# Proposta de minicurso SBRC 2024

## 1 Dados de identificação

- **Título do minicurso:** *Testbeds* para Pesquisa Experimental em Cibersegurança: Da Teoria à Prática
- **Autores:** Michelle Silva Wangham[‡⋆], Bruno H. Meyer[◇], Davi D. Gemmer[⋆], Khalil G. Q. de Santana[‡], Lucas Rodrigues Frank[∗], Luiz Eduardo Folly de Campos[⋆], Emerson Ribeiro de Mello[†] e Marcos Felipe Schwarz[⋆]

  † Instituto Federal de Santa Catarina – mello@ifsc.edu.br

  ‡ Universidade do Vale do Itajaí – khalil.santana@edu.univali.br

  ⋆ Rede Nacional de Ensino e Pesquisa – <michelle.wangham,davi.gemmer,luiz.campos, marcos.schwarz@rnp.br>

  ◇ Universidade Federal do Paraná – bruno.meyer@ufpr.br

  ∗ Universidade Federal de Juiz de Fora – lucasrodrigues@ice.ufjf.br
- **Apresentador(a) do minicurso**: Profa. Michelle Silva Wangham

## 2 Dados gerais

O relatório de Riscos Globais do *World Economic Forum* 2023 (FORUM, 2023) aponta que os ataques cibernéticos continuam entre os maiores riscos. A evolução constante das ameaças e dos ataques de segurança exige o desenvolvimento e o aprimoramento contínuo de soluções robustas de cibersegurança.

Desenvolver soluções robustas para prevenir, detectar e mitigar ataques de cibersegurança requer ferramentas e métodos para testá-los e validá-los. Para pesquisadores e profissionais da área de cibersegurança, a seleção de plataformas adequadas para validar soluções e testar hipóteses de pesquisa é uma tarefa complexa (CHOULIARAS et al., 2021). Essa busca envolve enfrentar desafios críticos, como a necessidade de encontrar ambientes para experimentação que atendam a requisitos fundamentais, incluindo reprodutibilidade, fidelidade, realismo de tráfego, isolamento, escalabilidade e custo (BENZEL, 2011; CHERNYSHEV et al., 2017; JUNIOR et al., 2021).

Na busca por validar sistemas, protocolos e implementações de segurança, os pesquisadores se deparam com a difícil escolha entre simuladores, emuladores e *testbeds*. Embora simuladores e emuladores forneçam ambientes controlados para experimentos reproduzíveis, muitas vezes carecem de realismo. Já os *testbeds* oferecem realismo e escalabilidade, mas podem ser limitados pelo custo e pela disponibilidade de equipamentos reais (GOMEZ et al., 2023). A impossibilidade de testar soluções em ambientes realistas em larga escala representa uma barreira significativa para empresas, instituições e fornecedores de soluções, resultando em atrasos na implementação de novos recursos e limitando a inovação em cibersegurança.

Este minicurso teórico-prático tem como objetivo apresentar *testbeds* especializados para a condução de experimentos em cibersegurança, com destaque para o MENTORED *Testbed*. Desenvolvido no âmbito do MENTORED Project[1], financiado pela FAPESP[2], esta plataforma será explorada como um estudo de caso. Os participantes obterão uma compreensão aprofundada sobre *testbeds* para cibersegurança, com ênfase na aplicação prática de conceitos teóricos. Serão apresentados dois cenários que os participantes poderão executar na prática os experimentos, bem como analisar os resultados gerados.

Este minicurso destina-se a profissionais, estudantes de graduação e pós-graduação e pesquisadores com conhecimentos básicos em segurança computacional, sistemas distribuídos e familiaridade com o ambiente Linux (comandos no terminal). O minicurso combinará sessões teóricas, demonstrações práticas e atividades interativas, proporcionando aos participantes uma experiência abrangente e *hands-on*.

## 3 Estrutura prevista do texto

1. Introdução
   - 1.1. Desafios para conduzir experimentos em cibersegurança
   - 1.2. Requisitos dos *testbeds* de cibersegurança
2. *Testbeds* para Experimentação
   - 2.1. Cluster Nacional (Kubernetes)
   - 2.2. Deterlab
   - 2.3. FIT IoT LAB
   - 2.4. Gotham Testbed
   - 2.5. Considerações sobre os *testbeds*
3. MENTORED *Testbed*
   - 3.1. MENTORED *framework*
   - 3.2. Recursos tecnológicos do MENTORED *Testbed*
     - 3.2.1. MENTORED Master
     - 3.2.2. Gestão de Projetos e Times
     - 3.2.3. Ciclo de vida do Experimento
4. Estudo de casos - hping e slowloris
   - 4.1. Descrição de experimentos
     - 4.1.1. Hping
     - 4.1.2. Slowloris
   - 4.2. Roteiros
     - 4.2.1. Roteiro para atividade prática I
     - 4.2.2. Roteiro para atividade prática II
5. Considerações finais

[1] https://mentored.dcc.ufmg.br/

[2] https://bv.fapesp.br/pt/auxilios/106148/mentored-da-modelagem-a-experimentacao-predizendo-e-detectando-ataques-ddos-e-zero-day

# 4 Descrição das seções e previsão de páginas

## Introdução (5 páginas)

Nesta seção serão apresentados o contexto, motivação, objetivos e a estrutura do capítulo do minicurso. Também serão apresentados os desafios para condução de experimentos em cibersegurança, bem como os requisitos de *testbeds* que possam ser usados para condução de experimentos em cibersegurança.

**Seção 1.1** Experimentos com cibersegurança, principalmente aqueles voltados para ataques de negação de serviço distribuído (DDoS, *Distributed Denial of Service*), exigem um grande número de dispositivos, com uma grande diversidade de capacidade dos dispositivos, e que precisam estar geograficamente dispersos (BENZEL, 2011; GOMEZ et al., 2023). O volume de dados gerado durante um experimento também são fatores que dificultam a realização desses experimentos em computadores isolados. Nessa seção serão detalhados esses desafios de forma que o leitor entenda como usar *testbeds* para condução de pesquisa experimental em cibersegurança.

**Seção 1.2** Caracterização dos principais requisitos para construção de *testbeds* em cibersegurança, adequados para condução de experimentos com diferentes dispositivos, como os usados na Internet da Coisas (IoT, *Internet of Things*). Serão comentados sobre reprodutibilidade, isolamento, fidelidade, escalabilidade, interface com o usuário para permitir a gestão de equipes e projetos, bem como a definição, execução e análise dos experimentos (PRATES JR et al., 2021; BENZEL, 2011; SIATERLIS; GARCIA; GENGE, 2013).

## *Testbeds* para Experimentação (15 páginas)

Nesta seção serão apresentados *testbeds* para experimentação que se destacam na literatura ou no seu amplo uso em pesquisas acadêmicas, com intuito de apresentar como estes podem ser usados em pesquisas aplicadas de cibersegurança e as diversas abordagens que estes oferecem, como virtualização, emulação, conteinerização, dentre outras.

**Seção 2.1** O Cluster Nacional, anteriormente chamado de Infraestrutura Definida por *Software* (IDS-RNP), é uma infraestrutura de nuvem Kubernetes distribuída nacionalmente e provida pelo serviço de *testbeds* da RNP[3]. Seus servidores estão presentes em 15 localidades, abrangendo todas as cinco regiões do Brasil. Além disso, o *cluster* conta com enlaces de até 10 GB/s, possibilitando a experimentação com grandes volumes de dados trafegados, como ataques DDoS volumétricos (Layer3/Layer4). O Cluster Nacional também conta com mais de 400 núcleos de CPU, 2 TB de memória RAM e 120 TB de armazenamento, possibilitando a execução de diferentes experimentos de forma simultânea. Nesta seção também serão apresentados alguns casos de uso e experimentos em cibersegurança que utilizam o Cluster Nacional.

**Seção 2.2** O *testbed* de cibersegurança Deterlab (WROCLAWSKI et al., 2016) é um dos mais reconhecidos da literatura, contando com recursos avançados de SDN (*Software Defined Networking*) para a construção dos ambientes de experimentação. Esse *testbed* conta com cinco níveis ou tipos de dispositivos, com graus variados de fidelidade e sobrecustos, visando possibilitar a execução de experimentos de larga escala, enquanto mantém a fidelidade dos dispositivos de interesse. Além disso, o *testbed* conta com tecnologias de isolamento (contenção) dos experimentos que possibilita um acesso granular dos dispositivos à Internet. Em 2023, o DeterLab passou por uma modernização de hardware e do software de gerenciamento, estas melhorias, bem como alguns casos de uso, serão apresentados nesta seção.

**Seção 2.3** O FIT IoT-Lab (ADJIH et al., 2015) é um ambiente para experimentação de larga escala, contando com 2.728 dispositivos *wireless* e 117 robôs móveis distribuídos em 6 lugares na França.

[3] https://www.rnp.br/servicos/testbeds

Esse *testbed* visa servir como ferramenta científica para o estudo e avanço de tecnologias sem fio e tópicos adjacentes como mobilidade. A exemplo disso, os autores trazem estudos sobre o impacto de sinais WiFi em uma rede IEEE 802.15.4, assim como um outro caso de estudo sobre a geolocalização de pessoas ou robôs num piso inteligente. Diante da relevância do paradigma IoT na atualidade, este *testbed* possui um grande potencial de auxiliar pesquisas nesta área, apesar de possuir poucos dos artifícios necessários para a execução de experimentos de cibersegurança. Esta seção apresentará alguns casos de uso do FIT IoT-Lab.

**Seção 2.4** Construído sobre o emulador de redes *open-source* GNS3, o *testbed* Gotham (SÁEZ-DE-CÁMARA et al., 2023) é um *middleware* e *scripts* para a geração de cenários e ataques no *testbed*. Esse *testbed* herda todos os recursos do GNS3, sendo capaz de gerar topologias arbitrárias, tal como utilizar uma mistura de virtualização e conteinerização nos dispositivos modelados. Esta alta flexibilidade permite que novos cenários sejam confeccionados, sendo que seu cenário principal possui 100 dispositivos, 30 switches e 10 roteadores. Tais dispositivos são representados como câmeras IP, sensores, *brokers* MQTT, dentre outros. Por fim, três grupos de atacantes são adicionados ao *testbed*, executando *scans* automatizados, tráfego botnet C&C (*Command and Control)*, realizando ataques DDoS e ataques contra protocolos IoT como MQTT e CoAP.

**Seção 2.5** Nesta seção serão descritas algumas limitações de escopo ou funcionalidade dos *testbeds* previamente apresentados, visando comparar e contrastar os mesmos em uma tabela com suas principais características.

## MENTORED *Testbed* (15 páginas)

O MENTORED *Testbed* é uma plataforma para condução de experimentos de cibersegurança com ênfase em dispositivos IoT, em específico para a análise de ataques de segurança e possíveis mecanismos de predição, detecção e mitigação. A arquitetura do MENTORED *Testbed* (GEMMER et al., 2023) tem como principal característica a sua independência dos recursos de processamento utilizados para construir o *testbed* e a diversidade de funcionalidades que facilitam a definição, execução e análise de experimentos. A atual versão do MENTORED *Testbed* possibilita seu uso por meio de um portal *Web*, em que o usuário pode se autenticar pela federação CAFe[4] e tem acesso a diferentes ferramentas para experimentação. Esta seção irá descrever o MENTORED *Testbed*, suas principais características e os recursos tecnológicos relevantes para o seu uso no contexto do minicurso.

**Seção 3.1** O *framework* utilizado pelo MENTORED *Testbed* considera um controlador geral, que é responsável por interligar os cinco principais módulos (GEMMER et al., 2023): 1) Provedor de recursos de IoT; 2) Provedor de recursos de processamento; 3) Canal de comunicação de recursos; 4) Provedor federado de identidades; 5) Orquestrador de e gerenciador de recursos para experimentos (*Master*). Esta seção irá detalhar de forma genérica como utilizar este *framework* para a experimentação em cibersegurança usando dispositivos IoT. Nesta seção serão descritos cada um dos módulos mencionados anteriormente e como eles se relacionam para que a plataforma permita a definição, execução e análise de experimentos em um *Testbed*.

**Seção 3.2** Nesta seção serão apresentados os detalhes técnicos para o entendimento do MENTORED *Testbed*. O MENTORED *Testbed* considera duas principais interfaces: um portal *Web* no qual o usuário pode utilizar uma interface gráfica e uma CLI (*Command Line Interface*) na qual o usuário poderá se conectar via um terminal por linha de comando. O portal se comunica com um módulo chamado MENTORED Master, que é implementado utilizando uma API REST. Esta API é responsável por se comunicar com um módulo de orquestração de experimentos, que gerencia uma sintaxe para definição de experimentos às quais são utilizadas para alocar recursos no *cluster* Kubernetes e simular uma topologia de rede em que o experimento será executado.

[4] https://www.rnp.br/servicos/cafe

Na segunda parte desta seção, a plataforma de experimentação do MENTORED *testbed* será explicada. Essa plataforma utiliza a tecnologia Kubernetes para se comunicar com o Cluster Nacional da RNP. Os recursos de *hardware* disponíveis no Cluster Nacional estão distribuídos dentre diferentes estados do Brasil, e possuem principalmente dois tipos de nós: servidores para grandes cargas de processamento e computadores de baixa capacidade de processamento. Por meio da tecnologia Kubernetes é possível utilizar esses recursos para simular grandes topologias de redes onde ataques DDoS são executados de forma controlada e segura. Além disso, o *testbed* foi proposto para que múltiplos usuários tenham acesso ao portal e possam executar experimentos, uma funcionalidade que será detalhada no roteiro do minicurso. Por fim, o MENTORED *Testbed* também utiliza um sistema de controle de gestão de projetos e times para que os experimentos possam ser organizados e isolados de forma correta considerando critérios de autorização e autenticação, o que será explicado na seção 3.2.2.

**Seção 3.2.1** O MENTORED Master é o principal módulo do MENTORED *Testbed*. Esta seção irá explicar o funcionamento deste módulo, que utiliza um sistema de gerenciamento de projetos e times e um sistema de orquestração de experimentos. Durante o minicurso serão explicadas as etapas necessárias para iniciar um experimento, onde o orquestrador recebe como entrada um arquivo do tipo YAML, com uma sintaxe similar à da tecnologia Kubernetes (amplamente documentada). No arquivo, um experimento é descrito considerando a topologia que deseja ser simulada, o tipo de conexão de rede dos nós da topologia e os softwares executados nos nós. Uma vez que o MENTORED Master recebe a definição de experimento, ele executa uma série de etapas incluindo validação, execução e armazenamento dos resultados do experimento. Todas as informações relacionadas às etapas do experimento podem ser acessadas pelo portal do MENTORED Master. Ao final desta seção, a pessoa que participa do minicurso terá o conhecimento necessário para definir experimentos no MENTORED *testbed*.

**Seção 3.2.2** O MENTORED Master permite o gerenciamento de projetos e times, possibilitando administrar os projetos criados e organizar os usuários e suas responsabilidades em cada projeto. Adicionalmente, essa gestão é realizada em conjunto com o COmanage que é um *framework* eficaz e seguro que permite que colaborações organizacionais, por meio de um conjunto de funcionalidades, atinjam seus objetivos (COMANAGE. . . , s.d.). Pelo acesso de forma federada, o COmanage ficará por conta de gerir a identidade do usuário advinda de sua instituição de origem, além de delegar papéis e lidar com a autorização dos seus membros em um único processo.

**Seção 3.2.3** Esta seção tem como objetivo descrever e exemplificar todas as etapas relacionadas ao ciclo de vida de experimentos no MENTORED *Testbed*. Em resumo, o ciclo de vida de um experimento pode ser dividido em três etapas: 1) Definição do experimento, onde o experimentador define topologias de rede, softwares e outros recursos que podem ser especificadas em uma sintaxe definida pelo MENTORED Master; 2) A execução do experimento, onde um experimentador seleciona uma definição de experimento e o momento em que esse experimento será iniciado; 3) As análises dos experimentos, que incluem armazenamento e processamento de *logs*, alertas e se necessário o monitoramento dos experimentos em tempo real. O roteiro do minicurso irá abranger exemplos de uso práticos do ciclo de vida de experimentos usando o MENTORED Master e o seu portal para realizar todas as etapas do ciclo considerando a perspectiva do experimentador.

### Estudo de casos - hping e slowloris (8 páginas)

Nessa seção serão apresentados dois casos de uso de ataques DDoS no MENTORED *Testbed*, onde serão descritos os dois cenários de ataques, como a topologia utilizada, número de atacantes e clientes utilizados no ataque.

**Seção 4.1.1** Esta seção detalha o cenário de ataques DDoS volumétricos utilizando a ferramenta hping3 (SANFILIPPO, 2006), onde será abordado o funcionamento, configuração e execução do ataque no MENTORED *Testbed*.

**Seção 4.1.2** Esta seção detalha o cenário de ataques DDoS camada 7 do modelo OSI, utilizando a ferramenta Slowloris (YALTIRAKLI, 2015), onde será abordado o funcionamento, configuração e execução do ataque no MENTORED *Testbed*. Na próxima seção será apresentado o roteiro que detalha a execução de ambos os experimentos.

### Roteiros

Nessa seção será apresentado o roteiro para a execução do experimento onde será mostrado o portal do MENTORED *Testbed*, ferramenta utilizada para configurar e inicializar os experimentos.

**Seção 4.2.1** Esta seção detalha o primeiro roteiro da atividade prática onde será elaborado um experimento de ataque DDoS utilizando a ferramenta hping3. Esse experimento será composto por um servidor *Web* que fará o papel de alvo único dos ataques, em conjunto com 30 clientes legítimos adicionados a 30 atacantes, distribuídos igualmente em 3 regiões do Brasil escolhidas previamente. Os resultados desse ataque serão apresentados demostrando sua efetividade.

**Seção 4.2.2** Esta seção detalha o segundo roteiro da atividade prática onde será elaborado um experimento de ataque DDoS utilizando a ferramenta Slowloris. A arquitetura e topologia utilizada neste cenário serão as mesmas utilizadas no cenário anterior. Os resultados desse ataque serão apresentados mostrando sua efetividade.

### Considerações finais (3 páginas)

Será feita uma consolidação dos assuntos apresentados, com uma pequena discussão sobre os *testbeds* apresentados e com uma ênfase maior sobre as possibilidades de uso do MENTORED *Testbed* para além dos estudos de casos apresentados.

## Bibliografia principal


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

BENZEL, Terry. The Science of Cyber Security Experimentation: The DETER Project. In: PROCEEDINGS of the 27th Annual Computer Security Applications Conference. Orlando, Florida, USA: Association for Computing Machinery, 2011. (ACSAC '11), p. 137–148. ISBN 9781450306720. DOI: 10.1145/2076732.2076752. Disponível em: <https://doi.org/10.1145/2076732.2076752>.

CHERNYSHEV, Maxim et al. Internet of things (iot): Research, simulators, and testbeds. *IEEE Internet of Things Journal*, IEEE, v. 5, n. 3, p. 1637–1647, 2017.

CHOULIARAS, Nestoras et al. Cyber Ranges and TestBeds for Education, Training, and Research. *Applied Sciences*, v. 11, n. 4, 2021. ISSN 2076-3417. DOI: 10.3390/app11041809. Disponível em: <https://www.mdpi.com/2076-3417/11/4/1809>.

COMANAGE - About the COmanage Project. https://spaces.at.internet2.edu/display/COmanage/About+the+COmanage+Project. Acessado: 06-01-2024.

FORUM, World Economic. *Global Cybersecurity Outlook 2023*. Jan. 2023. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/.

GEMMER, Davi Daniel et al. A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things. In: PROCEEDINGS of IEEE/IFIP Network Operations and Management Symposium (NOMS). Miami, FL, EUA: IEEE/IFIP, mai. 2023.

GOMEZ, Jose et al. A survey on network simulators, emulators, and testbeds used for research and education. *Computer Networks*, v. 237, p. 110054, 2023. ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2023.110054. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128623004991>.

JUNIOR, Nelson Prates et al. Um Ambiente de Experimentação em Cibersegurança para Internet das Coisas. In: ANAIS do XLI Congresso da Sociedade Brasileira de Computação (CSBC). Porto Alegre, RS: Sociedade Brasileira de Computação, 2021.

MEYER, Bruno H; POZO, Aurora et al. Federated Self-Supervised Learning for Intrusion Detection. In: IEEE. 2023 IEEE Symposium Series on Computational Intelligence (SSCI). 2023a.

_____. Uma proposta para Federated Learning em Cibersegurança. In: SBC. ANAIS da XXIII Escola Regional de Alto Desempenho da Região Sul. 2023b. P. 115–116.

MEYER, Bruno Henrique; GEMMER, Davi Daniel; ANDRADE, Allex Magno et al. Criação de Redes Virtuais no MENTORED Testbed: Uma Análise Experimental. In: 1º Workshop de Testbeds - 42º CSBC. Porto Alegre, RS: Sociedade Brasileira de Computação, ago. 2022.

MEYER, Bruno Henrique; GEMMER, Davi Daniel; SCHWARZ, Marcos et al. MENTORED: The Brazilian Cybersecurity Testbed. In: DEMO sessions of IEEE Global Communications Conference (GLOBECOM). Rio de Janeiro, RJ: IEEE, dez. 2022.

PRATES JR, Nelson G et al. Um ambiente de experimentaçao em cibersegurança para internet das coisas. In: SBC. ANAIS do VI Workshop do testbed FIBRE. 2021. P. 68–79.

SÁEZ-DE-CÁMARA, Xabier et al. Gotham testbed: a reproducible IoT testbed for security experiments and dataset generation. *IEEE Transactions on Dependable and Secure Computing*, IEEE, 2023.

SANFILIPPO, Salvatore. *Hping - Active Network Security Tool*. 2006. https://github.com/antirez/hping.

SIATERLIS, Christos; GARCIA, Andres Perez; GENGE, Bela. On the Use of Emulab Testbeds for Scientifically Rigorous Experiments. *IEEE Communications Surveys & Tutorials*, v. 15, n. 2, p. 929–942, 2013. ISSN 1553-877X. DOI: 10.1109/SURV.2012.0601112.00185. Disponível em: <http://ieeexplore.ieee.org/document/6226792/>. Acesso em: 24 abr. 2023.

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

YALTIRAKLI, Gokberk. *Low bandwidth DoS tool. Slowloris rewrite in Python*. 2015. https://github.com/gkbrk/slowloris.

# 5 Curriculum vitae resumido dos autores

## 5.1 Emerson Ribeiro de Mello

- **CV Lattes:** http://lattes.cnpq.br/1478274711167428
- **Ocupação profissional:** Professor do Instituto Federal de Santa Catarina
- **Formação acadêmica:** Obteve o título de doutor (2009) e de mestre (2003) em Engenharia Elétrica pela Universidade Federal de Santa Catarina e bacharel (2000) em Ciências da Computação pela Universidade do Oeste Paulista.
- **Trabalhos na área do minicurso**

  JUNIOR, Nelson Prates et al. Um Ambiente de Experimentação em Cibersegurança para Internet das Coisas. In: ANAIS do XLI Congresso da Sociedade Brasileira de Computação (CSBC). Porto Alegre, RS: Sociedade Brasileira de Computação, 2021

MEYER, Bruno Henrique; GEMMER, Davi Daniel; ANDRADE, Allex Magno et al. Criação de Redes Virtuais no MENTORED Testbed: Uma Análise Experimental. In: 1º Workshop de Testbeds - 42º CSBC. Porto Alegre, RS: Sociedade Brasileira de Computação, ago. 2022

MEYER, Bruno Henrique; GEMMER, Davi Daniel; SCHWARZ, Marcos et al. MENTORED: The Brazilian Cybersecurity Testbed. In: DEMO sessions of IEEE Global Communications Conference (GLOBECOM). Rio de Janeiro, RJ: IEEE, dez. 2022

GEMMER, Davi Daniel et al. A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things. In: PROCEEDINGS of IEEE/IFIP Network Operations and Management Symposium (NOMS). Miami, FL, EUA: IEEE/IFIP, mai. 2023

### 5.2 Michelle Silva Wangham

- **CV Lattes:** http://lattes.cnpq.br/8951163088992771
- **Ocupação profissional:** Professora na Universidade do Vale do Itajaí e Assessora de Pesquisa, Desenvolvimento e Inovação na RNP.
- **Formação acadêmica:** Obteve os títulos de doutora (2004) e de mestre (2000) em Engenharia Elétrica pela Universidade Federal de Santa Catarina. Engenheira eletricista (2000) pela Universidade Federal do Pará.
- **Trabalhos na área do minicurso**

  JUNIOR, Nelson Prates et al. Um Ambiente de Experimentação em Cibersegurança para Internet das Coisas. In: ANAIS do XLI Congresso da Sociedade Brasileira de Computação (CSBC). Porto Alegre, RS: Sociedade Brasileira de Computação, 2021

  MEYER, Bruno Henrique; GEMMER, Davi Daniel; ANDRADE, Allex Magno et al. Criação de Redes Virtuais no MENTORED Testbed: Uma Análise Experimental. In: 1º Workshop de Testbeds - 42º CSBC. Porto Alegre, RS: Sociedade Brasileira de Computação, ago. 2022

  MEYER, Bruno Henrique; GEMMER, Davi Daniel; SCHWARZ, Marcos et al. MENTORED: The Brazilian Cybersecurity Testbed. In: DEMO sessions of IEEE Global Communications Conference (GLOBECOM). Rio de Janeiro, RJ: IEEE, dez. 2022

  GEMMER, Davi Daniel et al. A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things. In: PROCEEDINGS of IEEE/IFIP Network Operations and Management Symposium (NOMS). Miami, FL, EUA: IEEE/IFIP, mai. 2023

### 5.3 Bruno Henrique Meyer

- **CV Lattes:** http://lattes.cnpq.br/1467037655437965
- **Ocupação profissional:** Aluno de doutorado em ciência da computação na Universidade Federal do Paraná e empresário individual.
- **Formação acadêmica:** Obteve o título de mestrado (2021) e bacharel (2018) em Informática Biomédica pela Universidade Federal do Paraná.
- **Trabalhos na área do minicurso**

  MEYER, Bruno H; POZO, Aurora et al. Federated Self-Supervised Learning for Intrusion Detection. In: IEEE. 2023 IEEE Symposium Series on Computational Intelligence (SSCI). 2023a

  GEMMER, Davi Daniel et al. A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things. In: PROCEEDINGS of IEEE/IFIP Network Operations and Management Symposium (NOMS). Miami, FL, EUA: IEEE/IFIP, mai. 2023

MEYER, Bruno H; POZO, Aurora et al. Uma proposta para Federated Learning em Cibersegurança. In: SBC. ANAIS da XXIII Escola Regional de Alto Desempenho da Região Sul. 2023b. P. 115–116

MEYER, Bruno Henrique; GEMMER, Davi Daniel; SCHWARZ, Marcos et al. MENTORED: The Brazilian Cybersecurity Testbed. In: DEMO sessions of IEEE Global Communications Conference (GLOBECOM). Rio de Janeiro, RJ: IEEE, dez. 2022

MEYER, Bruno Henrique; GEMMER, Davi Daniel; ANDRADE, Allex Magno et al. Criação de Redes Virtuais no MENTORED Testbed: Uma Análise Experimental. In: 1º Workshop de Testbeds - 42º CSBC. Porto Alegre, RS: Sociedade Brasileira de Computação, ago. 2022

### 5.4 Davi Daniel Gemmer

- **CV Lattes:** http://lattes.cnpq.br/9692515610336282
- **Ocupação profissional:** Analista de Operações e Sistemas na RNP.
- **Formação acadêmica:** Obteve o título de mestre (2021) em Ciência da Computação pela Universidade Tecnológica Federal do Paraná e bacharel (2018) em Sistemas de Informação pela Universidade Federal de Santa Maria - FW.
- **Trabalhos na área do minicurso**

  GEMMER, Davi Daniel et al. A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things. In: PROCEEDINGS of IEEE/IFIP Network Operations and Management Symposium (NOMS). Miami, FL, EUA: IEEE/IFIP, mai. 2023

  MEYER, Bruno Henrique; GEMMER, Davi Daniel; SCHWARZ, Marcos et al. MENTORED: The Brazilian Cybersecurity Testbed. In: DEMO sessions of IEEE Global Communications Conference (GLOBECOM). Rio de Janeiro, RJ: IEEE, dez. 2022

  MEYER, Bruno Henrique; GEMMER, Davi Daniel; ANDRADE, Allex Magno et al. Criação de Redes Virtuais no MENTORED Testbed: Uma Análise Experimental. In: 1º Workshop de Testbeds - 42º CSBC. Porto Alegre, RS: Sociedade Brasileira de Computação, ago. 2022

### 5.5 Luiz Eduardo Folly de Campos

- **CV Lattes:** http://lattes.cnpq.br/9591475230072965
- **Ocupação profissional:** Analista de Operações Senior na RNP.
- **Formação acadêmica:** Obteve o título de Mestrado MBA em Segurança Cibernética em 2021 (IGTI), tendo já o Bacharel em Engenharia Elétrica com ênfase em Telecomunicações em 2007 (UNESA)

### 5.6 Khalil Glevinski Queiroz de Santana

- **CV Lattes:** http://lattes.cnpq.br/5564990760504772
- **Ocupação profissional:** Mestrando em Computação Aplicada e pesquisador na área de Kubernetes e *testbeds* pela RNP.
- **Formação acadêmica:** Obteve o título de bacharel (2022) pela Universidade do Vale do Itajaí (UNIVALI), e realizando atualmente o Mestrado em Computação Aplicada na mesma instituição.

## 5.7 Lucas Rodrigues Frank

- **CV Lattes:** http://lattes.cnpq.br/2924098385985246
- **Ocupação profissional:** Aluno de mestrado em ciência da computação pela Universidade Federal de Juiz de Fora.
- **Formação acadêmica:** Obteve o título de bacharel em ciência da computação (2019) pela Universidade Federal de Juiz de Fora, e atualmente, cursa o mestrado em ciência da computação pela mesma universidade.

## 5.8 Marcos Felipe Schwarz

- **CV Lattes:** http://lattes.cnpq.br/8589380354903782
- **Ocupação profissional:** Gerente de P&D na RNP.
- **Formação acadêmica:** Obteve o título de mestre (2014) em Engenharia da Computação pela Universidade de São Paulo e bacharel (2011) em Ciência da Computação pela Universidade do Estado de Santa Catarina, atualmente é candidato a doutorando em Engenharia da Computação na Universidade Estadual de Campinas.
- **Trabalhos na área do minicurso**

  MEYER, Bruno Henrique; GEMMER, Davi Daniel; SCHWARZ, Marcos et al. MENTORED: The Brazilian Cybersecurity Testbed. In: DEMO sessions of IEEE Global Communications Conference (GLOBECOM). Rio de Janeiro, RJ: IEEE, dez. 2022

  GEMMER, Davi Daniel et al. A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things. In: PROCEEDINGS of IEEE/IFIP Network Operations and Management Symposium (NOMS). Miami, FL, EUA: IEEE/IFIP, mai. 2023