



**MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
DIRETORIA DE FABRICAÇÃO**

ANEXO - DFD nº 01/DTI-24

Justificativa da necessidade de prestação do serviço

1. Da estrutura organizacional do Órgão

A Diretoria de Fabricação (DF), Órgão do Departamento de Ciência e Tecnologia do Exército (DCT), tem por finalidade gerenciar as atividades relativas à produção, revitalização, repotencialização, manutenção nível industrial, modernização e nacionalização de Sistemas e Materiais de Emprego Militar (SMEM) em proveito da Força Terrestre (FT) e promover o relacionamento do Sistema de Ciência, Tecnologia e Inovação do Exército com a Base Industrial de Defesa (BID).

Compondo a estrutura organizacional da DF, há a Divisão Técnica Industrial (DTI) que dentro de suas atribuições estão o desenvolvimento de tecnologias, métodos e processos industriais; a gestão de projetos, desde a concepção até a implementação, coordenando equipes multidisciplinares; otimização de processos, identificando oportunidades de melhoria; gerenciamento dos processos de manutenção, revitalização e modernização de SMEM; e, treinamento e desenvolvimento de colaboradores do corpo técnico da DF em habilidades necessárias para desempenhar suas funções de forma eficaz e segura. Na referida divisão, se encontra estruturada a Seção de Sistemas Eletrônicos (SSE), a qual é responsável pela execução das atividades de desenvolvimento e gerenciamento de sistemas, que envolve projetar, desenvolver e manter os sistemas de sistemas utilizados, em sua maioria afeitos aos sistemas de armas e sistemas embarcados em viaturas militares; segurança da informação dos sistemas eletrônicos, implementando medidas de segurança cibernética e de detecção de falhas; integração de sistemas, garantindo adequação para eficácia e eficiência de sistemas embarcados, como sistemas de energia, de controle e comunicação; coletar dados relevantes e preparar relatórios técnicos para avaliar o desempenho e identificar áreas para otimização.

Para realização de tais atividades, a DF faz uso de um quadro de pessoal que seja conhecedor de diversos processos, e busca realizar periodicamente, através de planos de capacitação e treinamentos, relevantes às funções e responsabilidade do corpo técnico, cursos técnicos de desenvolvimento profissional, para garantir a utilização da últimas práticas, tecnologias e conhecimentos relevante para sus funções, em diferentes modalidades como, cursos presenciais, cursos de ensino a distância, workshops, palestras, seminários etc.

2. Das necessidades da atividade técnica

Na seara da SSE/DTI, que demanda peculiaridades técnicas e processos específicos a serem seguidos a fim de atender os requisitos de funcionamento de sistemas embarcados em viaturas e de armas, insere-se a realização de curso de cibersegurança, que tem como objetivo melhorar e ampliar o conhecimento sobre análise e interpretação de dados, detecção de ameaças, gerenciamento de vulnerabilidades, resposta a incidentes e arquitetura de segurança. Essas particularidades exigem pleno conhecimento especializado quanto ao aspecto de avaliação de vulnerabilidades dos sistemas

eletrônicos, entendimento de potenciais ameaças, além de habilidades e conhecimentos necessários para proteger esses sistemas, condições fundamentais para que os militares possam participar ativamente do desenvolvimento dos projetos correntes.

Dentre as atividades e projetos planejados em execução, a DF tem se destacado agregando o conhecimento adquirido em Sistemas Gerenciadores de Plataformas, Sistemas de Viaturas e Sistemas de Armamento, pelo desenvolvendo da iniciativa de um Sistema Integrador, o PROTEUS. Em linhas gerais, o PROTEUS é um *software* integrador de diversos subsistemas, definindo protocolos e regras de comunicação de sistemas eletrônicos que podem ser embarcados em viaturas. Esse desenvolvimento segue as metodologias "*Generic Vehicle Architecture*" (GVA) e "*NATO Generic Vehicle Architecture*" (NGVA), garantindo um trabalho integrado para proporcionar novas capacidades às plataformas.

Desta forma, o curso proposto visa capacitar os participantes a identificar e resolver problemas de segurança digital, especialmente devido ao armazenamento e compartilhamento de informações importantes de forma digital, além da proteção da privacidade. Ao final, deseja-se que o profissional tenha capacidade de avaliar a segurança de sistemas e dispositivos, identificar possíveis violações de segurança e rastrear atividades maliciosas em sistemas de terceiros que são inseridos dentro das plataformas desenvolvidas ou adquiridas pelo Exército.

Com isso, fica **evidenciada vinculação do curso pretendido com as funções e atribuições desempenhadas pelo militar**, caracterizando-se a real necessidade de disponibilizar o acesso ao conhecimento necessário que possa garantir o pleno e seguro desenvolvimento dos seus afazeres, ao que muito contribuirá a participação do militar no curso em tela.

3. Das características do curso

O Curso pretendido tem duração de 40 horas, distribuídas em 05 semanas de duração e mais 01 de encerramento, totalizando 06 semanas. É composto por 02 encontros *online* semanais com o tutor, perfazendo o total de 10 encontros. Os encontros serão ao vivo com a duração de 02 horas cada encontro. Em suma, o curso é presencial *online*, abarcando o vasto conteúdo no período de 10 (dez) encontros de 02 horas, diluídos em 05 semanas, não acarretando considerável prejuízo às atividades de expediente da Organização Militar onde o militar exerce suas atribuições funcionais.

Os conteúdos programáticos abrangidos pelo curso, de forma resumida são: Gestão de Ameaças e Vulnerabilidades, Ameaças em *Frameworks* (*Cyber Kill Chain*), Identificação de Vulnerabilidade Remediação/Mitigação, *Scanners* de Aplicações (Ferramentas e Técnicas de Avaliação de *Software* e Tipos de Ataque Vulnerabilidades), Pontos Fracos do Serviço em Segurança de Software e dos Sistemas Gestão de Ativos, Arquitetura Orientada a Serviço (*Service-Oriented Architecture* - *SOA*), Raiz de Confiança de *Hardware* (*Hardware Root of Trust*), Fundação e Processadores de Confiança (*Trusted Foundry and Processors*), Tecnologia de Confiança (*Trusted Technology*), Operações e Monitoramento de Segurança (Análises e Tendências *Endpoint*), Criptografia e Defesa Ativa, Plataformas de Segurança de *Software*, Processo de Resposta a Incidentes, Coordenação das Respostas Fatores de Criticidade dos Dados, Detecção e Análise Resposta a Incidentes, Atividades Pós-Incidentes (Indicadores de Comprometimento Relacionados ao *host*, à Rede e à Aplicações Exfiltração de Dados), Técnicas Básicas Forense Digital, Cálculo de Risco (Priorização de Riscos), Ameaças e Vulnerabilidades Associadas a Tecnologia Especializada, Rastreamento de Objeto e Contenção de Objeto, Conceitos e Protocolos de Automação, Treinamento e Exercícios Estruturas Políticas e Procedimentos Dados Auditorias e Avaliações etc.

Desta forma, **verifica-se que todas as matérias possuem aplicabilidade na função desempenhada pelo Militar** na Seção de Sistema Eletrônicos. Face à diversidade das matérias oferecidas pelo curso, almeja-se ampliar os conhecimentos do militar, de modo que possa, de forma

segura e alinhada com os ditames legais vigentes, estar em condições de além de desempenhar suas atribuições atinentes à atividade fim, prestar um assessoramento embasado e atualizado no que se refere aos assuntos correlatos ao desenvolvimento e gerenciamento de sistemas.

4. Da qualificação do instituto

Demonstrada a correlação do Curso com as atividades a serem desempenhadas, há de se expor também quanto à **notória qualificação da instituição e dos docentes do curso**, a fim de esclarecer a motivação para a escolha da instituição. A Escola Superior de Redes (ESR) é a unidade de serviço da Rede Nacional de Ensino e Pesquisa (RNP) criada para promover a capacitação, o desenvolvimento profissional e a disseminação de conhecimento em Tecnologias da Informação. Com 17 anos de atuação, mais de 1.100 instituições clientes e aproximadamente 40.000 alunos capacitados, a ESR visa o resultado prático e busca os maiores índices de qualidade em seus serviços, com a excelência no ensino e o bom atendimento ao cliente como premissas. Os docentes possuem anos de experiência em Segurança de Redes de TI, habilidades em reconhecer vulnerabilidades e ameaças de segurança da informação no contexto de gestão de risco, habilidades operacionais com sistemas operacionais, conhecimentos dos conceitos e framework de políticas de segurança da informação de redes e dispositivos, entendimento sobre conceito de redes e dos principais protocolos TCP/IP. O curso em tela é uma parceria entre a ESR e Ascend Education, instituição internacional e reconhecida na área.

A contratada trata-se de Organização Social, vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e ao Ministério da Educação (MEC), pessoa jurídica de direito privado, sem fins lucrativos, assim qualificada pelo Chefe do Poder Executivo, cujas atividades sejam dirigidas ao ensino, à pesquisa científica, ao desenvolvimento tecnológico, à proteção e preservação do meio ambiente, à cultura e à saúde.

Não obstante, salienta-se que, a **singularidade do serviço** se verifica pela adequação do conteúdo programático do curso a um dos ramos necessários para o aprimoramento técnico-profissional pretendido. Pode-se também enfatizar quanto a oportunidade da oferta do curso, que se mostra, neste momento, apta a atender às necessidades dessa Organização Militar, em conformidade com a disponibilidade de vagas, com a disponibilização dos créditos necessários para custear o curso e atendendo ao trâmite administrativo previsto para a concretização da contratação. Podendo-se assim, afirmar que, **neste momento, o curso atende às necessidades da SSE/DTI**.

5. Dos recursos financeiros

Vale destacar que conforme proposta anexa ao processo, fica evidente que o valor praticado para a contratação se encontra compatível com o valor praticado no mercado, junto a outras instituições públicas e privadas, além do público em geral, uma vez que é livre a consulta ao valor do pacote ofertado por meio de acesso ao link público <https://esr.rnp.br/cursos/ciberseguranca-ead-parceria-oficial-ascend-seg34/>. A Orientação Normativa nº 17-AGU, de 2009, na redação que lhe deu a Portaria nº 592, de 2011, do Advogado-Geral da União assim dispõe:

[...] a razoabilidade do valor das contratações decorrentes de inexigibilidade de licitação poderá ser aferida por meio da comparação da proposta apresentada com os preços praticados pela futura contratada junto a outros entes públicos e/ou

Convém apresentar que os recurso para a solicitação encontram-se incluída no **Plano de Descentralização de Recursos do DCT com a DF para o ano de 2024 (PDR DCT-DF 2024)**, quanto ao quesito capacitação do corpo técnico da DF para o ano de 2024.

6. Conclusão

Ao final do curso, o aluno será capaz de utilizar e aplicar inteligência proativa contra ameaças para apoiar a segurança organizacional, realizar atividades de gerenciamento de vulnerabilidade e aplicar soluções de segurança para gerenciamento de infraestrutura. Além disso, será capaz de explicar as melhores práticas de garantia de *software* e *hardware*, analisar dados como parte das atividades de monitoramento de segurança contínuas e implementar alterações de configuração nos controles existentes para melhorar a segurança. Também estará apto a utilizar procedimentos de resposta a incidentes apropriados, analisar indicadores potenciais de comprometimento e aplicar técnicas forenses digitais básicas no desenvolvimento das atividades e dos projetos correntes.

Rio de Janeiro, RJ, ____ de _____ de 2024.

THIAGO MARTINS SARDINHA - Maj
Chefe da Seção de Sistemas Eletrônicos / Divisão Técnica Industrial