

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

## 1. OBJETO

Este Termo de Referência tem por objetivo contextualizar a contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

## 2. JUSTIFICATIVA

As medidas de segurança da informação implementadas na PPSA, abrangendo desde soluções locais até defesas em nível de rede, constituem um sistema de proteção contra ameaças digitais. No entanto, a eficácia dessas medidas não pode ser assumida como constante sem uma avaliação periódica. A tecnologia evolui rapidamente, assim como as táticas dos atacantes, tornando essencial a realização regular de testes e revisões de segurança. Esta necessidade de validação sistemática visa assegurar que as barreiras de segurança permaneçam resilientes e eficazes frente às novas vulnerabilidades e métodos de ataque que surgem continuamente.

A prática de avaliações periódicas não apenas ajuda a detectar falhas antes que sejam exploradas por agentes mal-intencionados, mas também reforça a confiança na proteção dos dados. Implementar um processo de avaliação de segurança proporciona uma visão do desempenho das políticas e tecnologias de segurança em vigor, permitindo ajustes proativos e aprimoramento contínuo. Esse processo é essencial para manter a integridade, a disponibilidade e a confidencialidade das informações corporativas, fundamentais para a continuidade dos negócios da PPSA. A produtividade de qualquer organização pode ser seriamente prejudicada caso ocorram invasões ou vazamento de dados sensíveis.

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

### 3. DADOS REFERENCIAIS

3.1. A PPSA é uma empresa pública federal, vinculada ao Ministério das Minas e Energia (MME), com Sede, em Brasília-DF e Escritório Central na Av. Rio Branco, nº1 quarto andar, no centro da cidade do Rio de Janeiro-RJ.

3.2. Quantidade de servidores físicos: 4

3.3. Quantidade de servidores virtuais: 50

3.4. Aproximadamente 120 dispositivos na rede

3.5. Quantidade de Switches na rede: 11

3.6. Quantidades de IP domínio: 64 e 8 respectivamente

### 4. ESPECIFICAÇÃO DO OBJETO

#### 4.1. CONSIDERAÇÕES GERAIS

Através deste Termo de referência, a PPSA tem por objetivo a contratação de uma consultoria especializada em segurança da informação para realizar testes de penetração (PENTEST) e analisar vulnerabilidades sistemáticas na área de tecnologia da informação, conforme as melhores práticas de mercado e gerar relatórios detalhados nos níveis tático e estratégico. A CONTRATADA também deverá fazer apresentação dos resultados à GTI e à área de negócios da PPSA.

A Solicitação dos serviços mencionados nesse Termo de referência ocorrerá a critério único e exclusivo da PPSA, não se comprometendo em realizar a quantidade máxima destes serviços. Ao longo da execução deste Contrato a PPSA se compromete a garantir a realização da quantidade mínima que será de 1 (uma) solicitação por linha constante da tabela de formulação de preço.

Para a realização dos serviços de PENTEST e análises de vulnerabilidades a CONTRATADA deverá utilizar normativos (frameworks/orientações técnicas)

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

amplamente conhecidos no mercado para garantir a confiabilidade do resultado esperado. A CONTRATADA poderá utilizar-se de metodologia própria desde que demonstre que é complementar ou similar as listadas abaixo e aprovada previamente pela PPSA:

- PTES (Penetration Testing Execution Standard)
- NIST SP 800-53
- OWASP Guide Test (Open Web Application Security Project)
- OSSTMM (Open Source Security Testing Methodology Manual)
- ISSAF/PTF (Information Systems Security Assessment Framework)
- MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)

Entende-se como Teste de Intrusão ou Teste de Penetração (**PENTEST**) um conjunto de diretrizes e metodologias que visam identificar e explorar vulnerabilidades em sistemas de informação, redes e aplicativos.

O objetivo do PENTEST é simular ataques reais para avaliar a segurança da infraestrutura de TI, permitindo a detecção de falhas que possam ser exploradas por invasores. Esse processo envolve várias etapas, incluindo coleta de informações, modelagem de ameaças, análise de vulnerabilidades, exploração e **geração de relatórios com recomendações para mitigação dos riscos identificados.**

Para o objeto deste Contrato, a CONTRATADA irá utilizar-se de duas técnicas para os testes de penetração, o teste de **Black Box** e o teste de **Grey Box**:

- **Teste de Black Box**

Para o teste de Black Box será considerado que é o teste que utiliza técnicas de avaliação de segurança onde o testador não possui qualquer conhecimento prévio sobre a infraestrutura, aplicações ou sistemas-alvo.

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

Esta abordagem simula um ataque externo real, onde o invasor não tem acesso privilegiado ou informações internas. O objetivo principal é identificar vulnerabilidades exploráveis a partir da perspectiva de um atacante que não possui informações internas da organização.

- **Teste de Grey Box**

Para o teste de Grey Box será considerado que é o teste que utiliza técnicas onde o testador possui algum nível de conhecimento sobre a infraestrutura, aplicações ou sistemas-alvo, como credenciais de usuário ou uma visão geral da arquitetura de TI. Esta abordagem simula um cenário onde o invasor tem acesso limitado ou conhecimento parcial, semelhante ao que pode ser obtido através de phishing ou outras técnicas de engenharia social. As informações a serem fornecidas serão definidas durante as reuniões iniciais de cada solicitação.

**Teste de vulnerabilidade** será considerado que é o processo sistemático de avaliação da segurança dos sistemas de TI por meio da identificação, quantificação e priorização de vulnerabilidades. Este tipo de teste pode utilizar métodos automatizados para varrer o ambiente contra uma base de dados de vulnerabilidades conhecidas, criando um **inventário detalhado** das possíveis fraquezas que precisam ser corrigidas.

Para além dos relatórios produzidos durante as fases de testes de penetração e vulnerabilidade a CONTRATADA deverá realizar uma apresentação em linguagem de negócio de até 1 hora para os stakeholders da PPSA e uma apresentação de cunho técnico de no mínimo de 1 hora e até 3 horas para a GTI da PPSA.

Os serviços a serem realizados deverão ocorrer durante o horário acordado na reunião inicial de cada teste solicitado, durante o expediente de segunda-feira a

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

sexta-feira das 08:00 às 18:00. Excepcionalmente, para os testes que requererem procedimentos que para sua conclusão seja necessária a interrupção do serviço, serão definidos horários diferentes daqueles.

#### 4.2. TESTE DE PENETRAÇÃO (INTRUSÃO)

- 4.2.1. Para realização dos testes de penetração a CONTRATADA deverá considerar que serão realizados testes de black box (externo) e grey box (interno);
- 4.2.2. O teste black box será realizado externamente, ou seja, a CONTRATADA fará fora do ambiente da PPSA;
- 4.2.3. O teste grey box realizado internamente será aquele em que a CONTRATADA receberá acesso básico de um colaborador que trabalha no escritório da PPSA e tem acesso a rede interna e deverá ser feito como descrito no item 8 (Local De Prestação Dos Serviços);
- 4.2.4. A CONTRATADA juntamente com a equipe técnica da PPSA definirá quais informações serão fornecidas para realização dos testes Grey durante a reunião inicial da solicitação de cada teste ao longo da execução do Contrato;
- 4.2.5. Os PENTESTS (testes de penetração) visarão influenciar e comprometer a confiabilidade dos dados e processos dos sistemas que forem definidos durante a reunião inicial da solicitação do teste;
- 4.2.6. Os testes do tipo black box serão iniciados sem a CONTRATADA possuir nenhuma informação da PPSA além dos endereços fornecidos na reunião inicial e qualquer informação obtida deverá ser de domínio público;
- 4.2.7. Os recursos que serão utilizados para a realização dos testes deverão ser providos pela CONTRATADA (Hardware e Software). Nos testes grey box a CONTRATADA poderá utilizar os recursos de TI fornecidos pela PPSA;
- 4.2.8. Os testes não poderão comprometer a continuidade dos serviços em questão, qualquer atividade que seja interrompida sem autorização da

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

PPSA será de responsabilidade da CONTRATADA, que deverá restabelecer o serviço imediatamente;

4.2.9. A CONTRATADA tem por objetivo nos testes comprometer a confiabilidade e autenticidade dos dados e dos sistemas sem a consumação do fato em si, mas documentá-lo de forma extensiva com objetivo de que seja possível através desta documentação, a PPSA tomar ações corretivas em momento oportuno futuro;

4.2.10. A extração de informações durante a realização dos testes deverá ser realizada e demonstrada nos relatórios quais dados a CONTRATADA foi capaz de obter para si;

4.2.11. A CONTRATADA deverá demonstrar, caso obtenha sucesso nos testes realizados, que obteve acesso a algum sistema que foi fornecido na reunião inicial. Estes acessos deverão ser documentados e, havendo a possibilidade, ser demonstrados no relatório;

4.2.12. Além dos testes de alteração e extração, a CONTRATADA deverá, nos testes de Black Box e Grey Box, verificar a possibilidade de instalar ferramentas maliciosas que, de forma oculta, continuem extraindo informações de maneira contínua;

4.2.13. A CONTRATADA deverá também realizar a tentativa de sequestro dos dados da PPSA com encriptação, caso obtenha sucesso a CONTRATADA deverá documentar a tentativa sem executar a ação de fato, gerando provas suficientes para comprovar o êxito do teste.;

4.2.14. Nos testes de intrusão, a CONTRATADA não poderá utilizar, unicamente, ferramentas automáticas, devendo incluir técnicas não oferecidas por tais ferramentas e incluir procedimentos personalizados para garantir que agentes especializados também sejam cobertos durante os testes;

4.2.15. A indicação de profissionais para realização dos testes é responsabilidade da CONTRATADA, a PPSA não irá fornecer profissionais para realização dos testes;

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

- 4.2.16. Deverá procurar serviços privilegiados que estejam desprotegidos e portas ou protocolos que possam ser comprometidos;
- 4.2.17. Para os testes de DoS e DDOS a PPSA irá definir quais os horários poderão ser utilizados para a execução deles;
- 4.2.18. Deverão se consideradas tentativas de adulteração do DNS;
- 4.2.19. Testes de exploração de dispositivos de segurança tais como firewalls, roteadores, IPS, filtros e proxies e autenticadores;
- 4.2.20. Os testes deverão explorar o Site da PPSA;
- 4.2.21. A CONTRATADA deverá entender que se encontram listadas todas as ações necessárias para realização dos testes de black e grey box, não de forma extensiva, cabendo à CONTRATADA utilizar-se das técnicas mais atualizadas possíveis e dentro das metodologias listadas neste Termo de Referência.
- 4.2.22. Caso a PPSA identifique que a CONTRATADA não estabeleceu condições mínimas na realização dos testes seguindo os padrões esperados, poderá ser caracterizado o entendimento de inexecução parcial do Contrato, sujeito as sanções estabelecidas neste termo de referência;
- 4.2.23. Dos relatórios dos testes espera-se:
- 4.2.23.1. Descrição das descobertas, impactos, recomendações e uma contextualização generalizada de alto nível em linguagem não-técnica como introdução;
  - 4.2.23.2. Descrição das ferramentas e metodologias utilizadas;
  - 4.2.23.3. Por ordem de criticidade, do mais crítico para o menos crítico;
  - 4.2.23.4. IP do recurso de TI, se possível;
  - 4.2.23.5. Descrição do ativo, se possível;
  - 4.2.23.6. Nível de criticidade (informação, baixa, média, alta e crítica);
  - 4.2.23.7. Origem da ação realizada internamente/externamente;
  - 4.2.23.8. Data da execução da atividade;
  - 4.2.23.9. Mapeamento de redes, sistemas e equipamentos;

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

4.2.23.10. Evidências;

4.2.23.11. Procedimentos de correção ou paliativas;

4.2.23.12. Análise de impacto (categorização);

4.2.23.13. Os relatórios deverão ser entregues ao responsável designado pela PPSA para fiscalização do Contrato.

#### 4.3. TESTE DE VULNERABILIDADE

4.3.1. Para os testes de vulnerabilidade a CONTRATADA deverá utilizar ferramentas que façam descobrimento e mapeamento de acessos, sistemas e topologias que possam conter vulnerabilidades no ambiente da PPSA sem que seja de fato realizada uma ação que possa alterar, degradar ou interromper os serviços;

4.3.2. Para a realização dos testes de vulnerabilidade, a PPSA irá prover todas as informações e acessos necessários, incluindo estação de trabalho com ponto de rede e elétrica;

4.3.3. As ferramentas (hardware e software) para realização da varredura serão de inteira responsabilidade da CONTRATADA;

4.3.4. A equipe técnica da GTI(Gerência de Tecnologia da Informação da PPSA) realizará o acompanhamento dos testes de vulnerabilidades que deverão ser realizados no escritório da PPSA;

4.3.5. O teste deverá ser capaz de gerar relatório de inventários de servidores, aplicações, ativos da rede e realizar uma categorização dos artefatos encontrados;

4.3.6. Os testes de vulnerabilidade devem incluir a análise de configurações incorretas, patches de segurança ausentes, versões desatualizadas de software e outros pontos fracos conhecidos;

4.3.7. Dos relatórios dos testes de vulnerabilidade espera-se no mínimo:



**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

- 4.3.7.1. Descrição das descobertas, impactos, recomendações e uma contextualização generalizada de alto nível em linguagem não-técnica como introdução;
- 4.3.7.2. Descrição das ferramentas e metodologias utilizadas;
- 4.3.7.3. Por ordem de criticidade, do mais crítico para o menos crítico;
- 4.3.7.4. IP do recurso de TI, se possível;
- 4.3.7.5. Descrição do ativo, se possível;
- 4.3.7.6. Nível de criticidade (informação, baixa, média, alta, crítica);
- 4.3.7.7. Origem da ação realizada internamente/externamente;
- 4.3.7.8. Data da execução da atividade;
- 4.3.7.9. Mapeamento de redes, sistemas e equipamentos;
- 4.3.7.10. Evidências;
- 4.3.7.11. Procedimentos de correção ou paliativas;
- 4.3.7.12. Análise de impacto (categorização);
- 4.3.7.13. Os relatórios deverão ser entregues ao responsável designado pela PPSA para fiscalização do Contrato.
- 4.3.7.14. A CONTRATADA deverá entender que se encontram listadas todas as ações necessárias para realização dos testes vulnerabilidade, não de forma extensiva, cabendo a CONTRATADA utilizar-se das técnicas mais atualizadas possíveis e dentro das metodologias listadas neste termo de referência;
- 4.3.7.15. Caso a PPSA identifique que a CONTRATADA não estabeleceu condições mínimas na realização dos testes seguindo os padrões esperados poderá ensejar por parte da PPSA o entendimento de inexecução parcial do Contrato, sujeito as sanções estabelecidas neste termo de referência.

#### 4.4. APRESENTAÇÃO DOS RESULTADOS

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

- 4.4.1. Os relatórios que a CONTRATADA produzir referente aos testes de intrusão e vulnerabilidade deverão ser utilizados como base para construção de apresentação no formato mais adequado, preferencialmente em Power Point;
- 4.4.2. A apresentação deve conter linguagem de negócio com duração de até 1 hora para os stakeholders da PPSA e uma apresentação de cunho técnico de no mínimo de 1 hora e até 3 horas para a GTI da PPSA;
- 4.4.3. Apresentação deverá conter descritivo dos serviços realizados pela CONTRATADA na PPSA, demonstrando cada etapa que foi realizada;
- 4.4.4. Resultado dos testes, incluindo vulnerabilidades encontradas, classificadas por gravidade (informação, baixa, média, alta, crítica), e o impacto potencial de cada uma;
- 4.4.5. Deverá conter capturas de tela, logs e outros dados visuais que suportem as descobertas relatadas, facilitando a compreensão das vulnerabilidades;
- 4.4.6. Um plano de ação para implementar as medidas de mitigação recomendadas, com prazos sugeridos e responsáveis designados;
- 4.4.7. Apresentação poderá ser realizada de forma remota;
- 4.4.8. A apresentação deverá permitir um espaço de 1 hora para sanar dúvidas após as apresentações para os Stakeholders e para a equipe técnica da PPSA.

## 5. CRONOGRAMA

- 5.1. Abaixo, apresenta-se o cronograma estabelecido relativo à prestação dos serviços contratados:

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

Evento	Item	Descrição	Prazo	Responsável	Recorrência
A	-	Assinatura do contrato (execução e vigência)	Execução: 24 meses Vigência: 26 meses	PPSA/CONTRATADA	Não
B	-	Reunião Inicial	10 dias após início da vigência contrato (A)	CONTRATADA	Não
C	Teste de Penetração	Solicitação para realização do PENTEST (Grey ou Black box)	A critério da CONTRATANTE	PPSA	1 até 3
D	Teste de Penetração	Reunião de kickoff	Até 10 dias corridos após o evento C	CONTRATADA	1 até 3
E	Teste de Penetração	Execução do PENTEST (Grey ou Black box)	Até 30 dias corridos após o evento D	CONTRATADA	1 até 3
F	Teste de Penetração	Entrega do relatório do PENTEST (Grey ou Black box)	ATÉ 5 dias corridos após o evento E	CONTRATADA	1 até 3
G	Teste de Penetração	Aceite do Relatório do PENTEST (Grey ou Black box)	ATÉ 5 dias corridos após o evento F	PPSA	1 até 3
H	Teste de Penetração	recusa do relatório do PENTEST (Grey ou Black box)	ATÉ 5 dias corridos após o evento F	PPSA	1 até 3
I	Teste de vulnerabilidade	Solicitação para realização do Teste de vulnerabilidade	A critério da CONTRATANTE	PPSA	1 até 3
J	Teste de vulnerabilidade	Reunião de kickoff	Até 10 dias corridos após o evento I	CONTRATADA	1 até 3
k	Teste de vulnerabilidade	Execução do Teste de vulnerabilidade	Até 30 dias corridos após o evento J	CONTRATADA	1 até 3
L	Teste de vulnerabilidade	Entrega do relatório do Teste de vulnerabilidade	ATÉ 5 dias corridos após o evento K	CONTRATADA	1 até 3
M	Teste de vulnerabilidade	Aceite do Relatório do Teste de vulnerabilidade	ATÉ 5 dias corridos após o evento L	PPSA	1 até 3
N	Teste de vulnerabilidade	recusa do relatório do Teste de vulnerabilidade	ATÉ 5 dias corridos após o evento L	PPSA	1 até 3
O	Apresentação de resultados	Solicitação para realização de Apresentação de resultados	A critério da CONTRATANTE	PPSA	1 até 3
P	Apresentação de resultados	Reunião demonstrando a consolidação dos resultados	Até 10 dias corridos após o evento O	CONTRATADA	1 até 3
Q	Apresentação de resultados	Aceite do Apresentação	ATÉ 5 dias corridos após o evento P	PPSA	1 até 3
R	Apresentação de resultados	recusa da Apresentação	ATÉ 5 dias corridos após o evento P	PPSA	1 até 3

Para o início do Contrato serão considerados os eventos “A” e “B”. No evento “A” espera-se que a CONTRATADA e a PPSA façam as apresentações dos responsáveis pela continuidade do Contrato (formalização do preposto), e-mails, agenda e planejamento de execução de Contrato.

Para as reuniões de Kickoff (planejamento inicial) dos itens “D” e “J” a CONTRATADA deverá apresentar:

- Os cenários do plano de trabalho para cada PENTEST ou teste de vulnerabilidade;
- Atividades, indicando datas de início e término;
- Apresentação das metodologias a serem utilizadas;
- Lista dos recursos de software e hardware a serem utilizadas nos testes.

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

Para o serviço de teste de penetração (intrusão) ou vulnerabilidade será levado em consideração de 1 (uma) até 3 (três) recorrências dos eventos “C” até “R”. Caso a CONTRATADA receba a recusa do entregável no evento “H”, “N” ou “R” poderá realizar novamente o ciclo do cronograma deste serviço desde que seja aceito pela PPSA. Caso a CONTRATADA demonstre ser incapaz de realizar o serviço serão aplicadas as sanções e multas referentes ao item correspondente previstas em Contrato.

## 6. Acordo de nível de serviço (SLA)

- 6.1. Para as solicitações dos serviços mencionados neste termo de referência a CONTRATADA deverá disponibilizar um e-mail e um telefone de contato para que sejam realizados os pedidos dos serviços e acompanhamento.
- 6.2. A PPSA poderá solicitar a qualquer momento um relatório de Status durante a execução dos serviços, informando quais tarefas já foram realizadas, quais estão pendentes e um prazo para finalização.
- 6.3. A CONTRATADA será inteiramente responsável pelos profissionais e ferramentas para a execução dos serviços, não cabendo cobranças adicionais na prestação dos serviços que impliquem custos extras decorrentes da alocação dos profissionais ou ferramentas.
- 6.4. Caso a CONTRATADA, sem autorização prévia da PPSA, realize alguma ação que de alguma maneira afete o funcionamento dos serviços que hoje são oferecidos pela GTI da PPSA (inoperância total- Prioridade alta), deverá reestabelecer às suas expensas o serviço de maneira **imediata e mais breve possível**. Na impossibilidade de a CONTRATADA restabelecer o serviço serão aplicadas as sanções e multas correspondentes descritas neste termo de referência.
- 6.5. Para outros problemas decorrentes da prestação do serviço a CONTRATADA deverá realizar atendimento e registro das ocorrências para acompanhamento pelo e-mail e telefone fornecido anteriormente. A classificação do impacto

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

destes problemas será, a critério da PPSA, Média, Baixa ou Informação, e deverão ser resolvidos respectivamente em 3, 4 e 7 dias corridos após o seu registro.

## 7. CONFIDENCIALIDADE E SIGILO

Todas as informações a que a CONTRATADA tiver acesso em decorrência da prestação dos serviços relacionados ao objeto contratual serão consideradas “Informações Confidenciais” e serão objeto de sigilo, salvo se expressamente estipulado em contrário pela PPSA, sendo que:

- 7.1. A CONTRATADA se comprometerá a guardar confidencialidade e a não utilizar qualquer tipo de Informação Confidencial para propósitos estranhos àqueles definidos no Contrato firmado.
- 7.2. A CONTRATADA se comprometerá a adotar as medidas necessárias para que seus diretores, empregados, prepostos ou prestadores de serviços que estejam, direta ou indiretamente, envolvidos com a prestação de serviços objeto deste Contrato, que precisem conhecer a Informação Confidencial, mantenham sigilo sobre ela, adotando todas as precauções e medidas para que essas obrigações de confidencialidade sejam garantidas.
- 7.3. O compromisso de confidencialidade será permanente e se manterá durante o período de vigência do Contrato e após o seu término.
- 7.4. A divulgação de qualquer Informação Confidencial somente será possível mediante prévia e expressa autorização por escrito da PPSA ou quando requerida por Autoridades Governamentais, Administrativas e/ou Judiciárias e, nesses casos, a CONTRATADA deverá reportar o fato imediatamente à PPSA.

## 8. LOCAL DE PRESTAÇÃO DOS SERVIÇOS

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

8.1. Os serviços serão prestados no Escritório Central da PPSA, localizado no Centro Empresarial Internacional Rio Branco – RB1, na Av. Rio Branco nº 1, 4º Andar – Centro da cidade do Rio de Janeiro/RJ ou remotamente conforme acordado previamente com a PPSA.

## 9. ATRASO NA ENTREGA DO SERVIÇO E PENALIDADE ASSOCIADA

*O atraso na entrega do serviço é o tempo entre a data agendada para início da operação do serviço e a data efetiva do recebimento do entregável.*

9.1. Atrasos injustificáveis na entrega dos eventos “F”, “J”, “L” e “P” da tabela do cronograma irão resultar em multa de 0,5% do valor unitário, para o item referenciado na planilha de formulação da proposta, por dia de atraso, até o máximo de 5%. Atraso superior a este prazo de 10 dias corridos, poderá caracterizar, a critério da PPSA, inexecução parcial do Contrato, implicando a aplicação de sanções administrativas, sem prejuízo da multa por atraso prevista neste item.

9.2. Atrasos injustificáveis na realização dos eventos “E” e “K” da tabela do cronograma irão resultar em multa de 1% do valor unitário, para o item referenciado na planilha de formulação da proposta, por dia de atraso, até o máximo de 10%. Atraso superior a este prazo de 10 dias corridos, poderá caracterizar, a critério da PPSA, inexecução parcial do Contrato, implicando a aplicação de sanções administrativas, sem prejuízo da multa por atraso prevista neste item.

9.3. Para atrasos injustificáveis relacionados ao item 6.5 deste termo de referência a CONTRATADA irá pagar multa de 0,5% do valor global do Contrato por dia de atraso, até o máximo de 5%. Atraso superior a este prazo de 10 dias corridos, poderá caracterizar, a critério da PPSA, inexecução parcial do Contrato,

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

implicando a aplicação de sanções administrativas, sem prejuízo da multa por atraso prevista neste item.

## 10. MULTAS CONTRATUAIS E SANÇÕES ADMINISTRATIVAS

10.1. A PPSA aplicará à CONTRATADA, por atraso injustificado na execução do estabelecido no Instrumento Contratual, multa de 0,1% (zero vírgula um por cento) por dia de atraso, calculado sobre o valor contratado, até o limite máximo de 15% (quinze por cento) do valor total contratado.

10.2. Além de outras sanções previstas ao longo deste Contrato, à CONTRATADA serão ainda aplicadas as seguintes sanções, no caso da inexecução total ou parcial do Instrumento Contratual, garantidos os direitos ao contraditório e à ampla defesa:

10.2.1. Advertência;

10.2.2. Multa administrativa no percentual de 10% (dez por cento) do valor do Instrumento Contratual;

10.2.3. Suspensão temporária do direito de participar de licitações e de contratar com a PPSA, por prazo não superior a 2 (dois) anos.

10.3. A aplicação das penalidades estabelecidas neste item não impede que a PPSA rescinda unilateralmente o Instrumento Contratual, sem prejuízo do ajuizamento das ações cabíveis.

10.4. As multas aqui previstas poderão ser descontadas de qualquer valor devido à CONTRATADA ou cobradas mediante processo de execução, na forma da Lei Processual Civil.

10.5. Aplicam-se as disposições do Capítulo II-B do Título XI da Parte Especial do Decreto-Lei nº 2.848/1940 (Código Penal), nos termos da Lei nº 14.133/2021, conforme previsto na Lei nº 13.303/2016 (Lei das Estatais).

10.6. As sanções serão registradas e publicadas no Sistema de Cadastramento Unificado de Fornecedores – SICAF (“SICAF”).



**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

## 11. PRAZO DE EXECUÇÃO E EXIGÊNCIA

11.1. Os prazos de execução de 24 (vinte e quatro) meses e vigência dos serviços serão de 26 (vinte e seis) meses, contados da data de assinatura do Contrato.

## 12. FORMA E PRAZO DE PAGAMENTO

12.1. Após a conclusão e a aceitação de cada item contratado pela PPSA, a CONTRATADA deverá emitir o correspondente documento de cobrança e o respectivo boleto bancário, que deverá ser enviado para o e-mail financeiro@ppsa.gov.br, no prazo mínimo de 30 (trinta) dias antes de seu vencimento.

12.2. Os entregáveis considerados para o pagamento dos testes de penetração (Grey ou Black box) e vulnerabilidade será o envio dos relatórios entregues e aceitos pela PPSA para cada teste executado.

12.3. Para o pagamento da apresentação dos resultados serão considerados os arquivos utilizados durante a prestação do serviço e a gravação em vídeo da apresentação em formato amplamente utilizado.

12.4. A PPSA não reconhecerá nenhuma cobrança sem a formalização do aceite e recebimento do material dos entregáveis.

## 13. HABILITAÇÃO DA PROPONENTE

13.1. Um ou mais Atestados ou Declarações de Capacidade Técnica, em nome do proponente vencedor, emitidos por pessoa jurídica de direito público ou privado, que comprovem que a empresa já tenha executado, de forma satisfatória, serviço compatível com o objeto desta licitação.

13.2. Demonstrar que possui em seu quadro de funcionários profissional que seja capacitado com no mínimo 1 (um) dos certificados abaixo:

13.2.1. Offensive Security Certified Expert – OSCE

13.2.2. Offensive Security Certified Professional – OSCP



**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

13.2.3. Offensive Security Web Expert (OSWE)

13.2.4. SANS - GIAC Penetration Tester (GPEN)

13.2.5. SANS - GIAC Web Application Penetration Tester (GWAPT)

13.2.6. SANS - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

13.2.7. CEH MASTER - Certified Ethical Hacker Master

13.2.8. EC-COUNCIL – CNDA - Certified Network Defense Architect

13.2.9. CPTE - CERTIFIED Penetration Testing Engineer

13.3. Requisitos Econômico-Financeiros: a CONTRATADA deverá possuir patrimônio líquido positivo.

#### 14. OBRIGAÇÕES DA PRÉ-SAL PETRÓLEO – PPSA

- 14.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 14.2. Exercer o acompanhamento e a fiscalização dos serviços, por empregado especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis ou abrindo chamado no sistema da operadora;
- 14.3. Notificar a CONTRATADA por escrito (meio eletrônico) da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;
- 14.4. Pagar à CONTRATADA o valor resultante da prestação do serviço, no prazo e condições estabelecidas;
- 14.5. A PPSA não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.

**Número:**  
TR.DAFC.010/2024

**Emissão:** 25/07/2024

decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados;

14.6. Proporcionar todas as facilidades necessárias à boa execução dos serviços que deverão ser prestados;

14.7. Prover a infraestrutura física necessária à prestação dos serviços, às suas despesas, incluindo os sistemas de alimentação de energia, bem como local e instalações adequadas, dentro das condições mínimas.

## 15. OBRIGAÇÕES DA CONTRATADA

15.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta nas especificações técnicas deste termo de referência;

15.2. Relatar à PPSA toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

15.3. Manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

15.4. Garantir que todas as informações tratadas durante o período contratado são de exclusividade da PPSA;

15.5. Não utilizar, transferir e liberar dados, sistemas, processos e informações da PPSA para empresas nacionais, transnacionais, estrangeiras, ou países e governos estrangeiros;

15.6. Não utilizar as informações da PPSA para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

15.7. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício da atividade objeto desta licitação;

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

15.8. Responsabilizar-se por eventuais indenizações decorrentes de quaisquer danos ou prejuízos causados à PPSA ou a terceiros, por ação ou omissão própria ou de qualquer de seus empregados ou prepostos;

#### **16. Atendimento à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (“LGPD”):**

16.1. A CONTRATADA se compromete a observar, cumprir e respeitar, na sua integralidade, as normas de proteção e tratamento de dados pessoais ("Dados"), conforme o disposto na legislação de proteção de Dados vigente e aplicável, se vinculando integralmente à Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais" ou LGPD"), bem como à legislação superveniente que a substitua, altere ou que trate de matéria relacionada ao seu objeto, além de outras normas estabelecidas por autoridades nacionais ou agências responsáveis pela proteção de Dados.

16.2. A CONTRATADA compromete-se a manter a PPSA absolutamente indene de qualquer dano, prejuízo ou penalidade que possa vir a sofrer em decorrência de eventual infração à legislação de proteção de Dados perpetrada pela CONTRATADA.

16.3. Caso ocorra qualquer incidente na CONTRATADA envolvendo os Dados tratados juntamente com a PPSA (como violação de segurança, acessos não autorizados, perda, destruição, etc.), a CONTRATADA deverá comunicar formalmente o fato por meio do endereço eletrônico da DPO (dpo@ppsa.com.br), em até 24h (vinte e quatro horas), comprometendo-se, ainda, a auxiliar a PPSA em quaisquer questões envolvendo Dados tratados entre as organizações.

16.4. A CONTRATADA compromete-se que, ao subcontratar atividades envolvendo os Dados, realizará contrato escrito contendo as mesmas obrigações impostas por este contrato em relação à CONTRATADA, inclusive quanto às medidas

**Título:** Contratação de serviço de análise de vulnerabilidades e penetração para a Pré-Sal Petróleo – PPSA com apresentação de resultados.**Número:**  
TR.DAFC.010/2024**Emissão:** 25/07/2024

técnicas e de segurança das informações/dados pessoais que o subcontratado deverá implementar.

## 17. INFORMAÇÕES RELEVANTES FORMULAÇÃO DE PROPOSTA

17.1. A proposta deverá conter o valor unitário e o valor total multiplicado pela quantidade máxima de 3 (três) vezes por item, bem como o valor global:

Quantidade	Descrição	Tipo	Ambiente	Valor unitário	Valor Total
1 até 3	Teste de penetração	Black Box	Fora da PPSA	R\$ 00,0	R\$ 00,0
1 até 3	Teste de penetração	Grey Box	Dentro da PPSA	R\$ 00,0	R\$ 00,0
1 até 3	Teste de vulnerabilidade	-	-	R\$ 00,0	R\$ 00,0
1 até 3	Apresentação de resultados	-	-	R\$ 00,0	R\$ 00,0
Valor Global	-	-	-	-	R\$ 00,0

## 18. ANEXOS

18.1. Anexo I - Matriz de Risco.

Rio de Janeiro, 25 de julho de 2024.

**Elaborado por:**

**Aprovado por:**

**Gustavo Falquer Macabu**

**Samir Passos Awad**

**Gerente de TI**

**Diretor de Administração, Finanças e Comercialização**