



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

ESTUDO TÉCNICO PRELIMINAR

Anexo I ao Termo de Referência

SUMÁRIO

1. INFORMAÇÕES BÁSICAS	2
2. NECESSIDADE DA CONTRATAÇÃO	2
3. ÁREA REQUISITANTE.....	3
4. DESCRIÇÃO DA SOLUÇÃO E SEUS REQUISITOS	4
5. LEVANTAMENTO DE MERCADO.....	5
6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO.....	5
7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS	6
8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO	7
9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO	7
10. CONTRATAÇÃO CORRELATAS E/OU INTERDEPENDENTES.....	8
11. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO	8
12. IDENTIFICAÇÃO DE RISCOS	8
13. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO.....	8
14. PROVIDÊNCIAS A SEREM ADOTADAS	9
15. POSSÍVEIS IMPACTOS AMBIENTAIS	9
16. DECLARAÇÃO DE VIABILIDADE.....	9
16.1. JUSTIFICATIVA DA DECLARAÇÃO DE VIABILIDADE.....	10
17. RESPONSÁVEL	10

1. INFORMAÇÕES BÁSICAS

Processo Administrativo: nº xxx

Serviço a ser contratado: Treinamento na área de engenharia (CATSER 3832).

Curso: Cibersegurança.

Quantidade: 01 vaga.

Valor: R\$ 2.300,00.

2. NECESSIDADE DA CONTRATAÇÃO

O presente estudo tem por finalidade assegurar que processo de contratação pela administração pública seja feita de forma planejada, transparente e eficiente, garantindo que os recursos públicos sejam utilizados da melhor forma possível e que os objetivos da contratação sejam plenamente alcançados, sendo evidenciado no documento o problema a ser resolvido e a sua melhor solução, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação, conforme art. 18, §1º, da Lei nº 14.133, de 2021, e art. 3º, inciso I e art. 6º da Instrução Normativa SEGES/ME nº 58, de 08 de agosto de 2022.

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.

Foi identificada uma necessidade significativa de conhecimento técnico e prático dos militares lotados na SSE. Essa necessidade tem impacto diretamente na qualidade dos projetos, na eficiência

dos processos e na capacidade de inovação tecnológica. Além disso, a constante evolução das tecnologias na área exige uma atualização contínua das competências profissionais.

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. O treinamento visa aprimorar as habilidades técnicas dos militares, proporcionando-lhes conhecimentos atualizados sobre novas tecnologias, metodologias de trabalho, e práticas inovadoras no campo requisitado.

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.

3. ÁREA REQUISITANTE

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.

4. DESCRIÇÃO DA SOLUÇÃO E SEUS REQUISITOS

O curso pretendido tem a distribuição de 05 semanas de duração e mais 01 de encerramento para atividades, 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, outras 20 horas são destinadas para atividades práticas. Em suma, o curso é presencial online, no total de 40 horas, 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.

A execução do objeto seguirá a seguinte dinâmica:

- a) Início da execução do objeto será na data de abertura da turma, a ser fornecida pela empresa, quando do fechamento da turma.

- b) O treinamento terá duração de 06(seis) semanas, dispostos em 02(dois) encontros semanais, totalizando 10(dez) encontros nas 05(cinco) primeiras semanas, sendo a última semana para encerramento do treinamento e entrega de trabalhos, totalizando 40(quarenta) horas.
- c) Os encontros terão 02(duas) horas de duração, sendo realizados ao vivo na modalidade de ensino a distância.
- d) O treinamento terá 20(vinte) horas destinadas para atividades práticas.
- e) Para obtenção de certificado é necessário obter média 6,0 (seis) no questionário de avaliação final, ter realizado 50% das tarefas e ter presença superior a 50%.
- f) Os serviços serão prestados na modalidade de ensino a distância, em ambiente virtual próprio, com aulas sendo ministradas ao vivo.
- g) Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades estabelecidas na proposta comercial, promovendo sua substituição quando necessário.
- h) O material de apoio será disponibilizado em Ambiente Virtual de Aprendizagem (AVA).
- i) O material deve ter o conteúdo do curso, agenda do curso, tarefas, questionários ou simulados, materiais extras e vídeo do encontro online.
- j) Não é exigido garantia contratual dos serviços, estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).
- k) Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

5. LEVANTAMENTO DE MERCADO

Devido a relevância e detalhamento do assunto, este será tratado no Anexo I do Estudo Técnico Preliminar.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

Conforme art. 6º, XXIII, “c”, da Lei nº 14.133, de 2021, e o art. 9º, III, da Instrução Normativa Seges/ME nº 81, de 2022, a solução como um todo deve considerar todo o ciclo de vida do objeto. “Ciclo de Vida” é definido no art. 3º da Lei nº 12.305, de 02 de agosto de 2010, como sendo “série de etapas que envolvem o desenvolvimento do produto, a obtenção de matérias-primas e insumos, o processo produtivo, o consumo e a disposição final”.

Desse modo, a descrição da solução deve considerar não só suas características intrínsecas ao uso em si, mas também eventual sustentabilidade de sua produção, duração de seu consumo (se é menos ou mais durável) até a destinação final.

A preocupação com o ciclo de vida é mais comum para bens, porém, não se afasta, em princípio, analisar eventual cabimento desse aspecto no planejamento do serviço que envolver o emprego de bens, como ocorre em manutenção de veículos ou elevadores, por exemplo.

Para o caso, a contratação não envolve bens diretamente, todavia a aplicação do conhecimento será em futuros sistemas que transformarão em partes integrantes de Sistemas e Materiais de Emprego Militar (SMEM).

Assim, a descrição da solução envolve um conjunto integrado de ações que devem garantir a plena execução do treinamento, abrangendo todos os aspectos técnicos, operacionais e de sustentabilidade, incluindo itens detalhado neste estudo como:

- a) Identificação e contratação de fornecedor com comprovada experiência e capacidade técnica para ministrar o treinamento.
- b) Desenvolvimento de um currículo que aborde as mais recentes inovações e práticas na área de engenharia, alinhado às necessidades da instituição.
- c) Utilização de metodologias de ensino que promovam a interação e a absorção do conhecimento, como aulas práticas, estudos de caso e simulações.
- d) Garantia de instalações e equipamentos necessários para a realização do treinamento, incluindo salas de aula, recursos audiovisuais e materiais didáticos.
- e) Acompanhamento contínuo do impacto do treinamento nos processos da instituição e realização de ajustes e melhorias conforme necessários.

A solução escolhida deve ter carga horária adequada ao trabalho nas disciplinas, material didático adequado, professores capacitados e valores dentro do orçamento planejado para a atividade.

Diante do exposto acima, justifica-se a contratação de serviço técnico especializado em aperfeiçoamento pessoal, nos termos do art. 74, inc. III, alínea “f” da Lei nº 14.133/2021, a ser realizado por meio de inscrição no curso “Cibersegurança – parceria Ascend”, promovido pela Escola Superior de Redes.

7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

A demanda do órgão objetiva que o treinamento melhore o conhecimento do discente sobre análise e interpretação de dados, detecção de ameaças, gerenciamento de vulnerabilidades, resposta a incidentes e arquitetura de segurança.

A informação citada é relevante para o dimensionamento da proposta, assim, a estimativas da quantidade foi realizada pelo setor demandante, levando em consideração as condições ideais de atendimento aos militares envolvidos no projeto e portanto ao interesse público, respeitado o planejamento orçamentário.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

O valor da contratação é R\$ 2.300,00 (dois mil e trezentos reais). No valor estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, seguro e outros necessários ao cumprimento integral do objeto da contratação.

A estimativa preliminar dos custos envolvidos na contratação do treinamento revela-se compatível com o orçamento destinado para capacitação dos servidores. Os valores incluem honorários dos instrutores, materiais didáticos, infraestrutura necessária e outras despesas logísticas. A análise de custo-benefício demonstra que o investimento no treinamento trará retornos significativos em termos de aumento de produtividade e qualidade dos serviços prestados.

9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

O parcelamento da solução é a regra devendo a licitação ser realizada por item, sempre que o objeto for divisível, desde que se verifique não haver prejuízo para o conjunto da solução ou perda de economia de escala, visando propiciar a ampla participação de licitantes, que embora não disponham de capacidade para execução da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas.

A análise da possibilidade de parcelamento da contratação foi realizada considerando aspectos técnicos, operacionais e econômicos.

Decidiu-se pela não realização do parcelamento do treinamento em engenharia pelos seguintes motivos:

a) Coesão e Continuidade Didática: Parcelar o treinamento poderia comprometer a continuidade e a coesão dos conteúdos programáticos, dificultando a absorção do conhecimento pelos servidores.

b) Otimização de Recursos: A contratação de um único fornecedor para a realização integral do treinamento otimiza os recursos financeiros e logísticos, evitando a fragmentação dos custos e possíveis discontinuidades.

c) Qualidade do Ensino: A manutenção de um único cronograma e equipe de instrutores assegura a uniformidade na qualidade do ensino, permitindo uma abordagem pedagógica mais estruturada e eficiente.

d) Monitoramento e Avaliação: A gestão de um treinamento não parcelado facilita o acompanhamento do desempenho dos servidores e a avaliação dos resultados alcançados, proporcionando uma visão mais clara e integrada dos benefícios gerados pela capacitação.

10. CONTRATAÇÃO CORRELATAS E/OU INTERDEPENDENTES

Não foi verificado a necessidade de serem feitas quaisquer outras contratações correlatas e/ou independentes para que se atenda à solução proposta.

11. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO

A capacitação de pessoal é item previsto no controle interno da Administração, no Plano de Descentralização de Recursos 2024.

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 privados, ou outros meios igualmente idôneos. (Portaria nº 592-AGU, 2011)

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.**

12. IDENTIFICAÇÃO DE RISCOS

Os riscos associados à contratação do treinamento foram avaliados e considera-se que são mínimos e mitigáveis. Foram propostas medidas de mitigação como a elaboração de um cronograma detalhado, a definição clara dos objetivos e resultados esperados, e o acompanhamento contínuo do desempenho dos militares durante e após o treinamento.

13. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

A contratação servirá para suprir as necessidades imediatas de atividades essenciais da Organização Militar, especialmente aquelas ligadas diretamente a pesquisa e extensão, melhorando o conhecimento sobre análise e interpretação de dados, detecção de ameaças, gerenciamento de vulnerabilidades, resposta a incidentes e arquitetura de segurança.

Espera-se que, 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,

apresentando uma significativa melhoria em suas competências técnicas, ficando aptos a aplicar novas metodologias e tecnologias nos projetos desenvolvidos pela instituição, e contribuam para a inovação e excelência dos serviços de engenharia.

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.

14. PROVIDÊNCIAS A SEREM ADOTADAS

Para viabilizar a contratação do treinamento, deverão ser adotadas as seguintes providências:

a) Detalhar os requisitos técnicos e específicos do treinamento, incluindo conteúdo programático, carga horária, perfil dos instrutores e critérios de avaliação, em apoio ao Termo de Referência e ao próprio presente Estudo Técnico Preliminar.

b) Realizar uma pesquisa de mercado para identificar fornecedores qualificados, solicitar propostas e selecionar a melhor oferta com base em critérios técnicos e econômicos, em apoio ao Termo de Referência e ao próprio presente Estudo Técnico Preliminar.

c) Definir um cronograma detalhado para a realização do treinamento, prevendo todas as etapas desde a preparação até a conclusão e avaliação final, incluindo as atividades correntes de forma que sejam realocadas para não interferir na execução do curso.

d) Publicação em Boletim Interno dos militares que irão realizar o treinamento.

e) Monitorar a execução do treinamento, avaliando a satisfação dos participantes e o cumprimento dos objetivos estabelecidos.

f) Realizar uma análise pós-treinamento para verificar os impactos e benefícios alcançados.

15. POSSÍVEIS IMPACTOS AMBIENTAIS

A implementação do treinamento de engenharia também pode trazer impactos positivos ao meio ambiente. Com a capacitação dos servidores, espera-se que os projetos de engenharia passem a incorporar de forma mais efetiva as melhores práticas de sustentabilidade e gestão ambiental.

Isso inclui o uso de tecnologias limpas, a adoção de metodologias de construção sustentável, a melhoria na gestão de resíduos e a redução do consumo de recursos naturais.

Além disso, os militares estarão mais preparados para avaliar e mitigar impactos ambientais negativos em suas atividades profissionais, contribuindo para a preservação ambiental e o desenvolvimento sustentável.

16. DECLARAÇÃO DE VIABILIDADE

Esta equipe de planejamento declara viável a contratação do treinamento na área de engenharia.

16.1. JUSTIFICATIVA DA DECLARAÇÃO DE VIABILIDADE

A capacitação de militares na área técnica é pilar para um bom desempenho e desenvolvimento dos projetos de engenharia inerentes à Divisão Técnica da Diretoria de Fabricação, principalmente na área requisitada, por ser um ambiente de constante transformação e inovações.

Recomendando-se a execução do projeto conforme os termos descritos neste Estudo Técnico Preliminar, pelo procedimento de inexigibilidade de licitação, com fundamento na hipótese do art. 74, inc. III, alínea “f” da Lei n.º 14.133, de 2021, em razão da notória especialização dos instrutores e a robustez do conteúdo programático estabelecido, da comprovada experiência e capacidade técnica do instituto de treinamento que possui comprovada experiência e reconhecimento na área, do material utilizado como referência pertencente à instituto internacional de referência na área, pela distribuição de carga horária , e pelos valores compatíveis com o orçamento planejado.

Diante do exposto acima, justifica-se a contratação de serviço técnico especializado em aperfeiçoamento pessoal, nos termos do art. 74, inc. III, alínea “f” da Lei nº 14.133/2021, a ser realizado por meio de inscrição no curso “Cibersegurança – parceria Ascend”, promovido pela Escola Superior de Redes.

A implementação do treinamento é uma medida estratégica para assegurar o desenvolvimento técnico profissional contínuo dos militares.

17. RESPONSÁVEL

Rio de Janeiro, XXX de XXX de 2024.

THIAGO MARTINS SARDINHA – TC
Ch SSE

LEVANTAMENTO DE MERCADO E PESQUISA DE PREÇO

Por se tratar de contratação de serviço, a solução demandada foi avaliada conforme IN SEGES/ME Nº 65/2021, a fim de identificar as entidades e os valores praticados no mercado que atendem às necessidades do solicitante, como base para o parecer do presente estudos, e por consequência, ao Termo de Referência.

O primeiro ponto considerado é a existência de diversas alternativas para suprir a necessidade de capacitação, como a realização de treinamentos internos, a contratação de consultorias especializadas, e a utilização de plataformas de ensino a distância. Sopesando a área da demanda, que está em constante atualização, a primeira avaliação é que os benefícios e riscos de cada opção, indicam que a contratação de um curso especializado externo é a alternativa mais vantajosa, considerando a expertise dos instrutores e a qualidade dos conteúdos programáticos oferecidos.

Em seguida, para compor o procedimento administrativo, o início da pesquisa na contratação do serviço considerou prestadores de serviço disponíveis no mercado que trabalham na área. Para tanto, são identificados os seguintes temas afeitos à área de cibersegurança:

- a. Criptografia;
- b. Segurança de Redes;
- c. Segurança da Informação;
- d. Segurança de Aplicações;
- e. Segurança em Nuvem;
- f. Privacidade de Dados;
- g. Engenharia Social;
- h. Segurança de Infraestruturas Críticas;
- i. Resposta a Incidentes e Forense Digital;
- j. Governança, Risco e Conformidade (GRC);
- k. Cibercrime e Legislação;
- l. Inteligência de Ameaças (Threat Intelligence);

Percebe-se neste momento que o mero nome “cibersegurança” tem desdobramentos em diversas áreas, o que ocasiona que existam prestadores de serviços distintos na área de conhecimento que se relacionam, algumas vezes com assuntos comuns.

Na tabela seguinte são identificados os assuntos principais dentro da área de prestação de serviço, no aspecto da cibersegurança.

Tabela 01: Levantamento de áreas

Área de prestação de serviço relacionada	Assuntos principais
Criptografia	- Técnicas de criptografia simétrica e assimétrica; - Assinaturas digitais; e - Certificados digitais e Infraestrutura de Chaves Públicas (PKI).
Segurança de Redes	- Firewalls e sistemas de detecção de intrusão (IDS); - Redes privadas virtuais (VPNs); e - Segmentação de rede e controle de acesso.
Segurança da Informação	- Políticas de segurança; - Gestão de riscos; e - Continuidade de negócios e recuperação de desastres.
Segurança de Aplicações	- Desenvolvimento seguro de software (Secure Software Development Lifecycle - SSDLC); - Testes de penetração e análise de vulnerabilidades; e - Segurança em APIs e aplicativos móveis.
Segurança em Nuvem	- Modelos de serviço de nuvem (IaaS, PaaS, SaaS); - Governança e conformidade em ambientes de nuvem; e - Ferramentas e técnicas de segurança específicas para nuvem.
Privacidade de Dados	- Regulamentações de privacidade (GDPR, LGPD, CCPA); - Gestão de consentimento e direitos dos titulares de dados; e - Técnicas de anonimização e pseudonimização de dados.
Engenharia Social	- Phishing, spear phishing e outras formas de engenharia social; - Treinamento e conscientização de funcionários; e

	- Técnicas de mitigação.
Segurança de Infraestruturas Críticas	- Proteção de sistemas de controle industrial (ICS/SCADA); - Segurança em setores como energia, água, transportes e saúde; e - Resiliência de infraestruturas críticas.
Resposta a Incidentes e Forense Digital	- Planejamento e gestão de resposta a incidentes; - Investigação forense de ataques cibernéticos; e - Coleta e preservação de evidências digitais.
Governança, Risco e Conformidade (GRC)	- Estruturas e frameworks de governança (COBIT, ITIL); - Auditoria de segurança e conformidade regulatória; e - Gestão integrada de riscos.
Cibercrime e Legislação;	- Tipos de cibercrimes e técnicas usadas por cibercriminosos; - Legislação e regulamentação sobre crimes cibernéticos; e - Cooperação internacional em cibersegurança.
Inteligência de Ameaças (Threat Intelligence);	- Coleta e análise de dados sobre ameaças cibernéticas; - Compartilhamento de informações de inteligência; e - Plataformas e ferramentas de inteligência de ameaças.

Este segundo levantamento revela um cenário complexo para a comparação. Cibersegurança é um campo vasto e interdisciplinar que abrange diversos tópicos.

Ainda da Tabela 01, por exemplo, é possível verificar a área de cibersegurança pode ser voltada para questões legais como governança, acesso às informações públicas e crimes; administrativas como infraestruturas críticas; e mais especializadas como tratamento de dados e aplicações. Isto posto, fica demonstrado que a comparação carece de mais critérios, não sendo possível se limitar a critérios exclusivamente objetivos como uma conta da razão entre a carga-horária e o preço.

Iniciada uma terceira fase de levantamento, já focando em prestadores de serviço e valores, é possível elencar algumas instituições. Da consulta realizada as mais relevantes encontradas estão na tabela 02.

Tabela 02: Instituições com possibilidade de atendimento.

Item	Descrição
01	• Instituição: Fundação Getúlio Vargas; • Nome do curso: Ameaças Cibernéticas: Identificação e Táticas de Prevenção; • Carga horária: 30 horas (02 meses); • Indicação: Profissionais que atuam em funções de nível estratégico; • Valor: R\$ 1.077,55; e • Fonte: https://educacao-executiva.fgv.br/cursos/online/curta-media-duracao-online/ameacas-ciberneticas-identificacao-e-taticas-de-prevencao-1?oferta=109798
02	• Instituição: Escola Britânica de artes criativas e tecnologia; • Nome do curso: Cyber Security; • Carga horária: 23 horas (05 meses); • Indicação: Iniciantes em segurança cibernética; • Valor: R\$ 5.900,00; e • Fonte: https://ebaonline.com.br/cyber-security
03	• Instituição: Pontifícia Universidade Católica do Paraná ; • Nome do curso: Arquitetura de Software, Ciência de Dados e Cybersecurity; • Carga horária: 360 horas (02 anos); • Indicação: profissionais com curso superior nas áreas coligadas à Tecnologia da Informação, Sistemas de Informação, Engenharia e Ciência da Computação, ou que possuam notório saber em TIC; • Valor: R\$ 16.092,00 e • Fonte: https://posdigital.pucpr.br/cursos/ciencia-de-dados-arquitetura-de-software-e-cybersecurity?utm_medium=cpc&utm_source=Google&utm_campaign=PUCPR_PRF_CONV_SEARCH_POS-GRAD_Always-On_BR_ARQUITETURA-SOFT&utm_group=C_666_CONV_SEARCH_POS-GRAD_Always-On_SEGURANCA-CIBERNETICA&utm_term=treinamento%20seguran%C3%A7a%20cibern%C3%A9tica

	tica&gad_source=1&gclid=CjwKCAjwgdayBhBQEIwAXhMxtnKRx3pzz6tAzDzsS3FgRByYvPwZC8IAaRAotCnkfF7jYXgYB77zZxoC2RQQA vD BwE
04	• Instituição: Fundação Instituto de Administração; • Nome do curso: Cibersegurança e Proteção Digital de Negócios; • Carga horária: 360 horas (02 anos); • Indicação: Gestores de TIC; • Valor: R\$ 10.776,06; e • Fonte: https://www.fiaonline.com.br/pos/ciberseguranca-e-protecao-digital-de-negocios
05	• Instituição: Unopar; • Nome do curso: CYBERSECURITY E CYBERCRIMES; • Carga horária: 360 horas (6 meses); • Indicação: Profissionais com curso superior nas áreas coligadas à Tecnologia da Informação, Sistemas de Informação, Engenharia e Ciência da Computação, ou que possuam notório saber em TIC; • Valor: 2.178,00; e • Fonte: https://www.portalpos.com.br/mba-em-cybersecurity-e-cybercrimes-unopar-ead-6-meses/p?_gl=1*_1yzwioe*_gcl_au*MTQ4MTk4ODM3Mi4xNzE2OTEyMDMx*_ga*MTU0ODk2MzYwNy4xNzE2OTEyMDMz*_ga_2Z28X0P5MF*MTcxNjkxMjAzMy4xLjEuMTcxNjkxMjA3My4yMC4wLjIwMTg0NjQwNDI.&_ga=2.55259885.711520564.1716912033-1548963607.1716912033
06	• Instituição: Escola Superior de Redes; • Nome do curso: Cibersegurança EaD (parceria oficial Ascend); • Carga horária: 40 horas (06 semanas); • Indicação: Profissionais com experiência em Segurança de Redes de TI; • Valor: R\$ 2.300; e • Fonte: https://esr.rnp.br/cursos/ciberseguranca-ead-parceria-oficial-ascend-seg34

A conjuntura mostra uma diversidade ampla de possibilidades de treinamento. Há de se lembrar que a contratação do treinamento tem um objetivo específico, que é a capacitação de pessoal no desenvolvimento de sistemas na área de engenharia, **no rol de atividades atinentes à Diretoria de Fabricação**, mais especificadamente, no desenvolvimento do Sistema PROTEUS, o que implica que, mesmo sob a ótica de engenharia, mesmo no que tange o desenvolvimento de sistemas, há de se perceber as nuances de conteúdos distintos e o foco para públicos diferentes.

O preço no Processo Administrativo deve ser aferido com cautela, razoabilidade e proporcionalidade. Não é possível comparar, de forma totalmente objetiva objetos singulares em relação aos quais não existe possibilidade de estabelecer critérios completamente objetivos para tal comparação.

O curso de capacitação deve ter carga horária adequada ao conteúdo, mas sem prejudicar o andamento de outras atividades, conta com aulas online e ao vivo, uma vez que não há possibilidade de dedicação exclusiva dos militares na atividade no momento.

O material didático entregue pelo instituto deve ter reconhecimento e ser atualizado, dada a área que está em constante transformação.

Assim, a formação de preços não deve se pautar exclusivamente em eventuais serviços com descrição que se assemelhe ao tema, haja vista que o objeto é singular, e não pode ser comparado de forma totalmente objetiva, em todos os aspectos com outros. Fica prejudicada a comparação exclusiva de uma razão entre o valor e a carga-horária, por exemplo, de um curso de pós-graduação com um outro de pequena duração.

O levantamento demonstra a razoabilidade pela escolha da Escola Superior de Redes, por:

- a. Oferecer um treinamento que pode ser incluído nas atividades correntes, sem prejudicar demasiadamente o andamento de outras atividades, visto que não há necessidade de cessão exclusiva do militar;
- b. Publicidade dos valores praticados para outros entes, onde a empresa escolhida demonstra que os preços ofertados para a Administração contratante que guardam a exata consonância com o que é praticado no mercado, isto é, ofertados para outros órgãos e/ou outras entidades, inclusive pessoas físicas interessadas na capacitação; e
- c. Conteúdo didático bem direcionado à demanda, inclusive adotado em órgãos de reconhecimento internacional.