COMUNICADO

EDITAL Nº 03/2025 – 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 Desejadas:
Formação: Bacharel em Engenharia da Computação ou formação superior equivalente em curso e instituição de ensino reconhecida pelo MEC.

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;
- Pesquisa e Implementação de Tecnologias Avançadas de Segurança: explorar e aplicar inovações em cibersegurança, como inteligência artificial e criptografia, para proteger os Sistemas Industriais e de Defesa em geral contra ameaças emergentes;
- Desenvolvimento e Ministração de Treinamentos em Cibersegurança para Sistemas Industriais e de Defesa em geral: elaborar e ministrar treinamentos e workshops focados na cibersegurança de Sistemas Industriais e de Defesa capacitando a equipe em melhores práticas;
- Engajamento com a Missão e Objetivos Estratégicos do LaSC: contribuir para os objetivos estratégicos do LaSC, com foco em garantir que os Sistemas Industriais e de Defesa utilizados no projeto estejam alinhados com os padrões de segurança cibernética;
- Análise de Vulnerabilidades e/ou Testes de Penetração em Sistemas de Tecnologia da Informação (TI) e Tecnologia Operacional (TO): realizar análises de vulnerabilidades e testes de penetração nos sistemas elétricos, integrando as melhores práticas de segurança cibernética para prevenir ameaças;
- Monitoramento e Resposta a Incidentes de Segurança em Sistemas Industriais e de Defesa: implementar processos contínuos de monitoramento de segurança e resposta a incidentes em sistemas industriais, garantindo a proteção de redes e equipamentos elétricos críticos;
- Garantia de Conformidade com Normas de Cibersegurança para Sistemas Industriais e de Defesa: assegurar que os sistemas elétricos estejam em conformidade com normas específicas de cibersegurança, como a IEC 62443, aplicáveis a ambientes industriais, dentre outras normativas relacionadas a outros sistemas industriais;
- 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 de Ferramentas e Soluções de Segurança Cibernética para Sistemas Industriais e de Defesa: projetar e implementar ferramentas de segurança cibernética voltadas para sistemas de TI e TO em ambientes industriais, garantindo a resiliência das infraestruturas críticas;
- 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;
- Planejamento e Administração de Dados e Banco de Dados: gerenciar bancos de dados seguros, garantindo a integridade, disponibilidade e confidencialidade dos dados armazenados. Inclui o planejamento de backups e políticas de recuperação de desastres para manter a continuidade dos serviços essenciais;
- Planejamento, Coordenação e Execução de Tarefas de Projetos de Redes de Comunicação de Dados: coordenar projetos de redes de comunicação de dados para ambientes críticos, promovendo conectividade segura e implementação de redes definidas por software (SDN) e redes militares especializadas;
- 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; e
- Monitoração dos Sistemas como (IPS, IDS, SIEM, Firewalls, SOC, etc.) e Análise do Tráfego para Determinar a Causa e Mitigação de Incidentes Cibernético: manter operações contínuas de segurança, monitorando sistemas de defesa, analisando tráfego de redes e investigando incidentes para mitigar ameaças cibernéticas, promovendo resiliência das infraestruturas críticas.

Experiências anteriores e pré-requisitos:
- Conhecimentos inerentes à função; e
- Disponibilidade para comparecer presencialmente nas atividades do LaSC quando for requerido.

Qualidades desejadas:
- Mestrado e/ou doutorado em sistemas e computação ou áreas afins;
- Curso de extensão ou especialização em segurança cibernética;
- Experiência em projetos nas áreas de segurança da informação e segurança cibernética;
- Conhecimento avançado em programação;
- Conhecimento avançado em redes de computadores;
- 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;
- Certificações nacionais ou internacionais nas áreas de segurança da informação e cibernética;
- Experiência no apoio à coordenação de projeto de pesquisa, desenvolvimento ou inovação;
- Formação acadêmica complementar em nível de graduação em áreas correlatas à administração de negócios (qualquer especialidade);
- 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;
- Conhecimento avançado em Python;
- Conhecimento avançado em gerência de projetos.

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° 03/2025 – 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 01 a 31 de março de 2025
Entrevistas	De 01 a 15 de abril de 2025
Publicação do resultado da seleção	18 de abril de 2025
Apresentação de recursos	De 18 a 23 de abril de 2025
Publicação do resultado definitivo da seleção	25 de abril de 2025
Entrega da documentação do selecionado(a)	De 25 a 30 de abril de 2025
Previsão de início de atividades	A partir de 01 de maio de 2025