ÍNDICE DE REVISÕES

REV.	DESCRIÇÃO E/OU FOLHAS ATINGIDAS

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATA	12/05/2026								
EXECUÇÃO	GFRY								
VERIFICAÇÃO	FN3B								
APROVAÇÃO	TTSJ								

AS INFORMAÇÕES DESTE DOCUMENTO SÃO PROPRIEDADE DA TRANSPETRO, SENDO PROIBIDA A UTILIZAÇÃO FORA DA SUA FINALIDADE.

ÍNDICE

1 OBJETIVO 3

2 DOCUMENTOS DE REFERÊNCIA 3

3 DEFINIÇÕES DE TERMOS, SIGLAS E ABREVIATURAS 3

4 LOCAIS DE PRESTAÇÃO DOS SERVIÇOS 4

5 DESCRIÇÃO DAS ATIVIDADES / entregas 4

6 CRITÉRIOS DE MEDIÇÃO 19

7 CONTROLE DE QUALIDADE 22

8 SUBCONTRATAÇÃO 22

9 CONSIDERAÇÕES GERAIS 22

1 OBJETIVO

Esta Especificação Técnica (ET) estabelece os requisitos mínimos para execução dos serviços objeto deste Contrato. Este Anexo compreende especificações para a realização de serviços especializados de operação em Segurança da Informação e as ferramentas a serem empregadas.

2 DOCUMENTOS DE REFERÊNCIA

2.1 Deverão ser obedecidas as informações constantes nesta ET e demais documentos e anexos relacionados ao contrato, bem como a edição ou revisão atualizada das Normas, Instruções Normativas, Acordos e Convenções Coletivas de Trabalho, Resoluções e toda a Legislação vigente e/ou que porventura vierem a surgir acerca do assunto que envolve e/ou afeta a prestação dos serviços, durante a execução do contrato.

3 DEFINIÇÕES DE TERMOS, SIGLAS E ABREVIATURAS

3.1 TERMOS

i. **COMUNICADO DE LIBERAÇÃO DE MATERIAL - CLM (RELEASE NOTE):** Documento emitido pelo responsável pela inspeção de fabricação, atestando a conformidade do bem com a documentação contratual, permitindo a liberação do bem após cumpridos todos os eventos de sinalados no Plano de Inspeção e Testes como HP (Hold Point) ou WP (Witness Point);

ii. **PT: Permissão de Trabalho -** autorização dada por escrito, em documento próprio da Unidade Solicitante, que autoriza a execução dos serviços.

3.2 SIGLAS OU ABREVIATURAS

i. **FT - Fiscalização**

ii. **AS - Autorização de Serviço**

iii. **ET - Especificação Técnica**

iv. **PPU - Planilha de Preços Unitários**

v. **EPI - Equipamento de Proteção Individual**

vi. **RM - Relatório de Medição**

vii. **BAD - Boletim de Avaliação de Desempenho**

viii. **UN - Unidade**

ix. **RO - Relatório de Ocorrência**

x. **DSMS - Diálogo de Segurança, Meio Ambiente e Saúde**

4 LOCAIS DE PRESTAÇÃO DOS SERVIÇOS

4.1. Os serviços serão prestados de forma remota para a sede da TRANSPETRO no Munícipio do Rio de Janeiro - RJ. Excepcionalmente a prestação de serviços poderá ocorrer de maneira presencial em suas instalações ou se fazer necessário o comparecimento presencial para reuniões, ocasião em que será informado à CONTRATADA, sem acréscimo de custos para a TRANSPETRO.

5 DESCRIÇÃO DAS ATIVIDADES / ENTREGAS

5.1 PURPLE TEAM

5.1.1 Gestão de Vulnerabilidades

5.1.1.1 Scan

A CONTRATADA deverá executar atividades de varredura de vulnerabilidades (scan) nos ativos da TRANSPETRO, observando, no mínimo, as seguintes atividades:

i) planejar as varreduras de vulnerabilidades, definindo previamente quais sistemas, redes, aplicações ou dispositivos serão analisados, as ferramentas de varredura a serem utilizadas e o agendamento das execuções junto às áreas envolvidas, de forma a minimizar o impacto no ambiente produtivo;
ii) realizar varreduras automatizadas nos ativos definidos, com o objetivo de identificar vulnerabilidades conhecidas (com base em CVEs) e fraquezas de segurança, tais como configurações inadequadas, portas desnecessariamente abertas, serviços indevidamente expostos, entre outras;
iii) analisar os resultados das varreduras, classificando as vulnerabilidades por grau de criticidade (baixa, média, alta e crítica), validando e descartando eventuais falsos positivos e correlacionando os achados com o contexto específico do ambiente da TRANSPETRO;
iv) elaborar relatórios técnicos e executivos contendo, no mínimo, o detalhamento das vulnerabilidades identificadas, os riscos associados, as recomendações de correção e a priorização das ações, considerando o impacto e a probabilidade de exploração de cada vulnerabilidade.

5.1.1.2 Coordenação de tratamento de vulnerabilidades

A CONTRATADA deverá coordenar o tratamento das vulnerabilidades identificadas, observando, no mínimo, as seguintes atividades:
i) encaminhar às equipes responsáveis (por exemplo, infraestrutura, desenvolvimento, operações) as recomendações de tratamento das vulnerabilidades, tais como aplicação de patches, reconfiguração de sistemas, desativação de serviços desnecessários ou implementação de controles compensatórios;
ii) propor, em conjunto com a TRANSPETRO, Acordos de Nível de Serviço (SLA) para tratamento das vulnerabilidades, de acordo com a criticidade dos achados e as responsabilidades de cada equipe, assegurando que os prazos definidos constem nos encaminhamentos às equipes responsáveis;
iii) monitorar a execução das ações de tratamento, considerando a criticidade das vulnerabilidades e os prazos acordados em SLA, elaborando relatório executivo mensal com o status das tratativas, com destaque, no mínimo, para vulnerabilidades críticas em atraso;
iv) realizar nova varredura (re-scan) nos ativos afetados após a conclusão das ações de correção, a fim de verificar a efetiva resolução das vulnerabilidades, ajustando, quando necessário, a classificação de risco e atualizando a base de dados de vulnerabilidades;
v) manter registro atualizado de todas as ações executadas no âmbito da gestão de vulnerabilidades, de forma a possibilitar consulta futura, gestão do conhecimento, comprovação de trilhas de auditoria e melhoria contínua do processo, utilizando o repositório oficial definido pela TRANSPETRO.

5.1.1.3 Indicadores

A CONTRATADA deverá criar e manter dashboards integrados à base de dados de vulnerabilidades da TRANSPETRO, contendo, no mínimo, os seguintes indicadores:

i) tempo médio para correção (MTTR – Mean Time to Remediate): tempo entre a identificação de uma vulnerabilidade e sua correção, detalhado por criticidade;
ii) tempo médio para identificação (MTTD – Mean Time to Detect): tempo médio para detecção de novas vulnerabilidades, considerando o ciclo de varreduras;
iii) taxa de vulnerabilidades corrigidas versus identificadas: percentual de vulnerabilidades efetivamente tratadas em relação ao total identificado no período;
iv) número de vulnerabilidades críticas não corrigidas, incluindo, quando aplicável, percentual de vulnerabilidades críticas por tipo de ativo (servidores, endpoints, aplicações, dispositivos de rede, etc.);
v) cobertura de varredura de vulnerabilidades: percentual de ativos do ambiente que estão sendo escaneados regularmente em relação ao total de ativos mapeados;
vi) frequência de varreduras: periodicidade das análises de vulnerabilidades (por exemplo, diária, semanal, mensal), por tipo de ativo ou escopo;
vii) taxa de falsos positivos: percentual de alertas classificados como falsos positivos em relação ao total de vulnerabilidades inicialmente identificadas;
viii) tendência de vulnerabilidades ao longo do tempo: evolução do número de vulnerabilidades identificadas, tratadas e pendentes, permitindo verificar se o ambiente está se tornando mais seguro ou mais exposto;
ix) conformidade com SLA de correção: percentual de vulnerabilidades corrigidas dentro dos prazos estabelecidos em SLA, por criticidade;
x) taxa de reincidência de vulnerabilidades: percentual de vulnerabilidades previamente tratadas que voltam a ocorrer, por tipo de ativo, tecnologia ou causa-raiz;
xi) taxa de visibilidade e conformidade das informações dos ativos no CMDB: relação entre os ativos cadastrados e corretamente documentados no CMDB e os ativos identificados automaticamente nas varreduras, medindo a quantidade e a qualidade das informações de inventário de ativos.

5.1.2 DevSecOps

A CONTRATADA deverá executar atividades de DevSecOps, integrando segurança aos processos de desenvolvimento e entrega contínua, observando, no mínimo, as seguintes atividades:
i) realizar verificações estáticas (SAST), dinâmicas (DAST) e de componentes (SCA – Software Composition Analysis) das aplicações publicadas no ambiente produtivo da TRANSPETRO e, quando aplicável, em outras etapas do pipeline de desenvolvimento, conforme acordado com a TRANSPETRO;
ii) configurar, ajustar e manter os parâmetros, políticas e controles de segurança aplicáveis à cadeia de desenvolvimento (CI/CD), visando à melhoria contínua do processo, em alinhamento com as normas e diretrizes de segurança da TRANSPETRO;
iii) acompanhar o ciclo de vida das exceções de segurança autorizadas durante a cadeia de desenvolvimento, assegurando que estejam formalmente registradas, justificadas, aprovadas e revisadas periodicamente, conforme normativos internos da TRANSPETRO;
iv) elaborar relatórios contendo as vulnerabilidades identificadas nas aplicações analisadas, classificando-as por criticidade (baixa, média, alta e crítica) e indicando, sempre que possível, recomendações de correção ou mitigação;
v) produzir e manter dashboards e relatórios com, no mínimo, os seguintes indicadores de DevSecOps:
a) cobertura de segurança no pipeline: percentual de pipelines de desenvolvimento que possuem etapas de avaliação de segurança (SAST, DAST, SCA ou equivalentes) efetivamente executadas;
b) número de vulnerabilidades por versão de aplicação avaliada;
c) número de versões de aplicações bloqueadas por falhas de segurança;
d) tempo médio de correção de vulnerabilidades (MTTR);
e) cobertura de testes de segurança automatizados: percentual de aplicações e/ou pipelines que possuem testes de segurança automatizados configurados e em operação;
f) adequação às políticas de segurança: percentual de aplicações que atendem às políticas e padrões de segurança definidos pela TRANSPETRO, considerando critérios como tratamento de vulnerabilidades, uso de componentes aprovados e observância de exceções formalizadas.

5.1.3 Pentest

A CONTRATADA deverá executar serviços de teste de invasão (pentest), utilizando metodologia, infraestrutura e ferramentas próprias, alinhadas ao estado da arte em offensive cyber security, observando, no mínimo, as seguintes atividades:

i) realizar testes de intrusão em aplicações (incluindo aplicações desenvolvidas no paradigma SAP), sistemas operacionais, aplicações on-premises e nativas de nuvem (multivendor), infraestrutura de redes e demais componentes, propondo melhores práticas para reduzir o grau de exposição do alvo e as possíveis implicações sistêmicas decorrentes da exploração de vulnerabilidades;
ii) realizar testes de intrusão direcionados a redes, incluindo tentativas de acesso a segmentos segregados e evasão de equipamentos de proteção, emitindo recomendações para mitigação e redução do risco corporativo;
iii) realizar testes de intrusão a partir de infraestrutura própria segregada da rede da TRANSPETRO, empregando táticas, técnicas, procedimentos, metodologias, ferramentas e processos compatíveis com a literatura e a prática de offensive cyber security, sendo a CONTRATADA responsável pelo fornecimento de toda a infraestrutura necessária (servidores externos às instalações da TRANSPETRO, conectividade e acesso à Internet, no-breaks, etc.) e de quaisquer softwares utilizados (tais como BurpSuite Professional, acesso às APIs do Shodan, entre outros), incluindo licenciamento;
iv) realizar, de forma periódica, atividades de survey, footprint e fingerprint de serviços e aplicações internos e externos à TRANSPETRO, utilizando a infraestrutura própria mencionada, além de ferramentas de varredura externas, inclusive versões pagas (por exemplo, Shodan licenciado), sendo de responsabilidade da CONTRATADA o fornecimento e a gestão das licenças necessárias aos analistas de pentest;
v) gerar, analisar e revisar relatórios de pentest e de avaliações de vulnerabilidades de sistemas desenvolvidos interna ou externamente para a TRANSPETRO, incluindo aqueles cujo código-fonte seja de propriedade da TRANSPETRO, bem como de sistemas COTS (commercial off-the-shelf), com proposição de correções e/ou controles compensatórios;
vi) interpretar de forma aprofundada os resultados de ferramentas de scan, análises e postura de segurança, compreendendo os termos de Segurança da Informação e os relatórios de quaisquer ferramentas de análise de vulnerabilidades de infraestrutura, vulnerabilidades de software, correlação de eventos de segurança (SIEM), soluções de threat hunting e threat intelligence, soluções anti-DDoS, firewalls, IPS/IDS, packet brokers, proxies, NAV, DLP e demais soluções correlatas;
vii) realizar testes de invasão explorando vulnerabilidades apresentadas por ferramentas de DAST, SAST, SCA (avaliação de componentes abertos de terceiros incorporados ao software) e IAST, com a materialização do sucesso da exploração ou, ao menos, com evidências claras de todos os testes e técnicas empregados;
viii) realizar testes dinâmicos em aplicações web utilizando ferramentas gratuitas, open source ou outras que venham a ser adotadas pela TRANSPETRO; a CONTRATADA deverá possuir licenças de Burp Suite Professional e Metasploit Pro em quantidade igual ao número de especialistas e analistas de pentest alocados, de forma que cada profissional possa atuar de maneira independente, com acesso próprio aos recursos das ferramentas;
ix) realizar testes de intrusão em aplicações não-web por meio de técnicas como engenharia reversa, análise de fluxos de dados, avaliação de artefatos, avaliação de uso de pilha de memória, interrupção de processos, uso de frameworks como Metasploit/Meterpreter, entre outras técnicas adequadas;
x) interpretar e promover ataques em resposta a análises de segurança (scans) de imagens de contêineres em ambientes on-premises e em nuvem, avaliando a postura de segurança dos ambientes e a aderência às melhores práticas de proteção;
xi) desenvolver payloads maliciosos personalizados para utilização nas diversas ferramentas de ataque empregadas (tais como Metasploit, Meterpreter e Nmap), quando necessário para validação de cenários específicos de exploração de vulnerabilidades;
xii) utilizar APIs e desenvolver soluções de integração e interpretação de resultados gerados pelas ferramentas de segurança de aplicações e de infraestrutura empregadas pela TRANSPETRO, de forma a agregar, correlacionar e enriquecer os achados de segurança;
xiii) realizar testes de intrusão em aplicações desenvolvidas em paradigma low-code, como, por exemplo, aplicações desenvolvidas em plataforma Microsoft Power Apps/Power Platform (Microsoft 365) ou equivalente;
xiv) realizar testes de intrusão em aplicações e redes específicas de automação industrial, compreendendo, porém não se limitando a evasão de equipamentos de segregação de redes industriais, invasão de equipamentos de telecomunicações industriais, invasão de PLCs, sistemas SCADA, SDCD, Fieldbus, Modbus e demais protocolos e tecnologias de automação;
xv) elaborar relatórios executivos e técnicos para todas as atividades de pentest, contendo o detalhamento de todas as etapas, desde o survey/footprint até o eventual estabelecimento de canal de command and control (C2), se bem-sucedido, incluindo evidências, análise de risco e recomendações;
xvi) desenvolver painéis de Business Intelligence (BI) para apresentação dos resultados e

acompanhamento da evolução das atividades de pentest e do progresso das correções implementadas nos ambientes;
xvii) realizar retestes, de forma otimizada e sempre que houver implementação de correções relevantes, visando à verificação contínua da possível persistência dos achados e da efetividade das ações de remediação;
xviii) realizar testes em APIs, avaliando, inclusive, o tráfego por meio de ferramentas de inspeção de dados (tais como tcpdump e Wireshark), para avaliação da segurança dos dados em repouso e em trânsito, bem como para proposição de melhores práticas de implementação e proteção;
xix) realizar testes de intrusão em aplicações nativas de nuvem (desenvolvidas, construídas e implantadas para nuvem), avaliando, inclusive, a postura de segurança nos perímetros afetados e a qualidade dos artefatos de infraestrutura como código (Infrastructure as Code – IaC) empregados;
xx) realizar testes de intrusão em componentes mantenedores de nuvens (por exemplo, funções serverless como Lambdas e serviços de automação como Azure Automation), avaliando a qualidade da proteção do ambiente e das aplicações que utilizem tais componentes;
xxi) realizar testes de intrusão em dispositivos móveis (iOS e Android), incluindo ataques cibernéticos direcionados tanto aos aplicativos quanto aos respectivos sistemas operacionais;
xxii) realizar testes de intrusão, incluindo, mas não se limitando a, ataques do tipo man-in-the-middle, tampering e hacking, para avaliação da segurança de dispositivos físicos tais como periféricos que empreguem interfaces aéreas (WiFi, Bluetooth ou protocolos proprietários, como dongles de fabricantes específicos, teclados e fones sem fio), microprocessadores, controladoras, PLCs e outros; a CONTRATADA deverá disponibilizar todos os hardwares necessários à execução dessas atividades, arcando com os respectivos custos, incluindo, a título exemplificativo, equipamentos como Crazyradio PA 2,4 GHz USB dongle e SparkFun nRF24LU1+ breakout board;
xxiii) realizar testes de intrusão com o uso de equipamentos portáteis de hacking digital que possuam comunicação WiFi, Bluetooth, RF, RFID, NFC, infravermelho, interfaces GPIO e USB, entre outras; a CONTRATADA deverá arcar com a aquisição de, ao menos, dois desses equipamentos para realização de testes nas instalações da TRANSPETRO, com o objetivo de identificar vulnerabilidades exploráveis por agentes maliciosos que façam uso desses dispositivos;
xxiv) desenvolver e implantar programas de gamificação de hacking (tais como ambientes de Capture The Flag – CTF) para estimular, junto às equipes de desenvolvimento e demais áreas envolvidas, a cultura de desenvolvimento seguro (SSDLC – Secure Software Development Life Cycle).

5.1.3.1 Indicadores de Pentest

A CONTRATADA deverá criar e manter dashboards e relatórios referentes às atividades de pentest, contendo, no mínimo, os seguintes indicadores:
i) Quantidade de testes realizados: número de pentests realizados por período (mensal/trimestral/anual), por tipo de alvo (aplicações web, APIs, infra, OT, nuvem, dispositivos móveis, etc.);
ii) Cobertura de escopo: percentual de escopo efetivamente testado em relação ao escopo originalmente aprovado para cada pentest;
iii) Vulnerabilidades identificadas por pentest: quantidade média de vulnerabilidades identificadas por teste, segmentadas por criticidade (baixa, média, alta e crítica);
iv) Taxa de vulnerabilidades exploráveis: percentual de vulnerabilidades para as quais foi possível demonstrar exploração (PoC) em relação ao total de vulnerabilidades identificadas;
v) Tempo médio do ciclo de pentest: tempo médio entre o início do planejamento do teste e a emissão do relatório final (planejamento, execução, análise e reporte);
vi) Taxa de recomendações implementadas: percentual de recomendações de segurança provenientes de pentests que foram efetivamente implementadas pelas áreas responsáveis, por criticidade;
vii) Tempo médio até o reteste: tempo médio entre a implementação das correções e a realização de retestes para validação da remediação;
viii) Redução de vulnerabilidades entre ciclos: variação (absoluta e percentual) do número de vulnerabilidades (por criticidade) entre ciclos sucessivos de pentest sobre o mesmo ativo/ambiente;
ix) Recorrência de vulnerabilidades: percentual de vulnerabilidades já apontadas em ciclos anteriores de pentest que voltam a aparecer em novos testes sobre os mesmos ativos.

5.2 SOC

5.2.1 SIEM

A CONTRATADA deverá operar soluções de Segurança da Informação da TRANSPETRO, incluindo, no mínimo:

i) SIEM (Security Information and Event Management);
ii) SOAR (Security Orchestration, Automation and Response);
iii) EDR (Endpoint Detection and Response);
iv) XDR (Extended Detection and Response);
v) soluções de varredura/scan de vulnerabilidades;
vi) MISP (Malware Information Sharing Platform);
vii) ASM (Attack Surface Management);
viii) ferramentas de pentest;
ix) ferramentas de perícia digital;
x) ferramentas de DLP;
xi) ferramentas SASE;
xii) outras ferramentas correlatas com foco em segurança que venham a ser adotadas pela TRANSPETRO.

A CONTRATADA deverá operar todas as soluções de forma a garantir os níveis de serviço especificados e o atendimento a todos os requisitos desta Especificação de Serviços, observando, no mínimo, as seguintes atividades:

i) realizar o aprovisionamento, a desmobilização e a configuração dos coletores e do ambiente gerenciado em nuvem, incluindo a alocação, movimentação, cadastro e disponibilização de recursos físicos e lógicos, bem como a parametrização necessária para seu correto funcionamento;
ii) prover suporte especializado e administração do ambiente gerenciado, abrangendo as soluções de segurança sob sua responsabilidade;
iii) gerir os níveis de serviço do ambiente gerenciado, assegurando o cumprimento dos SLAs acordados com a TRANSPETRO;
iv) realizar o planejamento de capacidade do ambiente gerenciado, com vistas ao dimensionamento adequado, à expansão controlada e à prevenção de degradação de desempenho;
v) executar, participar e apoiar projetos de melhoria operacional, tais como consolidações, atualizações tecnológicas, migrações, integrações e desativações de componentes ou soluções;
vi) manter atualizadas as documentações e os procedimentos necessários para administração, operação e suporte do ambiente gerenciado, promovendo sua revisão sempre que houver mudanças relevantes;
vii) prestar esclarecimentos, fornecer informações e orientações técnicas necessárias à solução de problemas detectados no ambiente gerenciado;
viii) garantir a monitoração contínua, bem como acompanhar o desempenho e a disponibilidade das soluções, atuando para manter os níveis descritos nesta Especificação, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
ix) garantir a execução de todos os procedimentos, processos e padrões de gestão definidos pela TRANSPETRO, observando as diretrizes corporativas de Segurança da Informação;
x) atender às solicitações da TRANSPETRO, conforme processos e ferramentas por ela definidos, garantindo o cumprimento dos níveis de serviço estabelecidos nesta Especificação;
xi) gerenciar, de forma proativa, a capacidade das soluções, acompanhando, otimizando e realizando ajustes de desempenho do ambiente gerenciado;
xii) acionar diretamente o FABRICANTE, fornecedor ou suporte das soluções, quando necessário, para tratamento de incidentes, problemas ou demandas técnicas, bem como para obtenção de informações e revisão de recomendações relacionadas ao ambiente gerenciado;
xiii) garantir que a TRANSPETRO esteja sempre utilizando a versão mais atualizada e indicada pelo FABRICANTE dos coletores e demais componentes sob responsabilidade da CONTRATADA, incluindo a aplicação de patches e atualizações necessárias;
xiv) garantir que a TRANSPETRO esteja sempre utilizando, quando aplicável, a versão mais atualizada e indicada pelo FABRICANTE das soluções em nuvem, em consonância com o calendário de atualização e boas práticas do fornecedor;

xv) interagir com as equipes internas da TRANSPETRO (tecnologia, segurança, operação, entre outras) para resolução de problemas, alinhamento de configurações e tratamento de incidentes;
xvi) realizar a configuração de quaisquer funcionalidades, ajustes ou atividades necessárias para o pleno uso das soluções ofertadas, observando requisitos de segurança, desempenho e conformidade;
xvii) apoiar a TRANSPETRO na identificação, análise e tratamento de incidentes de segurança cibernética, utilizando os recursos e capacidades das soluções operadas, inclusive para fins de correlação, automação e orquestração de respostas;
xviii) realizar análise constante do ambiente da TRANSPETRO para recomendar e, quando aplicável, implementar a melhor forma de uso e configuração das soluções, interagindo com o FABRICANTE, fornecedor ou suporte das soluções, a fim de garantir aderência às melhores práticas indicadas pelo FABRICANTE e às diretrizes de Segurança da Informação da TRANSPETRO.

5.2.1.1 Indicadores de SIEM

A CONTRATADA deverá criar e manter dashboards e relatórios integrados às soluções de SIEM e correlatas, contendo, no mínimo, os seguintes indicadores:
i) Volume de eventos processados: número de eventos de segurança processados pelo SIEM por período (por dia/mês), por fonte de log e por tipo de evento;
ii) Cobertura de logging: percentual de ativos, sistemas e aplicações críticos que enviam logs ao SIEM em relação ao total de ativos definidos como escopo mínimo de monitoração;
iii) Número de alertas gerados vs. analisados: quantidade de alertas emitidos pelo SIEM e percentual de alertas analisados pela equipe em determinado período;
iv) Tempo médio de detecção (MTTD-SIEM): tempo médio entre a ocorrência de um evento de segurança relevante e a geração do alerta correspondente no SIEM;
v) Tempo médio até início de análise (MTTI): tempo médio entre a geração do alerta pelo SIEM e o início efetivo da análise pela equipe;
vi) Taxa de falsos positivos: percentual de alertas gerados pelo SIEM que, após análise, são classificados como falsos positivos;
vii) Taxa de casos de uso ativos: percentual de casos de uso implantados e operacionais em relação ao total de casos de uso planejados ou aprovados pela TRANSPETRO;
viii) Atualização de casos de uso: número de novos casos de uso criados e de casos de uso revisados/otimizados em determinado período;
ix) Disponibilidade da plataforma de monitoração: percentual de disponibilidade do SIEM e componentes associados (coletores, forwarders, correlação central) no período;
x) Integrações de fontes de log pendentes: número de integrações relevantes ainda não realizadas (por criticidade do sistema/ativo);
xi) Alertas por caso de uso: distribuição de alertas por caso de uso, com destaque para aqueles que mais contribuem para detecções relevantes ou maior volume de falsos positivos.

5.2.2 CSIRT

5.2.2.1 Forense Digital

A CONTRATADA deverá executar ações de Forense Digital em atendimento às solicitações da TRANSPETRO, atuando na aquisição, preservação, análise e recuperação de dados e/ou backups, entre outros, nas seguintes tecnologias e ambientes, no mínimo:

a) ambientes e sistemas SAP;
b) ambientes de correio eletrônico (MS Outlook);
c) dispositivos móveis e demais endpoints;
d) ambiente de Internet (roteadores, firewalls, caches, balanceadores, entre outros);
e) Microsoft AD e Microsoft Entra ID;
f) Microsoft Office 365 (Outlook, Teams, SharePoint, OneDrive, entre outros);
g) sistemas operacionais Windows;
h) sistemas Unix/Linux;
i) sistemas de banco de dados;
j) servidores de aplicação e webservers;
k) solução de SIEM;

l) solução de Data Lake;
m) ambientes de nuvem;
n) pacote Microsoft Defender.
No âmbito das atividades de Forense Digital, a CONTRATADA deverá, ainda, no mínimo:
i) operar com o uso das ferramentas de perícia digital amplamente reconhecida pelo mercado e em conformidade com o padrão forense reconhecido para a formação de cadeia de custódia firme e robusta, tais como FTK Imager, Autopsy, Volatility, IPED, Cellebrite, EnCase Forensic;
ii) realizar a administração e o suporte técnico dos softwares utilizados nos processos de Forense Digital na TRANSPETRO, incluindo instalação, configuração, atualização e troubleshooting;
iii) manter a infraestrutura dedicada à Forense Digital (servidores, sistemas operacionais, storages e demais componentes) atualizada e em condições adequadas de desempenho e segurança;
iv) interagir com as demais áreas e equipes da TRANSPETRO para obtenção das informações necessárias à execução das atividades de Forense Digital, observando as normas internas de acesso e confidencialidade;
v) executar transcrição de áudios, quando demandado, para integração com a plataforma NUIX ou soluções equivalentes;
vi) manter e evoluir as automatizações de coleta de artefatos e dispositivos nos sistemas operacionais suportados, de forma a otimizar o processo de obtenção de evidências;
vii) prover, quando tecnicamente possível e legalmente permitido, o desbloqueio de senha de dispositivos móveis de alta gama (Apple e Android), incluindo modelos mais recentes, com vistas à extração de evidências;
viii) automatizar, sempre que possível, a coleta e o processamento de evidências com base no sistema de solicitação de demandas da TRANSPETRO, integrando-o ao sistema de coleta e gestão de evidências;
ix) realizar a ingestão de dados nas ferramentas de Forense Digital, efetuar o processamento técnico das evidências e publicar os resultados em ambiente apropriado para revisão pelas áreas internas da TRANSPETRO;
x) realizar pesquisa, correlação e análise técnica das evidências e/ou logs, considerando contexto, linha do tempo, atores envolvidos e possíveis impactos;
xi) executar todas as demais ações necessárias à condução de processos investigativos demandados interna ou externamente (por exemplo, auditorias, apurações internas, requisições de órgãos competentes), observadas as normas legais e regulatórias aplicáveis;
xii) realizar o trabalho de coleta, indexação, preservação, análise e armazenamento das evidências, assegurando sua integridade, autenticidade e cadeia de custódia;
xiii) elaborar relatórios (ou registros formais) contendo a descrição das evidências, a análise técnica realizada, a identificação do possível perpetrador e do método de ataque ou conduta ilícita, os potenciais danos ao ambiente da TRANSPETRO e as medidas de proteção imediatas e definitivas recomendadas;
xiv) atuar em conformidade com as referências dos padrões ISO/IEC 27K aplicáveis à Forense Digital, em especial as normas ISO/IEC 27037, 27041, 27042, 27043 e 27050 (ou suas versões vigentes);
xv) atuar em conjunto com as áreas responsáveis por apurações/investigações (por exemplo, jurídico, compliance, recursos humanos, auditoria) para melhor entendimento das demandas, alinhamento de escopo e obtenção de informações adicionais;
xvi) gerar relatório consolidado mensal contendo o resumo de todas as demandas de Forense Digital atendidas no período, incluindo, no mínimo, tipo de caso, área demandante, status, principais achados e eventuais recomendações recorrentes.

5.2.2.2 Tratamento de incidentes

A CONTRATADA deverá monitorar e tratar incidentes de Segurança da Informação detectados por soluções de SIEM, Antivírus e demais ferramentas de segurança da TRANSPETRO, atuando em todas as etapas do ciclo de resposta a incidentes, em regime contínuo de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, incluindo, no período noturno, o papel de equipe de primeiro atendimento para outros serviços de Segurança da Informação (por exemplo, inteligência contra ameaças e vulnerabilidades emergenciais), observando, no mínimo, as seguintes atividades:

i) garantir que processos, pessoas e tecnologias estejam previamente preparados de forma adequada para o tratamento de incidentes, incluindo a manutenção de procedimentos operacionais, bases de conhecimento, meios de comunicação, listas de contato, treinamentos, hardware e software necessários, entre outros;

ii) monitorar e receber incidentes de Segurança da Informação, incluindo a monitoração proativa de eventos em busca de anomalias, o recebimento de alertas automatizados, o atendimento a notificações internas e externas à TRANSPETRO e a avaliação rotineira de relatórios gerados pelas ferramentas de segurança;
iii) realizar o tratamento do incidente identificado, desde o alerta inicial até sua resolução, contemplando, conforme aplicável, as etapas de preparação, monitoração, triagem, análise, contenção, erradicação e recuperação;
iv) conduzir atividades de pós-incidente, garantindo o registro adequado, a retroalimentação das lições aprendidas e a melhoria contínua do processo de resposta a incidentes;
v) propor e implementar, de forma proativa, melhorias nos processos, procedimentos, casos de uso, regras de detecção e fluxos de tratamento de incidentes;
vi) classificar os incidentes quanto à categoria, severidade e demais atributos definidos pela TRANSPETRO, observando critérios formais de priorização;
vii) qualificar incidentes como falsos positivos ou incidentes confirmados, registrando a justificativa e os elementos técnicos que suportam a conclusão;
viii) analisar causa raiz, abrangência e impactos dos incidentes, considerando ativos afetados, dados envolvidos, vetores de ataque, dependências e possíveis efeitos em cadeia;
ix) propor, coordenar e, quando estiver sob sua responsabilidade, executar soluções para contenção e/ou erradicação de ameaças, bem como para recuperação dos ativos afetados, em articulação com as áreas técnicas envolvidas;
x) coletar, processar, analisar e armazenar evidências relacionadas ao incidente, observando as diretrizes de Forense Digital, cadeia de custódia e requisitos legais aplicáveis;
xi) solicitar e coordenar a execução de atividades necessárias à resolução de incidentes que sejam de responsabilidade de outras áreas da TRANSPETRO e/ou de entidades externas (por exemplo, equipes de infraestrutura, desenvolvimento, fornecedores e outsourcers);
xii) coordenar o fluxo de comunicação durante e após o tratamento de incidentes, em conformidade com os planos e processos de comunicação definidos pela TRANSPETRO;
xiii) monitorar a eficácia das soluções aplicadas (técnicas e processuais), ajustando-as quando necessário e registrando as lições aprendidas;
xiv) realizar a devida escalação e notificação de incidentes, conforme critérios, níveis e fluxos de aprovação definidos pela TRANSPETRO;
xv) registrar de forma detalhada, em ferramenta oficial da TRANSPETRO, o tratamento dado a cada incidente em todas as suas etapas, contendo, no mínimo, datas, horários, responsáveis, ações executadas, decisões tomadas e situação final;
xvi) elaborar, a critério e demanda da TRANSPETRO, relatórios técnicos e/ou executivos sobre incidentes específicos, contendo síntese do ocorrido, linha do tempo, análise técnica, impactos, causa raiz e recomendações;
xvii) realizar o desenho, a análise crítica e a proposta de melhoria contínua de casos de uso de detecção, regras de correlação de eventos e demais mecanismos de alerta em qualquer ferramenta de segurança da TRANSPETRO (por exemplo, SIEM, EDR, Data Lake de segurança, DLP), alinhando-os à evolução do ambiente e do cenário de ameaças;
xviii) atuar, no período noturno, como equipe de primeiro atendimento para outros serviços de Segurança da Informação, conforme definido pela TRANSPETRO, assegurando o registro e, quando aplicável, o encaminhamento ou tratamento inicial de eventos relacionados à inteligência contra ameaças, vulnerabilidades emergenciais e demais ocorrências de segurança.

5.2.2.3 Indicadores de Forense Digital

A CONTRATADA deverá criar e manter dashboards e relatórios referentes às atividades de Forense Digital, contendo, no mínimo, os seguintes indicadores:

i) Quantidade de casos forenses: número de casos de Forense Digital abertos, em andamento e concluídos por período, por tipo de demanda (apuração interna, apoio a incidente, requisição externa, etc.);
ii) Tempo de resposta inicial: tempo médio entre a abertura da solicitação de Forense Digital e o início efetivo das atividades (coleta/análise);
iii) Tempo médio de conclusão de casos: tempo médio para conclusão das análises forenses e emissão do relatório correspondente, segmentado por tipo de caso e complexidade;
iv) Integridade e cadeia de custódia: percentual de casos em que toda a cadeia de custódia foi formalmente

registrada e mantida conforme procedimentos definidos;
v) Evidências coletadas: número médio de evidências coletadas por caso (imagens, logs, artefatos de sistema, dumps de memória, etc.), podendo ser agrupado por tipo de evidência;
vi) Automação de coletas: percentual de coletas realizadas por mecanismos automatizados, quando disponíveis, em relação ao total de coletas realizadas;
vii) Relatórios emitidos: número de relatórios técnicos e/ou executivos de Forense Digital emitidos por período;
viii) Retrabalho/novas coletas: quantidade de casos em que foi necessária nova coleta ou reprocessamento de evidências por falhas, incompletude ou necessidade de aprofundamento;
ix) Atendimento a prazos regulatórios/legais: percentual de demandas que possuíam prazo legal/regulatório e foram atendidas dentro do prazo.

5.2.2.4 Indicadores de Tratamento de Incidentes

A CONTRATADA deverá criar e manter dashboards e relatórios referentes ao tratamento de incidentes de Segurança da Informação, contendo, no mínimo, os seguintes indicadores:

i) Quantidade de incidentes: número de incidentes registrados por período, segmentados por categoria (malware, phishing, acessos indevidos, data leakage, indisponibilidade, etc.) e por severidade;
ii) Tempo médio de detecção (MTTD-Incidente): tempo médio entre a ocorrência do incidente e sua detecção (por SIEM, ferramenta, notificação de usuário ou outro canal);
iii) Tempo médio até início do tratamento (MTTI): tempo médio entre a detecção/registro do incidente e o início efetivo das ações de resposta pela equipe;
iv) Tempo médio de resolução (MTTR-Incidente): tempo médio entre o registro do incidente e sua resolução/encerramento formal;
v) Cumprimento de SLA de incidentes: percentual de incidentes tratados e encerrados dentro dos prazos estabelecidos em SLA, por severidade;
vi) Taxa de falsos positivos: percentual de registros inicialmente classificados como incidentes que, após análise, são reclassificados como falsos positivos;
vii) Distribuição por causa raiz: percentual de incidentes por causa raiz identificada (falha de processo, erro humano, falha de controle técnico, vulnerabilidade não corrigida, etc.);
viii) Recorrência de incidentes: percentual de incidentes recorrentes (mesmo tipo, mesma causa raiz ou mesmo ativo) em relação ao total de incidentes;
ix) Ações de melhoria pós-incidente: número de ações corretivas e preventivas geradas a partir de lições aprendidas, bem como percentual das ações implementadas no período;
x) Incidentes com impacto relevante: número de incidentes que resultaram em impacto significativo (por exemplo, indisponibilidade crítica, perda de dados, exposição de informação sensível), por período.

5.3 Segurança de ambientes

5.3.1 Nuvem, Corporativo e Automação

A CONTRATADA deverá atuar na segurança de ambientes em nuvem, corporativos e operacionais/industriais, elaborando pareceres técnicos, avaliações de risco e propondo controles, observando, no mínimo, as seguintes atividades:

i) elaborar pareceres técnicos e avaliações de risco, propondo controles de segurança para cenários de uso em nuvem (incluindo multicloud) e ambientes industriais/OT;
ii) definir, revisar e propor melhorias contínuas em políticas, normas, padrões, procedimentos e arquiteturas de segurança cibernética, em alinhamento com as diretrizes da TRANSPETRO;
iii) propor, planejar e executar projetos, iniciativas e provas de conceito (PoC) de soluções de segurança cibernética, incluindo testes de aderência, viabilidade técnica e benefícios esperados;
iv) realizar prospecção, estudo e avaliação de novas tecnologias e soluções de segurança, com foco no aumento da maturidade de segurança da TRANSPETRO;
v) definir, documentar e acompanhar baseline de segurança para serviços SaaS e ambientes industriais, incluindo requisitos mínimos de configuração, monitoramento e proteção;
vi) identificar lacunas e propor melhorias em políticas, processos, procedimentos e arquiteturas de segurança, com base em análises de risco, incidentes, vulnerabilidades e avaliações de maturidade;
vii) analisar ambientes (nuvem, multinuvem, corporativo e industrial) e propor arquiteturas e controles de

proteção, considerando segmentação, zero trust, proteção de perímetro, identidade, dados e aplicações;
viii) documentar especificações técnicas, arquiteturas, fluxos e procedimentos de segurança, garantindo que estejam atualizados e acessíveis às áreas envolvidas;
ix) realizar análises de boas práticas, benchmarkings e avaliações de maturidade com base em normas, frameworks e referências de mercado, tais como Gartner, Forrester, ISA/IEC 62443, ISA-95, NIST 800-82, NIST-CSF, NERC-CIP e ISO/IEC 27001 (ou suas versões vigentes);
x) monitorar e apoiar o tratamento de incidentes de Segurança da Informação relacionados a ambientes em nuvem, corporativos e industriais, incluindo escalonamentos e demandas críticas, em coordenação com o CSIRT/SOC;
xi) gerar relatórios, dashboards e gráficos dinâmicos com base em dados analisados, para apoio à tomada de decisão e acompanhamento de indicadores de segurança;
xii) adotar metodologias ágeis, tais como Scrum e Kanban, para gestão, priorização e acompanhamento das atividades de segurança, quando aplicável;
xiii) atuar na gestão e no compartilhamento de conhecimento técnico em segurança cibernética, promovendo workshops, treinamentos internos, documentação de lições aprendidas e repositórios de conhecimento;
xiv) avaliar e acompanhar indicadores internos e externos relacionados à segurança cibernética (por exemplo, indicadores de risco, ameaças emergentes, vulnerabilidades, trends de mercado), propondo ações de melhoria contínua.

5.3.1.1 Segurança de Endpoints

A CONTRATADA deverá atuar como referência técnica na área de proteção de estações de trabalho, servidores Windows e Linux e dispositivos móveis, tanto no ambiente corporativo quanto nos ambientes de navios e de automação/operacionais, em um ou mais processos de Segurança da Informação, a critério da TRANSPETRO, observando, no mínimo, as seguintes atividades:

i) executar atividades operacionais relacionadas à segurança de endpoints e tratar incidentes envolvendo estações de trabalho, servidores e dispositivos móveis;
ii) atuar em escalações e demandas de maior complexidade e/ou severidade, apoiando tecnicamente as equipes de primeira linha e outras áreas envolvidas;
iii) definir, revisar e manter atualizados processos e procedimentos relacionados à segurança de endpoints, incluindo padrões de configuração, hardening, resposta a incidentes e uso das soluções de proteção;
iv) atuar na gestão e compartilhamento de conhecimento técnico sobre segurança de endpoints, incluindo boas práticas, lições aprendidas, guias de uso e treinamentos internos;
v) propor e executar atividades de melhoria contínua em processos, ferramentas e configurações de segurança de endpoints;
vi) planejar e executar projetos, iniciativas e provas de conceito relacionados a soluções de segurança de estações, servidores e dispositivos móveis, avaliando desempenho, cobertura e aderência às necessidades da TRANSPETRO;
vii) prestar consultoria técnica e elaborar pareceres sobre temas relacionados à segurança de endpoints, incluindo análise de risco, aderência a políticas, impacto de mudanças e recomendações de mitigação;
viii) realizar avaliações de boas práticas e benchmarkings na área de segurança de endpoints, considerando referências de mercado, recomendações de fabricantes e normas aplicáveis.

5.3.1.2 Segurança de Rede

A CONTRATADA deverá atuar na área de segurança de redes de telecomunicações para redes de dados multimídia, incluindo os protocolos e elementos empregados, em um ou mais processos de Segurança da Informação, a critério da TRANSPETRO, observando, no mínimo, as seguintes atividades:

i) realizar a gestão de controles protetivos e da postura de Segurança da Informação em redes, incluindo firewalls, IPS/IDS, VPNs, proxies, segmentação de rede, NAC e demais componentes relevantes;
ii) apoiar o desenho, a evolução e a revisão da arquitetura de Segurança da Informação aplicada às redes de dados, considerando requisitos de desempenho, disponibilidade, segregação lógica e física e modelos como zero trust;
iii) atuar em atividades de threat hunting, detecção e tratamento de ameaças cibernéticas em redes, bem como em perícia digital, análise de malware e testes de invasão (pentest), de forma consultiva e integrada com as demais equipes (CSIRT, SOC, Purple Team);

iv) executar atividades operacionais e de tratamento de incidentes relacionados à segurança de redes, em coordenação com as áreas responsáveis;
v) atuar em escalações e demandas de maior complexidade e/ou severidade, apoiando a análise de causa raiz, definição de contramedidas e recuperação do ambiente;
vi) definir, revisar e manter atualizados processos e procedimentos relacionados à segurança de redes, incluindo padrões de configuração, gestão de mudanças, gestão de regras, revisões periódicas e resposta a incidentes;
vii) atuar na gestão e compartilhamento de conhecimento técnico em segurança de redes, promovendo documentação, treinamentos e disseminação de boas práticas;
viii) propor e executar atividades de melhoria contínua em processos, arquiteturas, controles e ferramentas de segurança de redes;
ix) planejar e executar projetos, iniciativas e provas de conceito em Segurança de Redes, incluindo avaliação de novas tecnologias, substituição de componentes e evolução arquitetural;
x) prestar consultoria técnica e elaborar pareceres sobre temas relacionados à segurança de redes, inclusive para projetos de negócio e de infraestrutura;
xi) realizar avaliações de boas práticas e benchmarkings em segurança de redes, com base em normas, frameworks e referências de mercado, propondo adequações à realidade da TRANSPETRO.

5.3.2 Indicadores de Segurança de Ambientes

A CONTRATADA deverá criar e manter dashboards e relatórios integrados às bases de dados de segurança da TRANSPETRO, contendo, no mínimo, os seguintes indicadores relacionados às atividades de segurança de ambientes:

i) cobertura de monitoração de ativos: percentual de ativos (nuvem, corporativos e industriais) efetivamente monitorados pelas soluções de segurança em relação ao total de ativos inventariados, por tipo de ambiente e tecnologia;
ii) aderência à baseline de segurança: percentual de serviços SaaS, workloads em nuvem, ambientes industriais e dispositivos (endpoints e rede) em conformidade com a baseline de segurança definida pela TRANSPETRO;
iii) número de desvios de configuração (drifts) detectados: quantidade de desconformidades em relação aos padrões e arquiteturas de segurança aprovados, por ambiente (nuvem, corporativo, industrial) e por tecnologia;
iv) tempo médio de entrega de pareceres técnicos: tempo médio entre a solicitação de parecer/análise de risco de segurança e a entrega do parecer técnico ou recomendação formal ao demandante;
v) tempo médio de implementação de controles recomendados: tempo médio para implementação dos principais controles/mitigações recomendados pela segurança de ambientes (quando sob responsabilidade da CONTRATADA ou com sua coordenação);
vi) quantidade de projetos, iniciativas e PoCs avaliados pela segurança de ambientes: número de projetos de negócio, iniciativas de TI/OT e provas de conceito de segurança analisados no período, com indicação de quantos receberam recomendações de ajuste de segurança;
vii) índice de recomendações acatadas: percentual de recomendações de segurança emitidas pela segurança de ambientes que foram efetivamente acatadas e implementadas pelas áreas responsáveis, por criticidade;
viii) maturidade de segurança por domínio: classificação periódica (por exemplo, em níveis ou score) da maturidade de segurança em domínios como nuvem, industrial/OT, endpoints e redes, com base em frameworks de mercado (por exemplo, NIST-CSF, ISA/IEC 62443, ISO/IEC 27001), com registro da evolução ao longo do tempo;
ix) quantidade de incidentes suportados pelo SOC: número de incidentes de Segurança da Informação em que o SOC atuou (de forma consultiva ou operacional), por tipo de ambiente e por severidade;
x) tempo médio de resposta a incidentes suportados (MTTR-SOC): tempo médio entre o acionamento do SOC e a entrega da análise técnica ou recomendação de ação para contenção/mitigação;
xi) volume de mudanças avaliadas sob o ponto de vista de segurança: número de mudanças de infraestrutura, rede, nuvem, endpoints ou serviços avaliadas e aprovadas sob o prisma de segurança no período;
xii) indicadores de gestão do conhecimento:
a) número de documentos técnicos, playbooks, padrões e arquiteturas de segurança produzidos ou atualizados;
b) quantidade de treinamentos, workshops ou sessões de compartilhamento de conhecimento realizadas

pela segurança de amabientes;
xiii) aderência a metodologias ágeis: percentual de sprints (ou ciclos de trabalho) com entregas concluídas dentro do planejado, quando aplicável o uso de Scrum/Kanban nas atividades da segurança de amabientes;
xiv) benchmarking e conformidade com boas práticas: registro periódico de avaliações comparativas (internas/externas) e grau de aderência às principais normas, frameworks e referências adotadas (por exemplo, ISA-IEC 62443, NIST 800-82, NIST-CSF, NERC-CIP, ISO/IEC 27001), com indicação de evolução ao longo do tempo.
A CONTRATADA deverá assegurar que os indicadores acima sejam apresentados, no mínimo, em formato de relatório executivo e dashboards dinâmicos, com periodicidade a ser definida pela TRANSPETRO, permitindo o acompanhamento da evolução da maturidade de segurança, a identificação de tendências e o suporte à tomada de decisão pelas áreas de governança e gestão de riscos.

5.4 CYBER THREAT INTELLIGENCE (CTI)

A CONTRATADA deverá prover serviços especializados, com uso de ferramentas e métodos próprios, nas disciplinas de Detecção de Ameaças Cibernéticas, Threat Intelligence e Threat Hunting, atuando de forma integrada com as demais capacidades de Segurança da Informação da TRANSPETRO, observando, no mínimo, as responsabilidades descritas a seguir:

5.4.1 Detecção de Ameaças Cibernéticas

A CONTRATADA deverá:

i) gerenciar casos de uso de detecção de ameaças ao longo de todo o seu ciclo de vida, incluindo modelagem, priorização, implementação, teste, homologação e aprimoramento contínuo de regras no SIEM e em outras ferramentas de segurança utilizadas pela TRANSPETRO;
ii) avaliar continuamente quais eventos, logs e telemetrias são necessários para a criação e evolução dos casos de uso, colaborando com as equipes da TRANSPETRO para garantir a adequada coleta, retenção e qualidade desses dados;
iii) apoiar a criação, revisão e manutenção de procedimentos operacionais e playbooks para o tratamento de incidentes gerados pelas regras de detecção, garantindo alinhamento com o CSIRT/SOC;
iv) ajustar e otimizar regras de detecção existentes, com foco em aumento da eficácia contra ameaças relevantes, redução de falsos positivos, melhoria da eficiência operacional e ampliação da cobertura de riscos;
v) documentar todas as modificações, criações e exclusões de casos de uso e regras de correlação no SIEM e em outras plataformas de segurança, mantendo trilhas de auditoria e garantindo rastreabilidade das mudanças;
vi) assegurar que as capacidades de detecção estejam alinhadas às ameaças mais relevantes ao negócio da TRANSPETRO, ao cenário de ameaças global e às boas práticas de mercado.

5.4.2 Threat Intelligence

A CONTRATADA deverá:

i) interagir com fornecedores e fontes de Threat Intelligence para garantir que as informações recebidas sejam relevantes, atualizadas e utilizáveis, contribuindo efetivamente para melhoria das atividades de detecção, contenção e erradicação de incidentes, bem como para identificação e correção de vulnerabilidades;
ii) receber e buscar proativamente informações de segurança, incluindo alertas públicos e privados, relatórios de ameaças, advisories de fabricantes e informações de comunidades especializadas, gerindo feeds automáticos para bloqueio de atividades maliciosas, de forma a otimizar o uso dos recursos de segurança;
iii) utilizar ferramentas de terceiros fornecidas pela TRANSPETRO (incluindo, mas não se limitando a, plataformas MISP e outras soluções de inteligência) para coletar, correlacionar e analisar dados de inteligência de ameaças, mantendo base de conhecimento atualizada sobre ameaças, campanhas e ataques relevantes ao contexto da TRANSPETRO;
iv) prospectar e monitorar novas técnicas, ferramentas de intrusão, campanhas e tendências emergentes, apoiando a identificação e mitigação de futuras ameaças e alimentando continuamente os casos de uso

de detecção;
v) analisar artefatos maliciosos (como malware, scripts, anexos suspeitos, URLs, etc.), compreendendo seus mecanismos de propagação, objetivos e impactos potenciais, de forma a aprimorar ações de detecção, bloqueio, remoção e defesa;
vi) gerar relatórios de inteligência sobre ameaças e ataques, incluindo, quando aplicável, análise de motivações e intenções de atacantes, bem como das táticas, técnicas e procedimentos (TTPs) utilizados, em alinhamento com padrões como MITRE ATT&CK;
vii) identificar lacunas de segurança a partir das informações de inteligência, fornecendo recomendações de mitigação e melhoria de controles, incluindo o reporte estruturado das fases de ataques cibernéticos (cyber kill chain);
viii) validar e encaminhar Indicadores de Comprometimento (IoCs) para bloqueio ou monitoração, utilizando, entre outras, a plataforma MISP, bem como outras soluções de segurança empregadas pela TRANSPETRO;
ix) realizar pesquisas de OSINT (Open Source Intelligence) para identificar potenciais ameaças, exposições indevidas, dados vazados ou superfícies de ataque relacionadas à TRANSPETRO;
x) extrair informações de inteligência de honeypots e de logs de outras ferramentas de defesa, utilizando esses dados para aprimorar continuamente as capacidades de detecção, resposta e endurecimento do ambiente.

5.4.3 Threat Hunting

A CONTRATADA deverá:

i) conduzir atividades proativas de Threat Hunting para identificar ameaças desconhecidas ou não detectadas automaticamente no ambiente da TRANSPETRO, utilizando hipóteses de ataque, técnicas avançadas de análise, telemetria de múltiplas fontes (SIEM, EDR/XDR, logs de nuvem, etc.) e ferramentas especializadas;
ii) documentar os achados de Threat Hunting de forma estruturada, incluindo hipóteses, fontes de dados utilizadas, evidências encontradas, conclusões e recomendações, fornecendo relatórios detalhados à equipe de segurança da TRANSPETRO;
iii) colaborar com as equipes de segurança (SOC, CSIRT, Forense, Vulnerabilidades, DevSecOps, etc.) na investigação e mitigação das ameaças identificadas, assegurando resposta coordenada, tempestiva e eficaz;
iv) realizar análises de comportamento de usuários, sistemas e aplicações, visando identificar anomalias indicativas de atividades maliciosas ou suspeitas, contribuindo para detecção precoce de ameaças e ajuste de casos de uso;
v) fornecer recomendações de melhoria das defesas da TRANSPETRO com base nos resultados das atividades de Threat Hunting, incluindo ajustes em regras de detecção, controles de acesso, segmentação, postura em nuvem, políticas de segurança e processos;
vi) garantir que as atividades de Threat Hunting sejam integradas e sinérgicas com os demais processos de segurança cibernética da TRANSPETRO (gestão de vulnerabilidades, resposta a incidentes, SIEM/SOC, Forense Digital, etc.), promovendo ciclo de melhoria contínua;
vii) registrar, em repositório oficial definido pela TRANSPETRO, todos os casos de Threat Hunting realizados, com indicadores mínimos (hipótese, escopo, tempo despendido, evidências relevantes, status, recomendações implementadas), de forma a fortalecer a gestão do conhecimento e a evolução da maturidade de segurança.

5.4.4 Indicadores de CTI (Detecção, Threat Intelligence e Threat Hunting)

A CONTRATADA deverá criar e manter dashboards e relatórios integrados às atividades de CTI, contendo, no mínimo, os seguintes indicadores:

a) Indicadores de Detecção de Ameaças (Casos de Uso)

i) Quantidade de casos de uso ativos: número de casos de uso de detecção implantados e operacionais, por tipo de ameaça, tecnologia ou domínio (endpoint, rede, nuvem, identidade, etc.);
ii) Evolução de casos de uso: número de novos casos de uso criados, desativados e revisados em determinado período;
iii) Cobertura de ameaças prioritárias: percentual de ameaças consideradas críticas/prioritárias pela

TRANSPETRO que possuem casos de uso específicos de detecção;
iv) Efetividade por caso de uso: quantidade de alertas relevantes e de falsos positivos gerados por cada caso de uso, permitindo identificar os mais efetivos e os que requerem ajuste;
v) Tempo médio de atualização de casos de uso: tempo médio entre a identificação de uma nova técnica/tática relevante e a atualização ou criação de caso de uso correspondente.

b) Indicadores de Threat Intelligence

i) Relatórios de inteligência emitidos: número de relatórios/boletins de Threat Intelligence produzidos por período (semanais/mensais/especiais), por tema (campanhas, vulnerabilidades, setores, actors, etc.);
ii) IoCs processados: quantidade de Indicadores de Comprometimento (IoCs) recebidos, analisados e integrados às ferramentas de segurança (SIEM, EDR/XDR, firewalls, proxies, etc.) por período;
iii) Tempo médio de integração de IoCs: tempo médio entre o recebimento/validação de IoCs e sua efetiva aplicação em regras de bloqueio, monitoração ou correlação;
iv) Taxa de IoCs acionáveis: percentual de IoCs que geraram alertas ou contribuições efetivas em incidentes/caças a ameaças, em relação ao total de IoCs integrados;
v) Cobertura de fontes de inteligência: número e tipo de fontes de Threat Intelligence ativas (comerciais, comunitárias, setoriais, OSINT, MISP, etc.) e percentual de fontes efetivamente consumidas/correlacionadas;
vi) Correlação CTI → Detecção: quantidade de casos de uso, regras ou ajustes de detecção criados ou revisados com base direta em informações de Threat Intelligence;
vii) Campanhas e threat actors monitorados: número de campanhas, grupos de ameaça ou famílias de malware monitorados de forma contínua, com indicação dos mais relevantes para a TRANSPETRO.

c) Indicadores de Threat Hunting

i) Casos de Threat Hunting realizados: número de exercícios de threat hunting conduzidos por período, por tipo de hipótese (baseada em CTI, em anomalia, em incidente prévio, etc.);
ii) Casos com achados relevantes: percentual de atividades de hunting que resultaram em identificação de ameaça real, comportamento suspeito ou fragilidade relevante;
iii) Tempo médio por exercício de hunting: tempo médio despendido em cada exercício de threat hunting (planejamento, execução, análise e recomendações);
iv) Ações geradas a partir de hunting: quantidade de ações de correção, melhoria de controles, criação de novos casos de uso ou ajustes de regras de detecção derivadas de atividades de threat hunting, bem como percentual de ações implementadas;
v) Fontes de dados utilizadas: quantidade média de fontes de dados (SIEM, EDR/XDR, logs de nuvem, AD, proxies, etc.) utilizadas por exercício, indicando a ampliação da visão e da correlação;
vi) Integração hunting–CSIRT/SOC: número de incidentes formalmente abertos ou reclassificados a partir de achados de threat hunting;
vii) Evolução de hipóteses: percentual de hipóteses de hunting descartadas, confirmadas ou convertidas em casos de uso permanentes de detecção.

5.5 FERRAMENTAS NECESSÁRIAS

5.5.1 Licenças da CONTRATADA a serem utilizadas e instaladas no ambiente da TRANSPETRO:

Gestão de Vulnerabilidades (Tenable ou Qualys)
DevSecOps (Veracode, GitLab CI/CD, Trivy)
Claroty

5.5.2 Licenças que a TRANSPETRO possui:

Trend Vision One
Trend Deep Security (Virtual Patch)
Trend Apex One
Pacote de Ferramentas de Segurança do Microsoft Defender (SOC/CSIRT)
Pacote de Ferramentas do Microsoft Azure
SSE (Security Service Edge)

SASE (Security Access Service Edge)
Sentinel (SIEM/CSIRT)
Microsoft Endpoint Manager
Microsoft Purview

5.5.3 Os serviços deverão ser planejados pela CONTRATADA de acordo com a Tabela a seguir:

Item	Serviço	Automação	Corporativo	Navios
5.3.1.2	Segurança de Rede	300 Switchs	72 Firewalls 380 Roteadores 1160 Switches 700 Access points	30 Switches 114 Roteadores
5.2.1	SIEM	900 Servidores Windows 144 Servidores Linux 630 ativos sem serem servidores (PLC, remotas, switches industriais) 990 Workstations	6 Dominios 72 Firewalls 380 Roteadores 1150 Switches 700 Access points 12500 Workstations 720 Servidores Windows 220 Servidores Linux	30 Servidores Windows 30 Switches 114 Roteadores 315 Workstations
5.2.2.2	Tratamento de Incidentes	Baseado no quantitativo apresentado por serviço		
5.1.1	Gestão de Vulnerabilidades	900 Servidores Windows 144 Servidores Linux 630 ativos sem serem servidores (PLC, remotas, switches industriais) 990 Workstations	12500 Workstations 720 Servidores Windows 220 Servidores Linux 600 Impressoras 180 Aplicações 72 Firewalls 380 Roteadores 1160 Switches 700 Access points	30 Servidores Windows 30 Switches 114 Roteadores 315 Workstations
5.3.1	Segurança de Ambientes (Nuvem, Corporativo e Operacional)	100% On-premise 900 Servidores Windows 144 Servidores Linux 630 ativos sem serem servidores (PLC, remotas, switches industriais) 990 Endpoints EDR	90% Nuvem 16 Subscription Azure 10% On-premise 6 Dominios 12500 Workstations 720 Servidores Windows 220 Servidores Linux 72 Firewalls 380 Roteadores 1160 Switches 700 Access Points 2 WAFs	30 Servidores Windows 30 Switches 114 Roteadores 315 Workstations
5.3.1.1	Segurança de Endpoint	2034	13410	345
5.1.2	DevSecOps	N/A	60 Aplicações	N/A
5.1.3	Pentest	3 Aplicações	600 IPs (externo e interno) 200 Aplicações	N/A
5.4	Cyber Threat Intell (CTI)	6 Dominios 1 Marca 10000 Contas de Usuários		
5.2.2.1	Forense Digital	12 por Ano		

5.6 EQUIPE DE REFERÊNCIA

A CONTRATADA deverá ter uma equipe de profissionais exclusivos para somente executar as atividades de Assessment da Segurança da Informação e Segurança Cibernética.

5.7 INFRAESTRUTURA NECESSÁRIA PARA REALIZAÇÃO DOS SERVIÇOS

5.7.1. É de responsabilidade da CONTRATADA o fornecimento para os profissionais que atenderão a este contrato, de todo equipamento e infraestrutura (energia elétrica, equipamentos, internet, telefonia etc.) suficientes e adequados para a prestação do serviço.

5.7.2. Cabe à CONTRATADA disponibilizar uma equipe para atendimento 24 h/dia, 7 dias/semana, 365 dias/ano para acionamento de suporte em eventos de crise, em português, através de e-mail e telefone.

5.7.2.1. No início da prestação de serviço as PARTES informarão dados de contato para acionamento em emergência.

5.7.3. A CONTRATADA deve contar com ferramenta de gerenciamento de demandas para o registro das atividades relacionadas a este contrato desde o surgimento de cada uma delas até o seu encerramento, com o histórico de seu desenrolar.

5.7.4. A Fiscalização da TRANSPETRO não aceitará justificativas de atraso baseadas em problemas para os quais a TRANSPETRO não deu motivo, a exemplo de falhas ou inadequações de equipamentos de informática ou de rede/velocidade de internet.

5.7.5 Cabe à CONTRATADA o dimensionamento de sua rede de internet, a fim de garantir que o desenvolvimento das entregas não seja prejudicado.

6 CRITÉRIOS DE MEDIÇÃO

6.1. Somente serão medidos os produtos concluídos e aceitos pela TRANSPETRO.

6.2. A CONTRATADA emitirá mensalmente um Relatório Consolidado de Entregas, após o término do período a ser medido, com a relação dos produtos emitidos e aprovados pela TRANSPETRO, sendo estes anexados como evidência. Os produtos das entregas deverão, obrigatoriamente, conter todas as entregas de serviços que foram executados no período.

6.3. Caso os produtos não sejam concluídos no prazo de tolerância descrito no momento da solicitação do serviço, a TRANSPETRO postergará o prazo para conclusão do(s) serviço(s) para o mês subsequente, desde que haja razoabilidade na justificativa de atraso da CONTRATADA.

6.4. Os serviços a serem executados pela CONTRATADA serão solicitados por meio de ferramenta corporativa (e-mail) da TRANSPETRO, de modo que haja o devido registro das solicitações, bem como do andamento das atividades realizadas e dos produtos entregues e aceitos pelos demandantes. Poderão ser aceitos outros mecanismos de solicitação de serviços ou demandas, desde que sejam corporativos e possuam as devidas evidências e rastreabilidade. A TRANSPETRO, poderá alterar a ferramenta adotada ao longo do contrato motivada pela evolução sistêmica das ferramentas internas.

6.5 A CONTRATADA deverá disponibilizar 4 Coordenadores Técnicos, sendo um para cada frente: Purple Team, SIEM/CSIRT, SOC e CTI (Cyber Threat Intelligence), estes serão os pontos focais dos serviços contratados pela TRANSPETRO, sendo responsáveis por gerenciar as demandas, coordenar as equipes, acompanhar os incidentes, elaborar relatórios e planos de ação, e garantir a qualidade e a satisfação da TRANSPETRO. O Coordenador Técnico deverá ter formação superior em áreas relacionadas à tecnologia da informação, experiência comprovada em gestão de projetos de segurança da informação e certificações reconhecidas no mercado. O Coordenador Técnico deverá estar disponível em horário comercial, podendo ser acionado em emergências fora desse horário, conforme acordado entre as partes. O Coordenador Técnico deverá ter disponibilidade para visitas periódicas à sede da TRANSPETRO, bem como participar de reuniões e apresentações remotas.

6.6 Requisitos de Capacitação:

6.6.1 Os profissionais da equipe técnica da empresa, responsáveis pela sustentação da solução, deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos;

6.6.2 Os profissionais da equipe técnica da CONTRATADA, responsáveis pela detecção, notificação e investigação de ataques cibernéticos, deverão ter certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das certificações descritas na Tabela de Qualificação, contabilizando no máximo 2 (dois) certificados por profissional.

6.6.3 Os profissionais da equipe técnica da CONTRATADA, responsáveis pela resposta a ataques cibernéticos, deverão ter certificação em segurança defensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das certificações descritas na Tabela de Qualificação, contabilizando no máximo 2 (dois) certificados por profissional.

6.6.4 A CONTRATADA deverá fornecer profissionais com ampla experiência, especialização e capacitação, atendendo aos requisitos de formação acadêmica determinados, plenamente aptos a operar com excelência os sistemas e ferramentas da TRANSPETRO descritas neste contrato, com domínio das rotinas de trabalho, iniciativa, perfil proativo e direcionado para trabalho em equipe de alta produtividade nas atividades que irão desenvolver.

6.6.5 Tabela de Qualificação com as certificações necessárias por serviço:

Item	Serviço	Certificações	Qualificação
5.3.3	Segurança de Rede	CompTIA Security+ CompTIA Network+ CompTIA CySA+ OFFSEC OSDA: OffSec Defense Analyst Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	Nível superior completo em área de Tecnologia da Informação e áreas afins
5.2.1	SIEM	CompTIA Security+ CompTIA CYSA+ CyberDefenders CCD: Certified CyberDefender EC-Council Certified SOC Analyst (CSA) Microsoft SC-900 (Security, Compliance & Identity Fundamentals) Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	
5.2.2.2	Tratamento de Incidentes	CompTIA Security+ CompTIA CySA+ GIAC Certified Incident Handler (GCIH) GIAC Enterprise Incident Responder (GEIR) CyberDefenders CCD: Certified CyberDefender OFFSEC OSDA: OffSec Defense Analyst Certified Information Systems Security Professional (CISSP)	
5.1.1	Gestão de Vulnerabilidades	CompTIA Security+ EC-Council Certified Vulnerability Assessment Professional (CVAP+) Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	
5.3.1	Segurança de Ambientes (Nuvem, Corporativo e Operacional)	Security Operations Analyst Associate (SC-200) Arquiteto de Segurança Cibernética da Microsoft (SC-100) Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	
5.3.2	Segurança de Endpoint	CompTIA Security+ OFFSEC OSDA: OffSec Defense Analyst Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	
5.1.2	DevSecOps	CompTIA Security+ Certified DevSecOps Professional (CDP EC-Council Certified DevSecOps Engineer (ECDE) Certified Kubernetes Administrator (CKA)	
5.1.3	Pentest	Offensive Security Certified Professional (OSCP) Certified Ethical Hacker (CEH) Certified Red Team Expert (CRTE) Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	
5.4	Cyber Threat Intell (CTI)	EC-Council CTIA: Certified Threat Intelligence Analyst OFFSEC OSDA: OffSec Defense Analyst Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	
5.2.2.1	Forense Digital	GIAC GREM: Reverse Engineering Malware Certification Certificação EnCE (Encase Certified Examiner) Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	
6.6	Coordenador Técnico	COBIT ITIL ISO 27001 ISO 27002 Certificação Project Management Professional (PMP) Professional Scrum Master (PSM) Professional Scrum Product Owner (PSPO) Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)	

6.6.6 Cada item da Planilha de Preços Unitários (PPU) representará as quantidades estimadas de unidades de serviços a serem solicitados. Nos itens cuja unidade de medida seja Mês, o valor cobrado será fixo mensal, correspondendo ao limite máximo de ativos, já nos itens cuja unidade de medida seja UN, cada unidade representa a prestação de serviços em um ativo durante o período de um mês.

6.6.7 Na PPU, na linha 24 “P1 – Terminal” refere-se ao serviço que compreende atividades de segurança em equipamentos e rede OT, incluindo gestão contínua de vulnerabilidades, monitoramento integrado e proteção da rede, com foco em identificar movimentações suspeitas, comunicações anômalas e possíveis riscos operacionais nos terminais de automação, com o uso de recursos de proteção de sistemas ciberfísicos. O valor de cada unidade de medição representa a prestação de serviço em um terminal pelo período de um mês.

6.6.8 Para os serviços relacionados às linhas 2, 4, 5, 6, 7, 8, 16, 17, 18, 21, 22, 23 e 26 o preço corresponde ao valor mensal do serviço aplicado ao conjunto de recursos aplicáveis a cada um deles, conforme discriminados na tabela do item 5.5.3, acima.

6.6.9 Para os serviços relacionados às linhas 10, 11, 12, 14 e 19 o preço de cada unidade de medição representa o valor de cada execução completa dos serviços descritos.

7 CONTROLE DE QUALIDADE

O Indicador de Desempenho (ID) incidirá de forma igualitária sobre os itens de serviços da planilha de preços unitários de acordo com a fórmula a seguir. O valor de ID é obtido na tabela 1, de acordo com o valor do BAD gerado no mês de referência.

Vm = PU × ID

Onde:
Vm = Valor que remunerará cada item da Planilha de Preços Unitários;
PU = Valor estipulado na Planilha de Preços Unitários;
ID = Indicador de desempenho pelas notas do Boletim de Avaliação de Desempenho

(BAD) conforme tabela 1.

Tabela 1 - Indicador de Desempenho (ID)

Nota do BAD	Fator multiplicador da medição
100	1,00
De 90 à 99	0,90
De 80 à 89	0,80
De 70 à 79	0,70
De 60 à 69	0,60
De 50 à 59	0,50
De 40 à 49	0,40
De 30 à 39	0,30
De 20 à 29	0,20
De 10 à 19	0,10
De 1 à 09	0,05

8 SUBCONTRATAÇÃO

8.1. Nenhuma das atividades que compõem a execução dos serviços poderá ser subcontratada.

9 CONSIDERAÇÕES GERAIS

9.1 ORIENTAÇÕES PARA PRESTAÇÃO DOS SERVIÇOS

Em linhas gerais, espera-se que a CONTRATADA:

- Busque a excelência na gestão (de pessoas, de processos, de pesquisas e de tecnologias) da prestação dos serviços;
- Apresente-se como parceira estratégica nos negócios da SI e da TRANSPETRO;

- Preste serviços adequados às necessidades da SI e da TRANSPETRO;
- Aporte conhecimento e experiência nos assuntos relacionados à segurança da informação;
- Garanta o cumprimento das atividades estabelecidas pela TRANSPETRO;
- Demonstre flexibilidade e agilidade na realização dos serviços, procurando sempre a melhoria contínua;
- Auxilie na adoção de conceitos e tecnologias que possam trazer melhorias, sempre proporcionando ganhos de produtividade e de segurança, redução de custos, bem como o aperfeiçoamento dos modelos de gestão com a SI e a TRANSPETRO.

A CONTRATADA deverá indicar um empregado próprio para garantir a gestão sobre sua equipe de profissionais, e para representá-la sobre os serviços prestados à TRANSPETRO. O preposto não poderá fazer parte da equipe técnica. Este empregado será denominado Gestor de Serviços.

Os serviços previstos neste Contrato serão solicitados pela TRANSPETRO ao Gestor de Serviços da CONTRATADA.

Consideramos, para fins de aferição do prazo, que:

. HORAS ÚTEIS são contadas de segunda-feira à sexta-feira, exceto feriados, em um expediente de serviços totalizando (oito) horas úteis diárias, excluindo-se o intervalo com duração de hora para almoço. Por exemplo, este expediente poderia iniciar às 08:00 horas e terminar às 17:00 horas, ou então iniciar às 09:00 horas e terminar às 18:00 horas.

. DIAS ÚTEIS são contados de segunda-feira a sexta-feira, exceto feriados, totalizando (oito) horas úteis diárias, que sejam realizadas na faixa de horário entre 08:00 horas e 18:00 horas.

. HORAS CORRIDAS são contadas de uma segunda-feira até a próxima segunda-feira no calendário, incluindo feriados e finais de semana, considerando uma semana de (sete) dias corridos, em um expediente que inicia às 09:00 horas e termina às 18:00 horas, não havendo contabilização de intervalos.

. DIAS CORRIDOS são contados de uma segunda-feira até a próxima segunda-feira no calendário, incluindo feriados e finais de semana, considerando-se uma semana de (sete) dias corridos.

. Considera-se como EXPEDIENTE NORMAL DE SERVIÇOS o período de serviços que são realizados em DIAS ÚTEIS e em HORAS ÚTEIS.

Os prazos acordados entre a TRANSPETRO e a CONTRATADA serão sempre considerados em DIAS CORRIDOS, tendo em vista o calendário da cidade do Rio de Janeiro.

Os serviços deverão ser executados pela CONTRATADA seguindo as normas, padrões, procedimentos e metodologias da TRANSPETRO, e as instruções de trabalho elaboradas e emanadas pela equipe de gestão do Contrato da TRANSPETRO.

A CONTRATADA obriga-se a cumprir e fazer com que o seu pessoal cumpra as normas e exigências de segurança da informação da TRANSPETRO.

A CONTRATADA deverá fornecer informações necessárias ao perfeito entendimento dos serviços executados no meio e prazos fixados pela TRANSPETRO.

Para a execução dos serviços a CONTRATADA deverá utilizar os sistemas de informações e correio eletrônico que lhe forem indicados e disponibilizados, dentro das regras e limitações que forem estabelecidas pela TRANSPETRO.

Os sistemas de informação e o correio eletrônico da TRANSPETRO que forem disponibilizados para a CONTRATADA são considerados como meios formais de comunicação entre as partes para o que estiver relacionado à execução dos serviços, desde o início da demanda até a aceitação de entrega.

As datas e os registros de horários registrados nos sistemas de informações e correios eletrônicos da TRANSPETRO são aceitos como de fé inquestionável para a execução dos serviços.

Os problemas identificados pela CONTRATADA durante a prestação dos serviços deverão ser tempestivamente comunicados à TRANSPETRO.

A CONTRATADA deverá prover todo o suporte técnico e administrativo para que os serviços possam ser realizados com qualidade e pleno atendimento às demandas da TRANSPETRO.

Os resultados disponíveis sobre os serviços prestados pela CONTRATADA serão avaliados pela equipe de Gestão do Contrato da TRANSPETRO durante o processo de medição e servirão de base para a avaliação da CONTRATADA através do Índice de Desempenho dos Fornecedores no SAP TRANSPETRO, assim como para elaboração do Relatório de Medição do Contrato - RM.

Os serviços serão realizados conforme necessidades da TRANSPETRO, não existindo uma quantidade mínima de serviços a serem realizados em qualquer período durante a execução do Contrato.

A priorização das atividades será realizada pela equipe de Gestão do Contrato da TRANSPETRO, junto ao Gestor de Serviços da CONTRATADA.

Fica assegurado à TRANSPETRO o direito de, no decorrer da execução dos serviços, efetuar inspeções na equipe e infraestrutura da CONTRATADA para verificar a adequação necessária à execução dos serviços e da qualificação do pessoal, bem como promover diligências destinadas a avaliar a capacidade operacional da CONTRATADA para atendimento das condições de prestação dos serviços.

. O relatório oriundo dessa inspeção será discutido com a CONTRATADA e, caso haja necessidade, um plano de ação será proposto pela CONTRATADA para acertar qualquer não conformidade observada. Este relatório também será usado como subsídio para elaboração da avaliação periódica de desempenho da CONTRATADA.

. Os casos não previstos nessa ESPECIFICAÇÃO DE SERVIÇOS deverão ser esclarecidos pela CONTRATADA junto à equipe de Gestão do Contrato da TRANSPETRO. E, caso necessário, a Gestão do Contrato tomará as ações pertinentes para a adequada prestação dos serviços do Contrato.

9.2. A CONTRATADA deverá desenvolver os serviços utilizando profissionais devidamente qualificados e com experiência na atividade a ser executada, sobre as quais assumirá toda e qualquer responsabilidade, sob pena de ter a medição impactada por não cumprimento dos prazos das entregas previstas, ou qualidade insatisfatória na entrega dos serviços, conforme previsto no item 7 - CONTROLE DE QUALIDADE.

9.2.1. A CONTRATADA deverá fornecer, para todos os serviços a serem executados, profissionais com ampla experiência, especialização e capacitação, plenamente aptos a operar com excelência os sistemas e ferramentas da TRANSPETRO descritas nesta ET, com domínio das rotinas de trabalho, iniciativa, perfil proativo e direcionado para trabalho em equipe e alta produtividade nas atividades que irão desenvolver.

9.2.2. É de exclusiva responsabilidade da CONTRATADA a seleção, admissão, gerência de seu pessoal, treinamento, deslocamento de pessoal, equipamento e/ou materiais e demais despesas que vierem a ser necessárias para a QUALIFICAÇÃO PROFISSIONAL de seu pessoal, além da definição da remuneração de qualquer membro de sua equipe.

9.3 MOBILIZAÇÃO E DESMOBILIZAÇÃO

A CONTRATADA terá o prazo de 30 (trinta) dias, contados a partir da data de início da prestação dos serviços definida na Autorização de Serviço (AS), para realizar a implantação de sistemas e demais providências necessárias à execução das atividades previstas. Esse período inclui todas as providências técnicas, operacionais, logísticas e administrativas indispensáveis para que a CONTRATADA esteja plenamente apta a executar, de forma contínua e eficaz, todas as atividades descritas no Item 5 – Descrição das Atividades/Entregas desta Especificação Técnica.

Para fins de remuneração da mobilização inicial, o percentual máximo aplicável não poderá exceder 2,5% (dois vírgula cinco por cento) do valor total do contrato, contemplando todas as despesas, custos e investimentos necessários à execução das atividades de implantação e preparação para o início da prestação dos serviços.