MAER-GAPBR-GRUPAMENTO DE APOIO DE BRASILIA/DF

Estudo Técnico Preliminar 113/2025

1. Informações Básicas

Número do processo: 010/CCABR/2025

2. Descrição da necessidade

2.1 Contratação dos cursos Novo Pentest Profissional, Pentest Experience + Certificação Desec Certified Penetration Tester (DCPT) e Evasão de Defesas, com o objetivo de capacitar os militares do Centro de Defesa Cibernética da Aeronáutica (CDCAER) em testes de invasão, diagnóstico de vulnerabilidades e implementação de controles na área cibernética, visando ao aprimoramento dos processos de identificação e tratamento de incidentes de rede.

3. Área requisitante

Área Requisitante	Responsável
Divisão Técnica	Jeanderson Medeiros da Silva - 1T QOENG CMP

4. Descrição dos Requisitos da Contratação

Requisitos Gerais

4.1. Disponibilizar todos os materiais do núcleo do curso em língua portuguesa (Português Brasil).

4.2. Garantir aos militares inscritos o acesso às aulas pré-gravadas, por meio da INTERNET, 07 (sete) dias por semana, 24 (vinte e quatro) horas por dia, durante 2 anos, incluindo o laboratório que terá acesso a VPN por 180 dias no período do curso.

4.3.O acesso ao laboratório será fornecido a VPN por 180 dias que será dividido por 3 períodos de 30 dias e 1 de 90 dias, o qual o militar poderá escolher quando usufruir os períodos no intervalo de 2 (dois) anos.

4.4. Será necessário a realização da prova, para certificação DCPT, no período de 2 anos.

4.6. Disponibilizar suporte completo e tutores durante todo o período de acesso ao curso.

Requisitos de Capacitação

4.7. O curso de Pentest Profissional deve capacitar seus participantes na área de testes de penetração, na identificação e na mitigação de falhas de segurança em sistemas e redes computacionais, esclarecendo a natureza do trabalho que um Pentest realiza.

4.8. Prover uma visão geral sobre o cenário do trabalho de tratamento de incidentes, incluindo os serviços prestados pelo Centro de Tratamentos incidentes em Redes (CTIR) às ameaças dos invasores e a natureza das atividades de resposta a incidentes.

4.9. O curso de Pentest Experience deverá abordar técnicas de exploração de falhas de segurança, incluindo o militar participante para operar em espaço virtualizado, simulando um ambiente real de exploração de vulnerabilidades,

aplicando técnicas de ataques comumente utilizados por invasores de sistemas, e aplicando técnicas de defesas que bloqueiem as ameaças presentes no ambiente cibernético.

4.10. O curso de Pentest Experience deverá promover e disponibilizar exercícios interativos, para que os alunos identifiquem e analisem eventos, propondo estratégias de respostas apropriadas.

4.11. O curso de Evasão de Defesas deverá capacitar os participantes em técnicas avançadas de comando e controle (C2), botnets e canal covert, com ênfase na implementação de servidores e agentes C2 em ambientes controlados, simulando cenários reais de ataque.

Requisitos legais

4.12. A CONTRATADA deverá seguir as exigências determinadas pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

Requisitos de Manutenção

4.13. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei n 14.133, de 2021, a instrução Normativa SEGES/ME N 65, de 7 de julho de 2021, Lei n 13.709 de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e a outras legislações aplicadas.

Requisitos Sustentabilidade

4.14. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.15. A CONTRATADA, quando cabível, deve priorizar a utilização de tecnologias não nocivas ao meio ambiente, com uso e aplicação de materiais e equipamentos recicláveis ou reutilizáveis, seguindo o Guia de Contratações sustentáveis, disponível na página da Advocacia -Geral da União (AGU).

4.16. A contratação observará o princípio do desenvolvimento nacional sustentável, conforme previsto na Lei nº 14.133 /2021, adotando práticas que reduzam impactos ambientais e promovam o uso eficiente dos recursos públicos.

Para tanto, deverão ser observados, sempre que aplicável:

I – priorização de materiais didáticos em formato digital, reduzindo o consumo de papel e insumos físicos;

II – utilização de plataformas virtuais de ensino, sempre que possível, minimizando deslocamentos e emissão de poluentes;

III – uso de infraestrutura tecnológica com eficiência energética adequada;

IV – incentivo à realização de atividades remotas ou híbridas, quando compatível com o objeto;

V – observância das diretrizes do Guia Nacional de Contratações Sustentáveis da Advocacia-Geral da União (AGU).

Requisitos de Obtenção de Certificado

4.17. A empresa contratada deverá emitir certificados de conclusão dos cursos para os militares que concluírem as respectivas formações com aproveitamento satisfatório, conforme os critérios estabelecidos.

4.18. Além do certificado de conclusão, será emitido o certificado oficial de Certificação DCPT para os militares que obtiverem aprovação na avaliação específica para a certificação, conforme os requisitos e critérios da Certificação DCPT.

Da Natureza dos Serviços e da Duração

4.19. Os serviços objeto da contratação têm natureza comum e não continuada, com acesso à plataforma na modalidade EaD. A duração do acesso será de 2 (dois) anos, conforme as condições estabelecidas para cada curso.

5. Levantamento de Mercado

5.1. Prospecção e Análise de Soluções:

A prospecção de mercado foi realizada com o objetivo de identificar empresas especializadas em treinamentos de alta performance na área de Segurança Ofensiva, com foco específico em Testes de Penetração (Pentest). A

pesquisa incluiu a análise de portais de compras públicas e a busca por fornecedores em ferramentas de pesquisa para identificar as principais referências no mercado nacional.

Durante o levantamento, constatou-se a existência de diversas empresas que oferecem cursos de segurança da informação. No entanto, a maioria possui um escopo generalista ou introdutório. A necessidade do Centro de Defesa Cibernética da Aeronáutica (CDCAER) é por uma capacitação de natureza eminentemente prática, aprofundada e que simule cenários reais de ataque, um nicho altamente especializado do mercado.

Nesse cenário, a empresa DESEC SECURITY SEGURANÇA DA INFORMAÇÃO LTDA destacou-se por seu posicionamento singular, conforme detalhado a seguir.

5.2. Justificativa da Escolha da Solução:

A análise de mercado demonstrou que a DESEC SECURITY é a solução que melhor atende, com excelência, aos requisitos técnicos e estratégicos do CDCAER, pelos seguintes motivos:

Notória Especialização e Certificação Exclusiva: A empresa é a criadora e única fornecedora da Desec Certified Penetration Tester (DCPT), a primeira e mais reconhecida certificação de Pentest da América Latina. A DCPT é focada na validação de habilidades práticas, exigindo que o profissional demonstre sua capacidade de identificar e explorar vulnerabilidades em um ambiente controlado, o que se alinha perfeitamente com as competências desejadas para os militares do Centro.

Alinhamento Técnico do Conteúdo: O escopo curricular dos treinamentos oferecidos pela DESEC é estritamente focado em segurança ofensiva e testes de penetração. O conteúdo programático detalhado, que abrange desde a coleta de informações até a pós-exploração, atende plenamente às necessidades de capacitação avançada do CDCAER, sem se dispersar em tópicos genéricos de segurança.

Metodologia de Ensino e Modalidade: A DESEC oferece os cursos na modalidade de Ensino a Distância (EaD), requisito que confere a flexibilidade necessária à rotina militar, permitindo que os alunos avancem conforme sua disponibilidade. Além disso, a metodologia é baseada em laboratórios práticos (hands-on), onde os alunos executam testes em ambientes controlados, o que é crucial para a fixação do conhecimento e o desenvolvimento de habilidades aplicáveis.

Reputação e Histórico Comprovado: A empresa possui um histórico consolidado no mercado, com altas taxas de aproveitamento e satisfação de seus alunos. É reconhecida por aplicar as melhores e mais atuais práticas do mercado de segurança ofensiva, garantindo que o conhecimento transmitido esteja alinhado com as técnicas e ferramentas mais recentes utilizadas no setor.

5.3. Conclusão do Levantamento de Mercado:

Em face do exposto, restou demonstrado que a empresa DESEC SECURITY SEGURANÇA DA INFORMAÇÃO LTDA possui uma solução singular no mercado, sendo a única a oferecer a combinação de um treinamento prático e aprofundado com uma certificação própria de notório reconhecimento na América Latina (DCPT).

6. Descrição da solução como um todo

6.1. **O curso Novo Pentest Profissional** proporciona uma base sólida e abrangente para que o profissional adquira conhecimento detalhado sobre TCP/IP, protocolos de rede, e criação de scripts em ambientes Linux (Bash) e Windows (PowerShell). O curso também aborda o funcionamento da web e oferece uma introdução robusta à programação em C e Python. Após essa fase inicial, os participantes avançam para o aprendizado das principais técnicas de ataque, com foco na exploração de sistemas. Essa etapa inclui o mapeamento da superfície de ataque externa, execução de testes de invasão em diferentes cenários – como Pentest Externo Black Box e Pentest Web –, bem como a análise de vulnerabilidades, exploração de softwares, desenvolvimento de exploits e aplicação de técnicas de engenharia social. Ao final do curso, o participante estará apto a desenvolver uma mentalidade voltada ao hacking ético, fundamentada em práticas e conhecimentos atualizados sobre segurança cibernética.

6.1.1 Tempo de acesso ao curso:02 (dois) anos;

6.1.2 Carga horária: 200 horas;

6.1.3 Modalidade: EAD – ONLINE (GRAVADO)

6.1.4 Total de Servidores a serem treinados: 27 militares.

6.1.5 Local de realização: forma remota, através da plataforma da empresa.

Ementa Novo Pentest Profissional:

- Introdução a Segurança da Informação
- Introdução ao Penetration Testing
- Carreira em Pentest
- Virtualização e Sistemas Operacionais
- Dominando o terminal do Linux
- Dominando o prompt do Windows
- Visão geral sobre WEB e HTTP
- Análise de Logs
- TCP/IP para Pentesters
- Analisadores de Protocolos
- Bash Scripting (Linux)
- Power Shell para Pentesters
- Linguagem C para Pentesters
- Python para Pentesters
- Python3 para Pentesters - react
- Swiss Army Knife
- Information Gathering - Business
- Information Gathering - INFRA
- Information Gathering - WEB
- Scanning
- Burlando Mecanismos de Defesa
- Trabalhando com Scapy
- Enumeração (Enumeration)
- Análise de Vulnerabilidades
- Metasploit Framework
- Hashes e Senhas - Linux
- Hashes e Senhas - Windows
- Pentest Interno: Do zero a Domain Admin
- Brute Force: Ataques em senhas
- Dev Exploitation: Assembly para Pentesters - Windows

- Dev Exploitation: Assembly para Pentesters - Linux

- Buffer Overflow para Pentesters: Windows 10

- Desenvolvimento de Exploits: Windows 10

- Mecanismos de proteção: DEP e ASLR

- Buffer Overflow - Linux

- Trabalhando com Exploits Públicos

- Pentest Web: Web Hacking

- Pós Exploração

- Engenharia Social

- O Profissional: Conduzindo o Pentest

6.2. **O Pentest Experience** é uma plataforma de estudos práticos que proporciona uma experiência realista de testes de penetração, permitindo que os participantes apliquem seus conhecimentos em ambientes simulados. O curso inclui dez projetos de Pentest Black Box, todos baseados em casos reais, garantindo máxima similaridade com desafios encontrados no mundo real. Cada projeto foi desenvolvido para explorar diferentes aspectos de um teste de invasão, possibilitando ao participante identificar e analisar vulnerabilidades variadas em diversos tipos de ambientes. Essa abordagem prática amplia a capacidade do profissional de realizar testes de segurança eficazes, adaptando-se a diferentes cenários e desafios encontrados na área de segurança cibernética.

6.2.1 Tempo de acesso ao curso:02 (dois) anos;

6.2.2 Carga horária: 200 horas;

6.2.3 Modalidade: EAD – ONLINE (GRAVADO)

6.2.4 Total de Servidores a serem treinados: 27 militares.

6.2.5 Local de realização: forma remota, através da plataforma da empresa.

Ementa Pentest Experience:

- Projeto: Orion Corp;

- Projeto: Decstore;

- Projeto: NewGen Solutions;

- Projeto: SecurePharma IT;

- Projeto: GrandBusiness;

- Projeto: Saturno Industrial;

- Projeto: Trixel Distribuidora;

- Projeto: Green Host;

- Projeto: GhostSolutions;

- Projeto: ZetraPark.

6.3. **O exame de Certificação Desec Certified Penetration Tester (DCPT):** Ao final dos projetos o participante estará apto a realizar o exame certificatório para a DCPT que conta com duas etapas de 24h seguidas. A primeira parte é a prática, a segunda etapa de 24h é direcionada para a produção de um relatório profissional sobre cada

passo da exploração durante o exame, o qual será validado e passado por validação da equipe de Pentesters da Desec Security.

6.3.1 Tempo de acesso ao curso:02 (dois) anos;

6.3.2 Modalidade: EAD – ONLINE (GRAVADO)

6.3.3 Total de Servidores a serem treinados: 27 militares.

6.3.4 Local de realização: forma remota, através da plataforma da empresa.

Militares participantes dos cursos DESEC PRO (Novo Pentest Profissional, Pentest Experience + Certificação DCPT):

- 1T VICTOR MACIEL;
- 1T MARCELO DE SOUZA PEREIRA JÚNIOR
- 2T ALESSANDRO FLORÊNCIO DIAS JÚNIOR;
- 2S ABNER;
- 2S PEDRO FLORENCIO DE OLIVEIRA NETO;
- 2S KLEITON SILVA LIMA;
- 2S MARCO MAURÍCIO RAMOS NOGUEIRA;
- 2S BRUNO BELFORT MELO DE AZEVEDO;
- 3S QSS PAULO VICTOR SANTOS DE LIMA;
- 3S QSS KÉSIA DA SILVA PEREIRA;
- 3S QSS WESLEY DE MEDEIROS FAGUNDES;
- 3S QSS LUCAS BARBOSA DA SILVA;
- 3S JAAZIEL SOARES DA SILVA;
- 3S EVELYN MENDES DE ALMEIDA;
- 3S SERGIO HEITOR SANTOS COSTA;
- 3S GABRIEL OLIVEIRA AREDO RODRIGUES DOS SANTOS;
- 3S ELIAS FORTUNATO DE JESUS PAULO;
- 3S MATHEUS CONSTERMANI ZITO;
- 3S BEATRIZ BRAINER GONÇALVES;
- 3S JÚLIA MONTEIRO DA SILVA VALENTIM;
- 3S LUIZ GUSTAVO MARCON DE MAGALHÃES;
- 3S VICTOR NOGUEIRA MACHADO XAVIER;
- 3S LUCAS SAMUEL SILVA DE ALMEIDA;
- 3S BIANCA FERNANDES CAVALCANTE;
- 3S KELVIN AUGUSTO MOREIRA CAMPOS;
- 3S ANDRÉ DE AZEVEDO LAMÔNICA;
- 3S JOÃO GUILHERME DE SOUZA PASCO;

6.4. **O curso Evasão de Defesas da Desec Security** é voltado para profissionais de segurança ofensiva, como pentesters e bug hunters, que desejam aprofundar seus conhecimentos em técnicas avançadas para contornar sistemas de defesa cibernética. O treinamento enfatiza a construção de ferramentas de Command and Control (C2) utilizando a linguagem Go, permitindo que os participantes desenvolvam soluções eficazes para a defesa cibernética.

6.4.1 Tempo de acesso ao curso: 02 (dois) anos;

6.4.2 Carga horária: 15 horas;

6.4.3 Modalidade: EAD – ONLINE (GRAVADO)

6.4.4 Total de Servidores a serem treinados: 02 militares.

6..5 Local de realização: forma remota, através da plataforma da empresa.

Ementa do Curso de Evasão de Defesas Security:

- C2 - Comando e Controle;

- Construindo um C2;

- C2 Intermediário: Refatoração;

- C2 Avançado: Novas Features; e

- C2 Avançado: Persistência.

Militares participantes do curso Evasão de Defesas.

- 2S Allan Victor De Araujo Ferreira
- 1T Angélica Lopes de Jesus

7. Estimativa das Quantidades a serem Contratadas

7.1. O volume de serviços necessários para atender à necessidade são os descritos a seguir:

Id.	Descrição do Bem ou Serviço	CATSER	Quantidade	Métrica
1	Novo Pentest Profissional (Curso completo)	3840	27	UN
2	Pentest Experience + DCPT	3840	27	UN
3	Evasão de Defesas	3840	2	UN

7.2. O quantitativo de vagas foi estimado em função do efetivo dos setores que necessitam deste treinamento para exercerem suas funções e não possuem essa capacitação.

JUSTIFICATIVA

7.3. A contratação dos cursos DESEC PRO (Novo Pentest Profissional e Pentest Experience + Certificação DCPT) e Evasão de Defesas é essencial para fortalecer a capacitação técnica dos militares da DT, CTIR e STA do CDCAER.

7.4. Durante o ano de 2024, a avaliação anual evidenciou a escassez de vagas para os novos integrantes do CTIR e das ETIRs, impactando diretamente a formação dos profissionais responsáveis pela segurança cibernética da instituição.

7.5. Com a chegada de novos militares em 2024 e 2025 e o aumento da complexidade das operações, a necessidade de especialização se torna ainda mais crítica. A evolução constante das ameaças cibernéticas exige que os integrantes do CDCAER estejam atualizados com as técnicas mais avançadas de pentest, evasão de defesas e resposta a incidentes, garantindo maior eficiência, proatividade e resiliência nas ações de defesa no Comando da Aeronáutica (COMAER).

7.6. Dessa forma, a contratação desses treinamentos objetiva suprir a carência identificada no último ciclo e também assegura que as equipes estejam plenamente preparadas para enfrentar os desafios emergentes no cenário cibernético, elevando o nível de proteção e resposta do COMAER.

8. Estimativa do Valor da Contratação

Valor (R$): 123.119,00

R$ 123.119,00 (cento e vinte e três mil, cento e dezenove reais)

9. Justificativa para o Parcelamento ou não da Solução

9.1. Considerando a natureza dos serviços a serem prestados, entende-se que não é viável o parcelamento da solução, por se tratar da contratação de uma empresa de notória especialização para o fornecimento do curso almejado. Para embasar essa decisão, foram considerados a viabilidade técnica e econômica, as eventuais perdas de escala e o aproveitamento do mercado.

10. Contratações Correlatas e/ou Interdependentes

10.1 Não há contratações correlatas e/ou interdependentes.

11. Alinhamento entre a Contratação e o Planejamento

11.2 A presente iniciativa está alinhada ao Plano Diretor de Tecnologia da Informação da Aeronáutica (PCA 11-320 – PDTIC 25-28), atendendo às diretrizes estratégicas por meio de projetos e ações de capacitação promovidos pelo CDCAER, conforme detalhado a seguir.

ALINHAMENTO AO PDTIC (25-28) – Anexo VII				
PORTFÓLIO	PROGRAMA	EMPREENDIMENTO	COD.	ATIVIDADE
SEGURANÇA D A INFORMAÇÃO	SEGURANÇA CIBERNÉTICA	CAPACITAÇÃO	A2502125021	CAPACITAR MILITARES P A R A DESEMPENHO D A S ATIVIDADES EM CIBERNÉTICA.

ALINHAMENTO AO PTA-CDCAER (2025)		
CÓDIGO	PERÍODO	TAREFA
25SCO008	2025	Capacitar os militares do CDCAER para as atividades técnicas do CDCAER.

11.1 Conforme estabelecido no Art. 2º da Portaria GABAER/GC3 Nº 1.465, de 27 de junho de 2024, que institui o Centro de Defesa Cibernética da Aeronáutica (CDCAER), este órgão tem a responsabilidade de gerenciar, executar e controlar as atividades relacionadas à Defesa Cibernética no âmbito do COMAER.

12. Benefícios a serem alcançados com a contratação

12.1 Capacitação dos militares do CDCAER em testes de invasão, diagnóstico de vulnerabilidades e implementação de controles de segurança cibernética.

12.2 Aprimoramento da capacidade de identificação, análise e resposta a incidentes cibernéticos.

12.3 Melhoria na avaliação e fortalecimento da segurança dos sistemas do COMAER.

12.4 Adoção de medidas preventivas e corretivas para mitigar ameaças emergentes.

12.5 Aumento da eficiência operacional na execução das atividades de Defesa Cibernética.

12.6 O cumprimento das medidas previstas no PDTIC do COMAER.

13. Providências a serem Adotadas

13.1 Não há providências a serem adotadas pela administração previamente.

14. Possíveis Impactos Ambientais

14.1 Em conformidade com Art.11, Inciso IV, da Lei 14.133/2020 a CONTRATADA deve seguir as normas ambientais vigentes através do Guia Nacional de Contratações Sustentável, 7ª edição de outubro de 2024, bem como as normas porventura criadas /alteradas durante o período de vigência do contrato, bem como o eventual ônus e adaptações a normas ambientais futuras.

15. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

15.1. Justificativa da Viabilidade

15.2.1 A partir dos presentes estudos preliminares e em atendimento ao art.6°, inciso XX, da Lei 14.133/2020 a Equipe de Planejamento declara a contratação pretendida viável, devendo prosseguir com a tramitação prevista.

16. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

RAYLA FARIAS DE LUCENA

INTEGRANTE REQUISITANTE - 1T QOENG CMP

JEANDERSON MEDEIROS DA SILVA

INTEGRANTE TÉCNICO - 1T QOENG CMP

CARLA LUIZA MADERS

INTEGRANTE ADMINISTRATIVO / 1T QOCON ADM

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO

Documento:	ETP DIGITAL
Data/Hora de Criação:	27/02/2026 14:28:42
Páginas do Documento:	10
Páginas Totais (Doc. + Ass.)	11
Hash MD5:	c4485f3bc9b44af8270fd9cab4fa2c16
Verificação de Autenticidade:	https://autenticidade-documento.sti.fab.mil.br/assinatura

Este documento foi assinado e conferido eletronicamente com fundamento no artigo 6º, do Decreto nº 8.539 de 08/10/2015 da Presidência da República pelos assinantes abaixo:

Assinado via ASSINATURA CADASTRAL por 1º Ten JEANDERSON MEDEIROS DA SILVA no dia 03/03/2026 às 13:44:43 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por 1º Ten CARLA LUIZA MADERS no dia 03/03/2026 às 14:47:03 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por 1º Ten RAYLA FARIAS DE LUCENA no dia 03/03/2026 às 16:01:34 no horário oficial de Brasília.