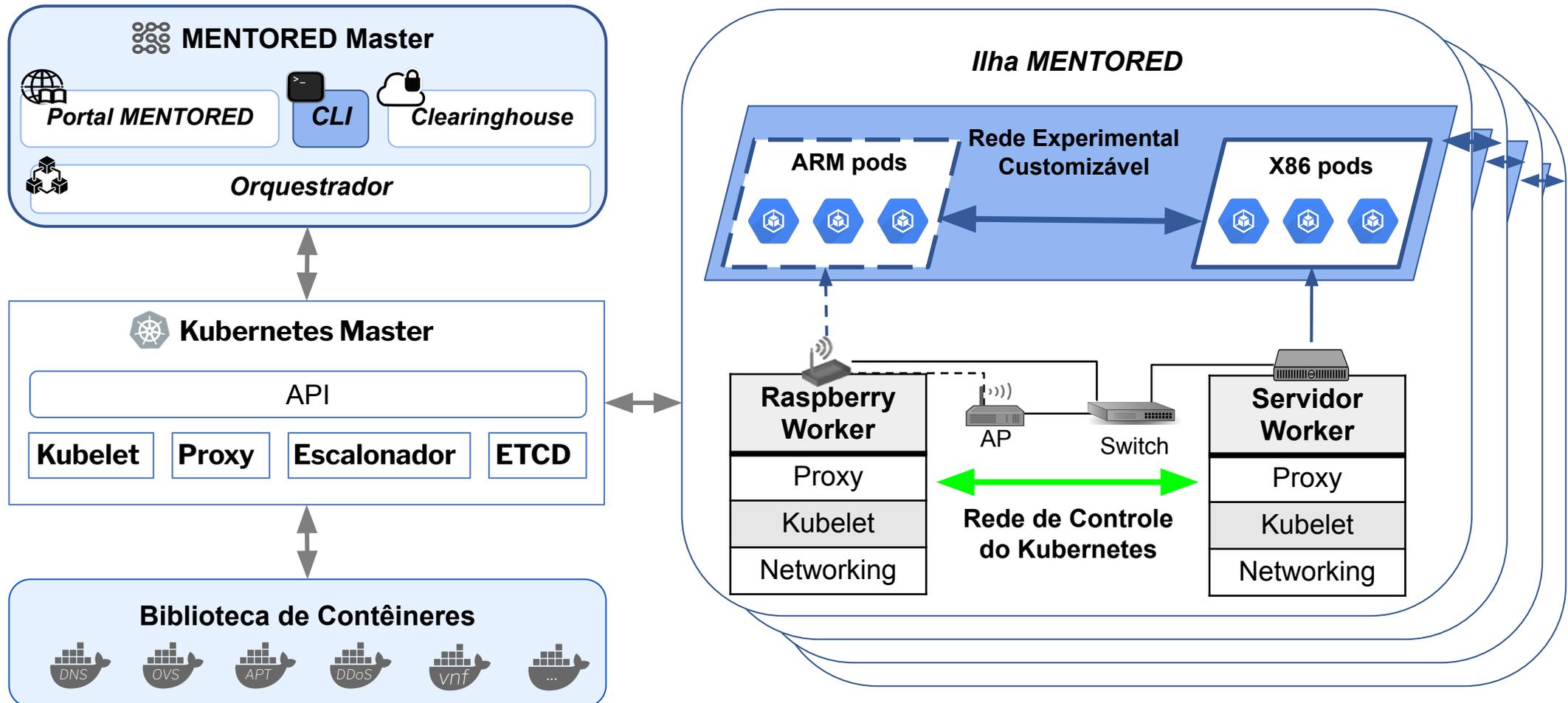


# MENTORED Testbed

## Arquitetura



MENTORED

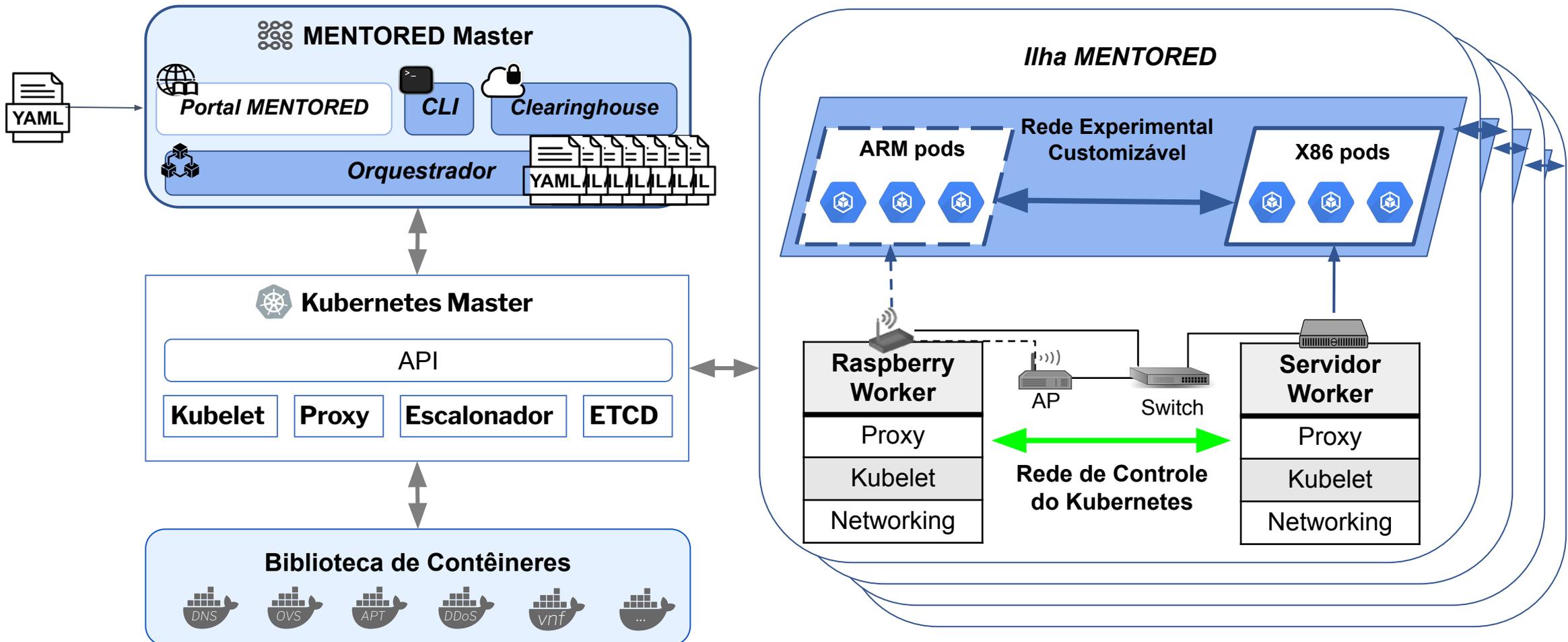


# MENTORED Testbed

## Arquitetura



MENTORED

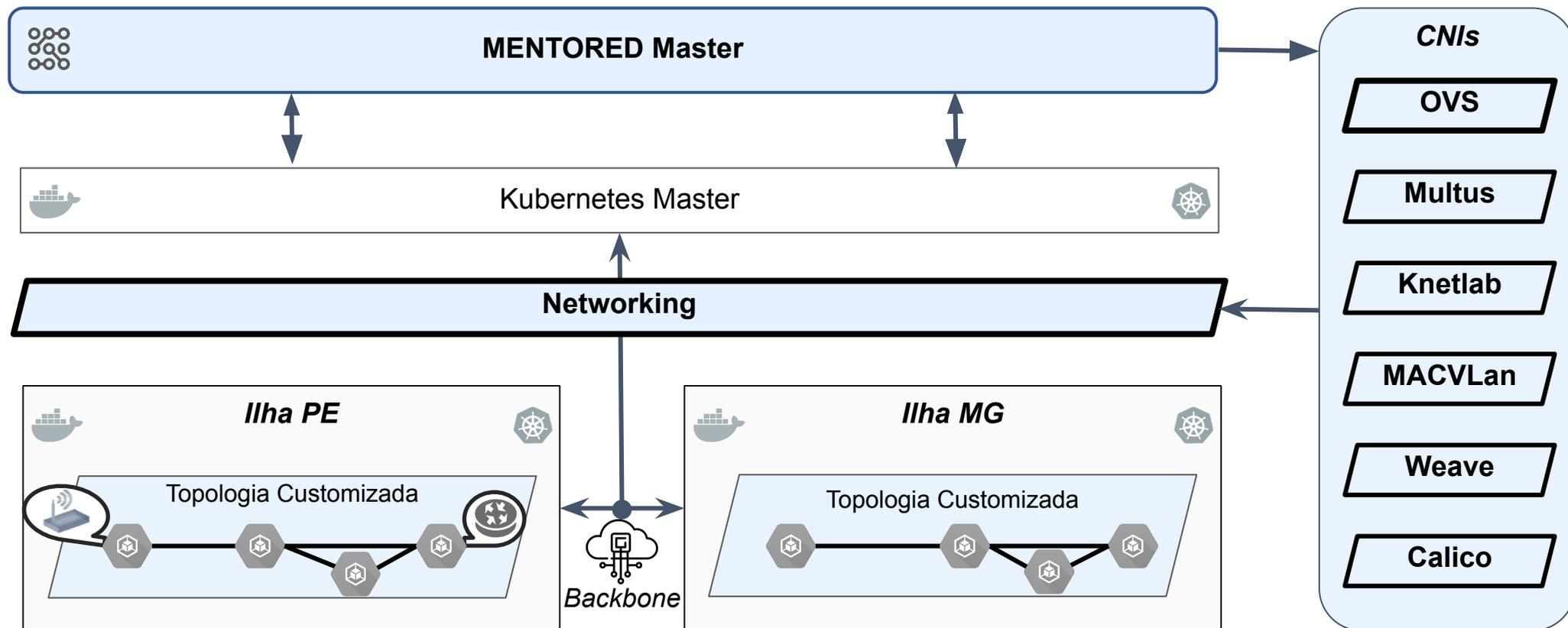


# MENTORED Testbed

## Container Network Interfaces - CNIs



MENTORED

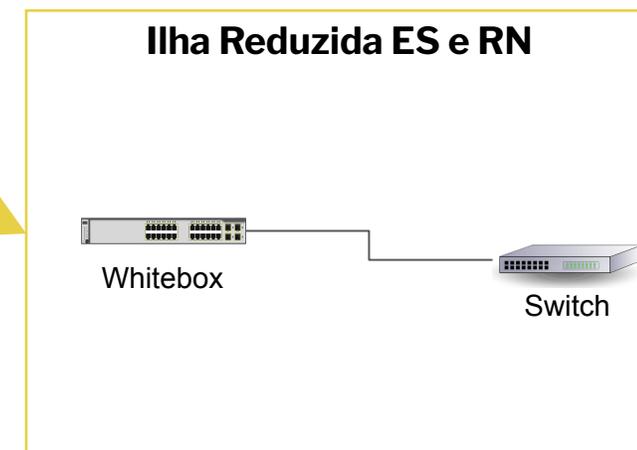
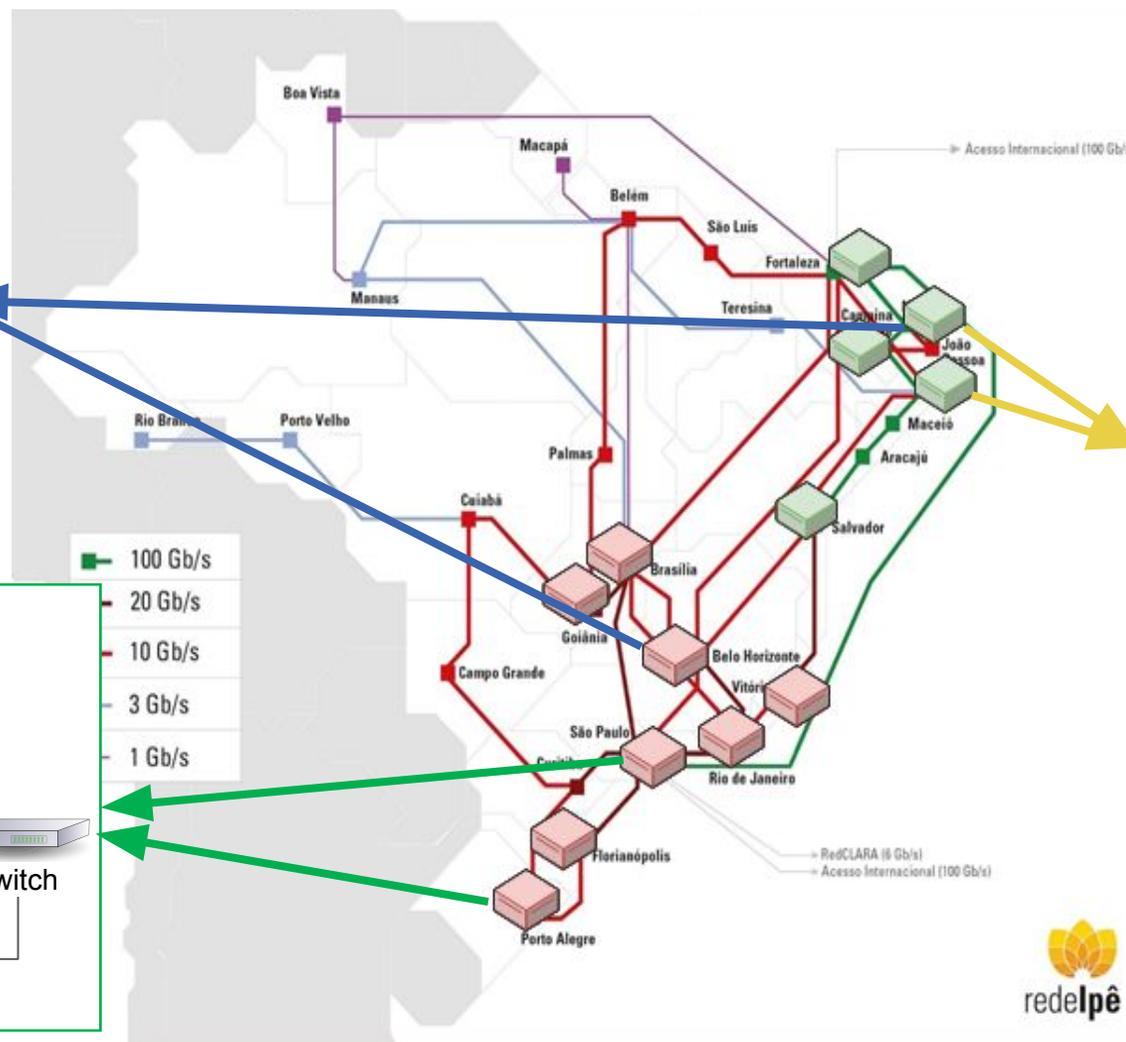
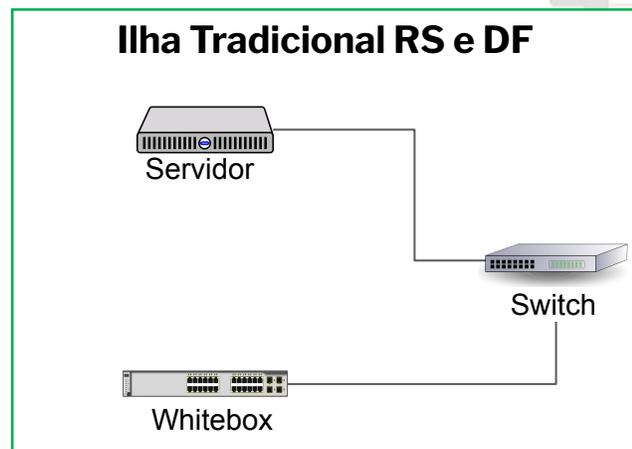
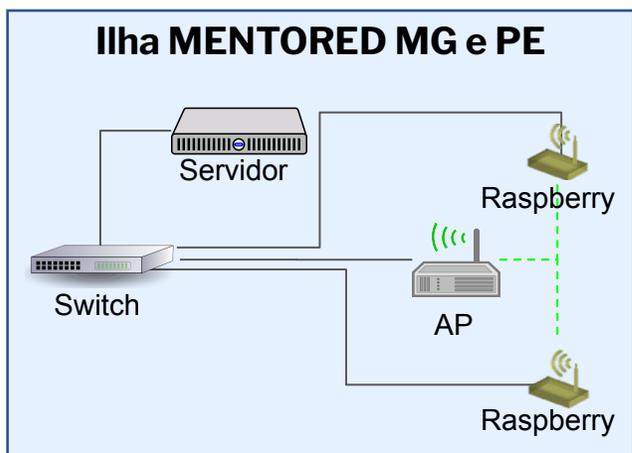


# Estudo de caso - botnets

## Infraestrutura



MENTORED



redelpê



**Perguntas?**  
**[www.mentoredproject.org](http://www.mentoredproject.org)**

Michele Nogueira, D.Sc.  
Pesquisadora Responsável  
[michele@dcc.ufmg.br](mailto:michele@dcc.ufmg.br)

23 de Maio de 2022



**23° WRNP**  
Workshop RNP

