**COMUNICADO**

**EDITAL Nº 08/2025 – ITSC2ICCOM**

**CONTRATAÇÃO DE EMPRESA PARA DISPONIBILIZAÇÃO DE RECURSOS HUMANOS ESPECIALIZADOS**

**Fundação de Apoio à Pesquisa Desenvolvimento e Inovação – Exército Brasileiro (FAPEB)**

A FAPEB anuncia que está aberto o processo seletivo para a contratação de empresa para fornecimento de mão de obra qualificada para trabalhar no Projeto "Inovações Tecnológicas para Segurança Cibernética de Sistemas Ciberfísicos Aplicadas a Infraestruturas Críticas e Comunicações Estratégicas e Táticas", nas condições descritas a seguir:

**Local de Trabalho:**
Instituto Militar de Engenharia - IME
Endereço: Praça General Tibúrcio, n° 80, Praia Vermelha, Rio de Janeiro - RJ.

**Benefícios**:
Remuneração bruta mensal máxima a ser paga à empresa contratada: até R$ 12.500,00.

**Condições**:
Função: Engenheiro de Computação.
Descrição geral: Apoio à coordenação e à geração de inovação no projeto.
Disponibilização de carga horária de trabalho: 40 h semanais.
Prazo estimado de contratação: até 24 meses (máximo), contrato inicial de 6 meses renovado a cada 6 meses se for do interesse da contratante.

**Competências Obrigatórias**:
Formação: Bacharel em Engenharia da Computação em curso e instituição de ensino reconhecida pelo MEC.

**Competências Desejadas**:
Formação: Pós-Graduação *Stricto Sensu* em Engenharia Elétrica ou em Sistemas e Computação ou equivalente em curso e instituição de ensino reconhecida pelo MEC/CAPES.

**Atividades a serem executadas**:
As inerentes à função, destacando:

- Assessoria à coordenação e à administração quanto às especificações técnicas de todo o material dos projetos de PD&I;

- Atuação em ligação com a coordenação e a administração do projeto de pesquisa garantindo o fluxo correto de informações de forma a não faltar condições para as atividades de PD&I;
- Manutenção da coordenação e da administração informadas de todos os eventos ocorridos na esfera de sua atribuição;
- Integração Segura entre Sistemas de TI e TO: desenvolver estratégias para a integração segura entre os sistemas de TI/TO, garantindo interoperabilidade e proteção contra ameaças cibernéticas;
- Desenvolvimento de Trabalhos de Natureza Técnica na Área de TI, Visando o Atendimento das Necessidades do Projeto: projetar, implementar e testar soluções técnicas voltadas para o desenvolvimento de ferramentas e sistemas utilizados nos projetos de pesquisa do LaSC. As atividades incluem análise de requisitos, documentação técnica e desenvolvimento de software seguro para aplicações em ambientes de TI e TO;
- Desenvolvimento, Implantação e Realização da Manutenção nos Sistemas de Informação: atividades relacionadas a sistemas de informação voltados à segurança cibernética, promovendo sua integração segura e funcionalidade contínua. A manutenção inclui atualizações periódicas, correções de falhas e melhorias baseadas nas melhores práticas de cibersegurança aplicadas a infraestruturas críticas.
- Identificação e Correção de Falhas nos Sistemas: monitorar e realizar análises preventivas e proativas para identificar vulnerabilidades e aplicar correções em tempo hábil. Este processo inclui o uso de ferramentas de análise de código, auditorias de segurança e simulações cibernéticas;
- Elaboração de Pareceres e Notas Técnicas Relacionadas à Área de Atuação, Bem como de Anotações de Responsabilidades Técnicas, se for o caso: produzir pareceres e relatórios técnicos que documentem avanços, soluções propostas e resultados alcançados nos projetos de pesquisa e desenvolvimento conduzidos pelo LaSC;
- Concepção, desenvolvimento e manutenção de cenários de Cyber Range (TI e TO/ICS): definição de objetivos pedagógicos/técnicos, desenho de topologias, serviços e artefatos, criação de datasets e “injects”, e padronização de templates reutilizáveis;
- Automação de laboratórios com Infraestrutura como Código (IaC): provisionamento e orquestração usando Terraform/Ansible, virtualização (KVM/Proxmox/VMware), containers (Docker/Podman) e, quando aplicável, Kubernetes; versionamento e reprodutibilidade dos ambientes;
- Programação e engenharia de software para o Cyber Range: desenvolvimento de back-ends (preferencialmente em Python e Java), APIs (REST/gRPC), microsserviços, integrações com bancos de dados (PostgreSQL/SQLite) e filas/mensageria; implementação de “scoring engine” e módulos de avaliação;
- Portais e dashboards do exercício: construção de front-ends (React/Next.js ou equivalente), painéis operacionais e relatórios de desempenho, com instrumentação para telemetria e observabilidade;
- Integração de ferramentas de segurança e de rede no range: IDS/IPS, coleta de logs e fluxos (Syslog/NetFlow/PCAP), SIEM, scanners e geradores de tráfego (por ex., Scapy/tcpreplay), além de simuladores/protocolos industriais (p.ex., Modbus, DNP3, OPC UA) quando necessário;
- Testes, qualidade e entrega contínua: criação de pipelines CI/CD, testes automatizados (unitários/integração), empacotamento (Docker) e “hardening” básico de serviços do range; documentação técnica e manuais de operação;
- Orquestração de exercícios cibernéticos: definição de cenários Red/Blue/Purple Team, cronogramas de injects, critérios de avaliação, coleta de evidências e automação de reset/rollback do ambiente;

- Ferramentas de apoio e scripts operacionais: desenvolvimento de scripts para provisionamento, validação, “fuzzing” e coleta de métricas; criação de kits de laboratório e conteúdo para trilhas de capacitação no próprio Cyber Range.

Experiências anteriores e pré-requisitos:

- Conhecimentos inerentes à função e às atividades a serem executadas; e
- Disponibilidade para comparecer presencialmente nas atividades do LaSC quando for requerido.

Qualidades desejadas:

- Curso de extensão ou especialização em Telecomunicações;
- Experiência em projetos nas áreas de segurança da informação e segurança cibernética;
- Conhecimento avançado em programação;
- Experiência sólida em desenvolvimento de software, com proficiência em Python e Java;
- Conhecimento avançado em gerência de projetos e/ou métodos ágeis;
- Conhecimento avançado em segurança cibernética;
- Conhecimento avançado em sistemas operacionais baseados em Linux e/ou Windows;
- Experiência no apoio à coordenação de projeto de pesquisa, desenvolvimento ou inovação;
- Experiência na administração pública;
- Experiência em ambiente militar;
- Habilidades de organização, comunicação clara, facilidade para trabalhar em equipe e saber agir estrategicamente;
- Boa comunicação oral e escrita em português;
- Habilidade em resolução de problemas;
- Habilidade em planejamento e organização;
- Flexibilidade;
- Capacidade de se adaptar a mudanças.

**Processo seletivo**:
Exame curricular e de demais documentos comprobatórios de experiências prévias e qualificações desejadas, e entrevista com perguntas diversas, incluindo algumas técnicas na área de atuação, experiências e de outras áreas abrangidas pelo LaSC como ambientes industriais, segurança cibernética, redes de computadores, virtualização, sistemas operacionais e programação.

Responsável: Prof. Araujo (e-mail: araujo@ime.eb.br)

Demais informações em: Termo de Referência N° 08/2025 – ITSC2ICCOM.

Dúvidas técnicas deverão ser dirigidas à Coordenação do Projeto pelo e-mail: coord.lasc@ime.eb.br.

Enviar dados da empresa (ficha de Cadastro Nacional da Pessoa Jurídica – Receita Federal), currículo do candidato e demais documentos comprobatórios para coord.lasc@ime.eb.br, com cópia para pellanda@ime.eb.br e fapeb@fapeb.com.br.

**PRAZOS**

| | |
|---|---|
| **Período de inscrição** | De 23 de outubro a 24 de novembro de 2025 |
| **Entrevistas** | De 25 a 28 de novembro de 2025 |
| **Publicação do resultado da seleção** | 2 de dezembro de 2025 |
| **Apresentação de recursos** | De 2 a 3 de dezembro de 2025 |
| **Publicação do resultado definitivo da seleção** | 5 de dezembro de 2025 |
| **Entrega da documentação do(a) selecionado(a)** | De 5 a 10 de dezembro de 2025 |
| **Previsão de início de atividades** | A partir de 1º de janeiro de 2026 |