

ANEXO I – TERMO DE REFERÊNCIA

GERÊNCIA REQUISITANTE: Divisão da Tecnologia da Informação

SOLICITAÇÃO DE COMPRAS: Nº 07/2026

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 – Contratação de empresa especializada em Segurança da Informação para execução de serviços técnicos de Auditoria Externa de Segurança, Teste de Intrusão (Pentest) do tipo Black Box e análise de vulnerabilidades no perímetro externo, serviços publicados, aplicações web e demais ativos diretamente expostos à Internet, contemplando 05 (cinco) endereços IP externos previamente autorizados pela CONTRATANTE, com elaboração de relatórios e recomendações técnicas para correção das vulnerabilidades identificadas.

1.2 – Os serviços objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3 – O prazo de vigência da contratação é de 12 meses, contados a partir da assinatura do contrato, na forma do artigo 105, da Lei nº 14.133 de 2021.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 – A fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1 – A descrição da solução como um todo se encontra pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

4.1 – SUBCONTRATAÇÃO

4.1.1 - Os serviços objeto desta licitação poderão ser executados diretamente pela contratada, por meio de profissionais integrantes de sua equipe técnica, de profissionais por ela contratados (inclusive com vínculo de prestação de serviços como pessoa jurídica), ou ainda, de forma parcial, por meio de subcontratação mediante prévia e expressa autorização desta autarquia. Em qualquer das hipóteses, permanecerá a contratada com a responsabilidade integral e exclusiva pela execução, qualidade, segurança, confidencialidade e pelo cumprimento de todas as obrigações previstas no contrato.

4.2 – GARANTIA DA CONTRATAÇÃO

4.2.1 – Não haverá exigência da garantia da contratação, conforme art. 96 e seguintes da Lei nº 14.133 de 2021, pelas razões constantes do Estudo Técnico Preliminar

4.3 – VISTORIA

4.3.1 – Não há necessidade de realização de avaliação prévia do local de execução dos serviços

4.4 – PARTICIPAÇÃO EXCLUSIVA DE ME/EPP

4.4.1 - A presente contratação será destinada exclusivamente à participação de microempresas e empresas de pequeno porte, nos termos do art. 48, inciso I, da Lei Complementar nº 123/2006, considerando que o valor estimado do objeto é de R\$ 46.000,00.

A execução dos serviços ocorrerá de forma remota, não sendo exigida prestação presencial ou estabelecimento da contratada na região do DAAE.

A participação exclusiva não afasta a exigência de comprovação da qualificação técnica, certificações profissionais, experiência, capacidade operacional e demais requisitos previstos neste Termo de Referência e no edital.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1 – CONDIÇÕES DE EXECUÇÃO

5.1.1 – A execução do objeto seguirá a seguinte dinâmica:

5.1.1.1 – A CONTRATADA terá o prazo de até 15 (quinze) dias úteis, contado da assinatura do contrato, para mobilização e preparação do início dos serviços.

As atividades principais deverão ser concluídas em até 90 (noventa) dias úteis, contados do início efetivo da execução, após a mobilização, a disponibilização das informações necessárias e a emissão das autorizações pertinentes.

O reteste deverá ser solicitado pela CONTRATANTE em até 180 (cento e oitenta) dias após a entrega do relatório do Pentest e será limitado à revalidação dos achados identificados na execução inicial, sem cobrança adicional.

A vigência contratual será de 12 (doze) meses, contados da assinatura do contrato.

5.1.1.2 – Descrição dos serviços

ESPECIFICAÇÕES GERAIS:

- O objeto deverá ser fornecido conforme especificações pactuadas, observando as disposições do Edital, da Proposta da Detentora, da Nota de Empenho ou outro documento equivalente.
- **Metodologia do Teste:** Black Box: Sem conhecimento prévio da infraestrutura.
- **Análise e Testes Realizados:**
 - Alvos Principais: Firewalls, serviços publicados, aplicações web e quaisquer ativos críticos diretamente expostos à internet.
 - Os testes ou atividades que possam ocasionar impacto nos serviços deverão, quando tecnicamente necessário, ser executados fora do horário comercial, mediante alinhamento e autorização prévia da CONTRATANTE, sem caracterizar alteração do escopo ou cobrança adicional quando estiverem compreendidos nas atividades previstas para o Pentest. O serviço será executado de forma remota.
 - Controles de segurança como firewall, WAF, IPS/IDS, CDN, anti-DDoS, rate limiting, bloqueios por reputação de IP, geoblocking, bot protection ou soluções equivalentes poderão permanecer ativos durante a execução, a fim de refletir o cenário real de exposição do ambiente. Caso tais controles impeçam completamente a execução dos testes autorizados ou bloqueiem de forma recorrente as atividades técnicas, o contratante deverá avaliar, sob sua responsabilidade,

a criação de exceções temporárias, allowlist dos IPs de origem da equipe executora ou ajuste controlado das políticas de segurança durante a janela previamente acordada.

- **Metodologia de execução:**

- Os serviços deverão ser executados utilizando metodologia reconhecida de mercado, compatível com o tipo de ativo avaliado e com a criticidade do ambiente, incluindo:

Penetration Testing Execution Standard — PTES.

OWASP Web Security Testing Guide — OWASP WSTG

OWASP API Security Top 10

NIST SP 800-115

OSSTMM

MITRE ATT&CK, quando aplicável à análise de cadeias de ataque e técnicas de exploração.

- A metodologia deverá combinar ferramentas automatizadas, validações manuais e análise técnica especializada. A simples execução de scanners de vulnerabilidade não será considerada suficiente para atendimento integral ao objeto.
- A Contratada deverá validar manualmente os achados classificados como críticos, altos ou que apresentem potencial impacto relevante ao negócio, desde que a validação possa ser executada de forma segura e dentro das regras de engajamento aprovadas.
- A classificação de risco deverá considerar a criticidade e o contexto técnico dos achados, incluindo, quando aplicável, probabilidade de exploração, exposição do ativo, impacto técnico e de negócio, existência de exploração conhecida e controles compensatórios. A pontuação CVSS poderá ser utilizada como referência técnica, sem constituir, isoladamente, o único critério de priorização.
- Reteste para validar as correções aplicadas, mediante solicitação da CONTRATANTE no prazo de até 180 (cento e oitenta) dias após a entrega do relatório do Pentest. O reteste estará incluído no escopo e no valor da contratação, sem cobrança adicional, desde que restrito à revalidação das vulnerabilidades identificadas no Pentest inicial.

- **Volumetria:**

- Teste dos IPs externos da Sede do DAAE e das Unidades Anhumas I, II e Paiol que comunicam através de VPNs e também do site www.daaeararaquara.com.br, conforme definição da CONTRATANTE. Total de endereços IP externos: 05 (cinco). www.daaeararaquara.com.br

- **Alvos do Pentest:**

- Firewalls, serviços publicados, aplicações web e quaisquer ativos críticos diretamente expostos à Internet e associados aos 05 (cinco) endereços IP externos previamente autorizados.

- **Entregáveis:**

- Relatório Técnico:
 - a) Descrição detalhada dos testes realizados
 - b) Identificação das vulnerabilidades encontradas
 - c) Evidências da exploração das vulnerabilidades
 - d) Avaliação detalhada dos impactos de cada vulnerabilidade.

- Relatório Executivo:

- a) Resumo dos principais resultados do Pentest
- b) Nível de risco das vulnerabilidades encontradas
- c) Recomendações priorizadas para correção das vulnerabilidades
- d) Plano de ação para mitigação das vulnerabilidades identificadas

Relatório Preliminar: Documento consolidado após o primeiro teste, contendo as atividades executadas, resultados obtidos, evidências técnicas, recomendações e próximos passos.

Relatório Específico de OSINT: Documento consolidando os resultados das atividades de reconhecimento e OSINT, contemplando, quando identificados, domínios, subdomínios, endereços IP, serviços, tecnologias, certificados digitais, informações DNS, documentos e repositórios expostos, credenciais ou informações corporativas expostas e demais informações relevantes.

Relatório de Reteste: Documento apresentando a comparação direta com o Pentest inicial e o status das correções implementadas, classificando as vulnerabilidades como corrigidas, parcialmente corrigidas ou não corrigidas, com as evidências pertinentes.

Documentação técnica: quando aplicável, poderão ser entregues scripts ou procedimentos utilizados na execução dos serviços, observados os limites de segurança e propriedade intelectual das ferramentas.

- **Validação Técnica:**

Na execução dos serviços, a CONTRATADA deverá utilizar ferramentas adequadas e dispor de profissionais capacitados e recursos técnicos suficientes para o atendimento do objeto, observadas as regras de engajamento, os limites do escopo e os requisitos de segurança estabelecidos neste Termo de Referência.

- **Certificações da equipe do projeto:**

A exigência de certificações profissionais relacionadas a testes de intrusão justifica-se pela natureza especializada do objeto, que envolve auditoria externa de segurança da informação, identificação e exploração controlada de vulnerabilidades, análise de aplicações e infraestrutura expostas à internet e elaboração de recomendações técnicas.

As certificações destinam-se a demonstrar que os profissionais indicados possuem formação prática compatível com a execução das atividades, não constituindo exigência de marca ou de certificação específica. Por essa razão, serão aceitas certificações equivalentes, desde que comprovem formação prática e conhecimentos compatíveis com testes de intrusão em aplicações e infraestrutura, em nível equivalente ao exigido para o objeto.

Considerar-se-á equivalente a certificação que:

- a) seja emitida por instituição reconhecida no mercado de segurança da informação;
- b) possua conteúdo predominantemente prático em testes de intrusão, análise de vulnerabilidades ou atividade técnica correlata;
- c) abranja, conforme o profissional indicado, testes em aplicações web, APIs, infraestrutura, redes ou ambientes expostos à internet; e
- d) apresente nível de complexidade compatível com as atividades previstas na contratação.

A comprovação da equivalência deverá ser acompanhada de documentação que permita verificar a instituição certificadora, o conteúdo, a modalidade da avaliação e a validade ou data de emissão da certificação.

A equipe responsável pela execução deve possuir profissionais com certificações reconhecidas no mercado, observando os seguintes critérios:

- a) **Certificação Principal (Obrigatória):** comprovação de ao menos 02 (duas) certificações práticas reconhecidas no mercado em Testes de Intrusão, de nível compatível com a complexidade do serviço, tais como OSCP, DCPT, CEH Practical, Solyd Certified Pentester, CAPT, Smart Recon ou equivalente.
- b) **Certificações Complementares e Especializações:** comprovação de capacitação técnica compatível com testes de intrusão em aplicações e infraestrutura, mediante certificações reconhecidas no mercado ou equivalentes, quando aplicável às atividades desempenhadas pela equipe.
- **Validade das Certificações:** As certificações e comprovações apresentadas devem estar válidas e/ou dentro do prazo de vigência na data de submissão da proposta.
- As certificações e os documentos comprobatórios deverão ser apresentados pelo licitante vencedor na fase de habilitação, após o julgamento das propostas e antes da adjudicação e homologação do certame.
- **Qualificação Técnico Operacional:**

A licitante deverá comprovar capacidade técnico-operacional mediante apresentação de atestado(s) emitido(s) por pessoa jurídica de direito público ou privado, que demonstre(m) a execução anterior de serviços compatíveis, em características e complexidade, com o objeto da contratação, abrangendo auditoria externa de segurança da informação, teste de intrusão — Pentest Black Box — e análise de vulnerabilidades em infraestrutura, serviços publicados ou aplicações web expostas à internet, isolada ou conjuntamente.

Será admitida a apresentação de um ou mais atestados, inclusive mediante somatório, desde que o conjunto comprove experiência compatível com o objeto.

Os atestados deverão identificar a contratante, o objeto, os serviços executados e o período de execução, admitida a solicitação de documentos complementares para comprovação de sua autenticidade.

Não será exigida comprovação de percentual mínimo do quantitativo do objeto.

O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do atestado, apresentando, quando solicitado pela administração, nota fiscal do serviço prestado, contatos do responsável, endereço atual da contratante e local em que foram prestados os serviços, entre outros documentos.

- **Cronograma:**
 - Após a assinatura do contrato, a CONTRATANTE poderá convocar a CONTRATADA para reunião inicial de alinhamento, devendo a mobilização para início das atividades ocorrer em até 15 (quinze) dias úteis. A reunião terá por objetivo alinhar escopo, objetivos, cronograma, responsáveis, regras de comunicação e demais pontos necessários à execução dos serviços.
 - O projeto será desenvolvido em três fases principais, sem prejuízo das atividades de reteste e encerramento descritas neste Termo de Referência:
 - a) **Fase de Planejamento:** Envolve a definição detalhada do escopo dos testes, identificação de ativos a serem avaliados e preparação das atividades necessárias para a execução do Pentest.

- b) **Execução do Pentest:** Consiste na realização dos testes de intrusão, coleta de dados, reconhecimento e identificação/validação de vulnerabilidades nos ativos e serviços externos definidos no escopo. A execução do Pentest deverá ocorrer em até 30 (trinta) dias úteis, contados do início efetivo dessa etapa. A conclusão de todas as atividades principais, incluindo os demais levantamentos, análises e entregáveis previstos no Termo de Referência, deverá ocorrer em até 90 (noventa) dias úteis, contados do início efetivo da execução contratual, após a mobilização e a disponibilização das informações e autorizações necessárias.
- c) **Análise e Relatórios:** Engloba a compilação dos dados obtidos, análise detalhada das vulnerabilidades encontradas e elaboração dos relatórios técnicos e executivos com as respectivas recomendações de mitigação.
- Todas as atividades principais descritas acima não poderão ultrapassar o prazo limite de 90 (noventa) dias úteis, a partir do início das atividades. O reteste será realizado posteriormente, mediante solicitação da CONTRATANTE e dentro do prazo máximo de 180 (cento e oitenta) dias após a entrega do relatório do Pentest.

ESPECIFICAÇÕES TÉCNICAS

O escopo técnico desta contratação está limitado à execução remota de Pentest Black Box no perímetro externo, abrangendo 05 (cinco) endereços IP externos previamente autorizados e os serviços diretamente expostos por esses ativos.

ITEM	DESCRIÇÃO
1	PENTEST (CYBERSECURITY)

Cronograma	
Etapa	Descrição / Requisito Mínimo
1. Kick-off	A CONTRATADA deverá realizar reunião inicial de alinhamento com a CONTRATANTE para definição do escopo, objetivos, cronograma, responsáveis, regras de comunicação e coleta das informações necessárias para execução dos serviços, garantindo um plano de trabalho personalizado e aderente ao ambiente.
2. Preparação do Ambiente	A CONTRATADA deverá disponibilizar e configurar todas as ferramentas, infraestrutura e recursos técnicos necessários à execução dos testes de segurança, incluindo estações de trabalho, ferramentas especializadas e ambiente dedicado, garantindo precisão, rastreabilidade e continuidade das atividades sem impacto ao ambiente da CONTRATANTE.

3. Coleta de Informações (Reconhecimento / OSINT)	A CONTRATADA deverá executar atividades de reconhecimento utilizando técnicas de OSINT (Open Source Intelligence), identificando informações publicamente acessíveis, ativos expostos, domínios, endereços IP, serviços, credenciais eventualmente vazadas e demais informações relevantes para avaliação da superfície de ataque da organização.
4. Scans de Vulnerabilidades	A CONTRATADA deverá realizar varreduras automatizadas e manuais nos ativos externos definidos no escopo, abrangendo os 05 (cinco) endereços IP externos e os serviços diretamente expostos por esses ativos, com o objetivo de identificar vulnerabilidades, serviços expostos, falhas de configuração, softwares desatualizados e demais riscos de segurança aplicáveis ao ambiente avaliado.
5. Análise Técnica e Validação dos Achados	A CONTRATADA deverá validar tecnicamente todas as vulnerabilidades identificadas, eliminando falsos positivos e classificando os riscos conforme sua criticidade. Caso sejam identificadas vulnerabilidades críticas que representem risco iminente ao ambiente, a CONTRATANTE deverá ser comunicada imediatamente para adoção das medidas cabíveis.
6. Testes de Exploração (Penetration Testing)	A CONTRATADA deverá realizar testes controlados de exploração das vulnerabilidades identificadas, utilizando técnicas e ferramentas especializadas, com o objetivo de comprovar a viabilidade de exploração, mensurar o impacto real das falhas e produzir evidências técnicas das vulnerabilidades exploráveis.
7. Testes de Aplicações Web (OWASP)	Quando houver aplicações web no escopo, a CONTRATADA deverá executar testes de segurança baseados, no mínimo, no OWASP Top 10 vigente, contemplando vulnerabilidades como SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Broken Access Control, Server-Side Request Forgery (SSRF), entre outras aplicáveis ao ambiente.
8. Revisão Técnica dos Resultados	A CONTRATADA deverá realizar análise consolidada dos resultados obtidos, correlacionando vulnerabilidades, impactos, probabilidade de exploração e riscos ao negócio, definindo a criticidade de cada achado e as respectivas recomendações técnicas de remediação.

DETALHAMENTO DO SERVIÇO:

O serviço objeto deste edital consiste na execução de Teste de Intrusão Externo do tipo Black Box, realizado de forma 100% remota, com foco no perímetro tecnológico exposto à Internet. O objetivo principal é avaliar a resiliência dos ativos críticos, reproduzindo, de forma controlada, metódica e não destrutiva, as táticas, técnicas e procedimentos (TTPs) empregados por agentes maliciosos no mundo real, limitado aos 05 (cinco) endereços IP externos e aos serviços diretamente expostos por esses ativos.

Para assegurar a fidelidade da simulação, a avaliação deverá ser conduzida sem conhecimento interno prévio do ambiente corporativo da CONTRATANTE, baseando-se em frameworks e metodologias reconhecidas internacionalmente, tais como PTES (Penetration Testing Execution Standard), NIST SP 800-115, OWASP WSTG, OWASP API Security Top 10, OSSTMM e MITRE ATT&CK, conforme aplicabilidade ao escopo.

Premissas e Regras de Engajamento

A CONTRATADA atuará com nível mínimo de informação inicial, não sendo fornecidos diagramas de rede, inventário de ativos, credenciais, códigos-fonte ou qualquer documentação que reduza artificialmente a complexidade do teste.

O fornecimento de informações adicionais ocorrerá apenas em caráter excepcional, mediante justificativa formal da CONTRATADA e aprovação da CONTRATANTE, visando a continuidade segura dos testes ou a validação de impactos muito específicos.

Os testes deverão ser realizados de forma estritamente controlada e proporcional ao ambiente avaliado, sendo proibidas ações que provoquem indisponibilidade, como ataques de Negação de Serviço (DoS/DDoS), degradação intencional de desempenho, corrupção de dados ou impacto operacional sistêmico.

A CONTRATADA deverá manter canal de comunicação direto e seguro com a equipe técnica da CONTRATANTE para reporte imediato caso identifique vulnerabilidades críticas com risco iminente de exploração ou indícios de comprometimento prévio do ambiente por terceiros.

Fase de Inteligência e Reconhecimento (OSINT)

A etapa inicial deverá focar na coleta e análise de informações públicas para mapear a superfície de ataque e compreender o ecossistema de negócio da organização, servindo de insumo para os vetores de ataque.

Executar atividades de reconhecimento em fontes públicas e abertas (OSINT) para identificar vazamentos de dados, credenciais corporativas eventualmente expostas, repositórios públicos, documentos expostos e demais informações relevantes para avaliação da superfície de ataque, sem realização de testes intrusivos em fontes que não façam parte do escopo autorizado.

O levantamento deve incluir a presença digital completa, englobando domínios, subdomínios, portais institucionais, ASNs, blocos IP associados, redes sociais corporativas e relações institucionais com clientes e fornecedores.

Realizar, quando aplicável, a identificação e correlação de informações publicamente acessíveis relacionadas ao ambiente avaliado, incluindo domínios, subdomínios, endereços IP, serviços, tecnologias, certificados digitais, informações DNS, documentos, repositórios e credenciais ou informações corporativas eventualmente expostas.

Correlacionar as informações obtidas com a superfície de ataque para identificar vetores exploráveis, documentando a origem, a relevância da exposição e o impacto potencial para a continuidade do teste.

A CONTRATADA deverá empregar ferramentas adequadas, atualizadas e compatíveis com as atividades de identificação, análise e validação de vulnerabilidades, combinando automação, validações manuais e análise técnica especializada.

Poderão ser utilizadas ferramentas comerciais, de código aberto, comunitárias ou gratuitas, desde que sejam tecnicamente adequadas ao escopo e permitam a produção de evidências técnicas confiáveis, rastreáveis e auditáveis.

A CONTRATADA será responsável pela legalidade do uso das ferramentas, pela obtenção das licenças eventuais necessárias e segurança e integridade dos dados tratados durante a execução dos serviços.

a) As ferramentas utilizadas deverão ser adequadas à finalidade dos testes e mantidas em condições de uso durante a execução dos serviços, permitindo a obtenção de evidências técnicas suficientes para suportar os achados apresentados nos relatórios.

b) Os resultados automatizados deverão ser registrados e apresentados de forma rastreável, sempre que aplicável, juntamente com as evidências técnicas necessárias à validação dos achados e à compreensão das vulnerabilidades identificadas.

c) A atualização das ferramentas e respectivas bases de conhecimento deverá ser realizada de modo compatível com a execução dos testes e com as boas práticas de segurança da informação.

Não serão aceitos:

- ferramentas ou versões que comprometam a confiabilidade, a rastreabilidade, a segurança ou a completude dos resultados, independentemente do modelo de licenciamento;
- bases de vulnerabilidades desatualizadas;
- ferramentas cujo mecanismo de detecção seja baseado exclusivamente em fingerprinting, banners de serviços ou identificação superficial de versões de software;
- relatórios convertidos ou importados de outras ferramentas;
- utilização de múltiplos scanners com consolidação posterior dos resultados para simular a saída de uma única ferramenta;
- relatórios cuja origem dos resultados automatizados não possa ser comprovada mediante apresentação dos respectivos arquivos nativos da ferramenta utilizada.

A CONTRATANTE poderá solicitar, durante a execução ou até o aceite definitivo dos serviços, as evidências técnicas e registros necessários à validação dos resultados apresentados, observados os limites de confidencialidade, segurança da informação e propriedade das ferramentas utilizadas.

Mapeamento da Superfície e Infraestrutura

Esta fase exige a análise técnica ativa do perímetro descoberto, visando encontrar serviços desatualizados, portas abertas indevidamente e falhas de arquitetura, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Realizar o mapeamento abrangente de portas, serviços, banners, protocolos legados, interfaces administrativas de firewalls, VPNs e ambientes de homologação ou desenvolvimento esquecidos (shadow IT) expostos à Internet.

Avaliar a exposição indevida de infraestruturas em nuvem, incluindo buckets de armazenamento, serviços de mensageria, filas, bancos de dados, instâncias de computação e consoles de gerenciamento, considerando falhas de autenticação e credenciais padrão.

Analisar o nível de hardening do perímetro, identificando configurações inseguras em servidores web, proxies reversos, balanceadores de carga, WAFs, serviços de DNS (como zone transfers) e servidores de e-mail (falhas em SPF/DKIM/DMARC).

Avaliar a postura criptográfica dos serviços expostos, analisando versões e suítes TLS, cadeia de certificados, uso de algoritmos obsoletos, suscetibilidade a falhas conhecidas de implementação e ausência de cabeçalhos de segurança (HSTS).

Exploração de Vulnerabilidades Aplicacionais e de Rede

A exploração deve ser conduzida para comprovar o impacto real das falhas identificadas, sempre respeitando os limites operacionais e a perspectiva de um atacante externo não autenticado, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Testar exaustivamente a robustez dos fluxos de autenticação, englobando recuperação de conta, alteração de senhas, SSO, integrações de identidade e mecanismos de MFA, avaliando a resistência a técnicas de bypass, reutilização de tokens e ataques de MFA fatigue, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Avaliar a proteção de segredos em trânsito e em repouso, buscando senhas, chaves de API, JWTs e tokens de sessão expostos em URLs, logs, cabeçalhos HTTP, cache ou no código-fonte publicado (client-side), sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Executar testes de enumeração de contas e resistência a ataques de força bruta, password spraying e credential stuffing, burlando ou mapeando as respostas de mecanismos de bloqueio (rate limiting e WAFs) sem comprometer a disponibilidade de contas legítimas, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Identificar e explorar vulnerabilidades de injeção aplicáveis às tecnologias do ambiente, incluindo SQLi, NoSQLi, OS Command Injection, Server-Side Template Injection (SSTI), XPath Injection, XML e XXE, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Avaliar os mecanismos de sanitização e codificação de entradas, identificando falhas de Cross-Site Scripting (XSS Refletido, Armazenado e DOM) e falhas de processamento de entidades externas, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Testar a manipulação de parâmetros, identificadores (IDOR) e variáveis de negócio visando escalação de privilégios (vertical e horizontal) e ataques de mass assignment, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Identificar inconsistências avançadas de roteamento e interpretação de requisições HTTP, como HTTP Request Smuggling, Host Header Injection, Cache Poisoning e bypass de controles de borda (CDN/WAF), sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Validar vulnerabilidades em rotinas de upload de arquivos (bypass de MIME type, path traversal, execução remota de código) e analisar o comportamento de mensagens de erro detalhadas (stack traces) que vazem dados de infraestrutura, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Verificar vulnerabilidades em componentes compilados e de baixo nível (como buffer overflow, integer overflow e race conditions), exclusivamente quando aplicável ao contexto e dentro dos rigorosos limites de segurança operacional, sempre que aplicável aos ativos e serviços externos autorizados e dentro dos limites das regras de engajamento.

Exploração de Vulnerabilidades Avançadas

Além das vulnerabilidades anteriormente descritas, a CONTRATADA deverá realizar, quando aplicável às tecnologias, arquitetura e serviços identificados durante o reconhecimento e sempre dentro do escopo dos ativos externos autorizados, a exploração controlada de vulnerabilidades pertencentes aos seguintes grupos:

Segurança de APIs Modernas

Broken Object Level Authorization (BOLA)

Broken Function Level Authorization (BFLA)

Excessive Data Exposure
Unsafe Consumption of APIs
Avaliação de APIs REST, SOAP, GraphQL, gRPC e WebSockets.

Falhas Lógicas de Negócio

Business Logic Flaws
Bypass de fluxos transacionais
Manipulação de estados da aplicação
Validação inadequada de regras de negócio
Escalada indireta de privilégios decorrente de falhas funcionais.

Vulnerabilidades Server-Side

Server-Side Request Forgery (SSRF)
Insecure Deserialization
Local File Inclusion (LFI)
Remote File Inclusion (RFI)
Server-Side Includes (SSI), quando aplicável.

Segurança de Aplicações Modernas

Single Page Applications (SPA)
Manipulação de JavaScript Client-Side
CORS Misconfiguration
HTTP Parameter Pollution
Cache Deception
HTTP Request Splitting.

Segurança de Autenticação Federada

OAuth 2.0
OpenID Connect (OIDC)
SAML
Validação de Identity Providers (IdPs)
Avaliação da emissão, renovação e revogação de tokens.

Cadeias de Exploração

Sempre que tecnicamente viável e seguro, deverão ser identificadas e demonstradas cadeias de ataque (Attack Chaining), correlacionando múltiplas vulnerabilidades ou exposições que, exploradas em conjunto, possam resultar em comprometimento relevante do ambiente. As cadeias de exploração validadas deverão ser documentadas com evidências e contextualização de impacto nos relatórios do projeto.

Será necessária validação manual e controlada dos achados relevantes, com evidências que demonstrem o ativo afetado, pré-condições, vetor de exploração, impacto técnico, impacto de negócio, controles compensatórios e recomendação priorizada de remediação.

Reteste:

Realização de validações adicionais após a implementação das correções recomendadas, restritas às vulnerabilidades identificadas no Pentest inicial.

Validação do status das vulnerabilidades identificadas no Pentest inicial, classificando-as como corrigidas, parcialmente corrigidas ou não corrigidas, conforme evidenciado durante o reteste.

O reteste deverá ser solicitado no prazo de até 180 (cento e oitenta) dias após a entrega do relatório do Pentest e estará integralmente incluído no valor da contratação, sem cobrança adicional, desde que restrito à revalidação das vulnerabilidades identificadas no Pentest inicial.

Documentações e Materiais Disponibilizados

Relatório Preliminar

A CONTRATADA deverá entregar relatório preliminar após a execução do primeiro teste, contendo a consolidação inicial das atividades realizadas, dos resultados obtidos e das evidências técnicas coletadas durante a execução dos serviços.

O documento deverá apresentar, de forma clara e organizada, a descrição das atividades executadas, os ativos avaliados, a metodologia aplicada, os principais achados identificados, bem como eventuais vulnerabilidades, exposições, falhas de configuração ou pontos de atenção observados até o momento.

O relatório também deverá conter as evidências técnicas que sustentem os resultados apresentados, incluindo registros, capturas de tela, logs, saídas de ferramentas, referências técnicas ou demais comprovações pertinentes, sempre respeitando os limites de segurança e confidencialidade das informações.

Além disso, deverão ser apresentadas recomendações preliminares para tratamento dos achados identificados, priorização inicial das correções e indicação dos próximos passos necessários para continuidade dos testes, validações complementares, mitigação dos riscos ou preparação para o reteste, quando aplicável.

Relatório Específico de OSINT

A CONTRATADA deverá entregar relatório específico referente à etapa de OSINT — Open Source Intelligence, contendo os resultados obtidos por meio de fontes públicas e abertas, sem realização de testes intrusivos.

O relatório deverá apresentar, quando identificadas, informações relacionadas à CONTRATANTE, incluindo domínios, subdomínios, endereços IP, serviços expostos, tecnologias utilizadas, certificados digitais, registros DNS, documentos expostos, repositórios públicos, credenciais ou dados corporativos eventualmente expostos e demais informações relevantes obtidas durante o reconhecimento.

Nos casos de vazamentos de dados identificados em fontes públicas, deverão ser informados, quando disponíveis, a origem da exposição, data do vazamento ou da identificação, tipo de dado exposto, evidências, impacto potencial e criticidade, preservando-se informações sensíveis e observando-se os limites legais e de segurança aplicáveis.

Cada achado deverá conter descrição, origem da informação, evidência, risco associado e recomendação de mitigação, diferenciando informações confirmadas de indícios ou falsos positivos e preservando a segurança de dados sensíveis, especialmente senhas, tokens ou chaves, que deverão ser apresentados de forma mascarada.

Ao final, a CONTRATADA deverá apresentar resumo executivo dos principais riscos encontrados e recomendações priorizadas para redução da exposição pública da organização.

Relatório Final

A CONTRATADA deverá entregar relatório final consolidado ao término do projeto ou serviço, contemplando todas as atividades executadas durante a contratação, incluindo as etapas de planejamento, reconhecimento, testes, validações técnicas, análise dos resultados, recomendações de correção e reteste.

O documento deverá apresentar, de forma clara, organizada e rastreável, os resultados obtidos ao longo de toda a execução, demonstrando os achados identificados, ativos avaliados, vulnerabilidades confirmadas, impactos técnicos e riscos associados ao ambiente da CONTRATANTE.

O relatório deverá conter, no mínimo:

- Descrição das atividades executadas, incluindo o reteste;
- Resultados obtidos em cada etapa do serviço;
- Vulnerabilidades identificadas e respectiva classificação de criticidade;
- Evidências técnicas coletadas durante os testes e validações;
- Comparativo entre os achados iniciais e os resultados do reteste;
- Indicação das vulnerabilidades corrigidas, parcialmente corrigidas ou ainda pendentes;
- Recomendações finais de mitigação e melhoria da postura de segurança.

As evidências técnicas deverão incluir registros, capturas de tela, logs, saídas de ferramentas, provas de conceito controladas ou demais comprovações pertinentes, sempre observando os limites de confidencialidade, segurança da informação e integridade do ambiente avaliado.

Ao final, o relatório deverá apresentar conclusão técnica sobre o nível de risco residual após as validações realizadas, bem como recomendações priorizadas para tratamento das pendências remanescentes e fortalecimento da segurança do ambiente.

6. MODELO DE GESTÃO DO CONTRATO

6.1 - O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderão pelas consequências de sua inexecução total ou parcial.

6.2 - Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3 - As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim. É vedada a utilização de WhatsApp.

6.4 - O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5 - Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.6 – PREPOSTO

6.6.1 – O Contratado designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contrato.

6.6.2 – O Contratado *não necessitará* manter preposto da empresa no local da execução do objeto *durante o período de contratação*.

6.6.3 – O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que o Contratado designará outro para o exercício da atividade.

6.7 – DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

6.7.1 – A gestão e fiscalização do respectivo contrato serão realizadas pelos seguintes servidores:

. FISCAL DO CONTRATO: David Wilian Quitério – MATRÍCULA Nº 1378 – nomeado pela Divisão da Tecnologia da Informação

. GESTOR DO CONTRATO: Renildo Moreira de Almeida – MATRÍCULA Nº 1708 – Chefe da Divisão da Tecnologia da Informação

6.7.1.1 – No caso de ausência dos servidores designados no item acima, ficam designados os servidores como substitutos:

. FISCAL DO CONTRATO: Não há designação de fiscal substituto, pois não há mais pessoas elegíveis nesta divisão.

. GESTOR DO CONTRATO: Eduardo João Galati – MATRÍCULA Nº 1565 – Chefe de Setor da Divisão da Tecnologia da Informação.

6.7.2 – CABE AO FISCAL DO CONTRATO:

. Acompanhar a execução para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

. Anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

. Identificada qualquer inexecução ou irregularidade, o fiscal emitirá notificações para a correção da execução do contrato, determinando prazo para saná-la;

. Informar ao gestor, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor;

. Comunicar ao gestor, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

. Verificar a manutenção das condições de habilitação da contratada, acompanhar o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário;

. Caso ocorra descumprimento das obrigações contratuais, o fiscal atuará tempestivamente na solução do problema, reportando ao gestor para que tome as providências cabíveis, quando ultrapassar a sua competência;

6.7.3 – CABE AO GESTOR DO CONTRATO:

. Coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da Administração;

. Acompanhar os registros realizados pelo fiscal do contrato, de todas as ocorrências relacionadas à execução e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

- . Acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;
- . Emitir documento comprobatório da avaliação realizada pelo fiscal do contrato quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações;
- . Tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções previstas no artigo 156 inciso III e IV, da Lei nº 14.133, de 2021, e encaminhar o respectivo processo para a Unidade de Gestão de Contratos;
- . Elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração;
- . Enviar a documentação pertinente para o procedimento de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. PAGAMENTO

7.1 – Os preços incluem todas as taxas ou despesas adicionais, tais como transporte, carga, descarga de equipamentos, funcionários, e demais despesas. Qualquer item não mencionado será considerado como incluído nos preços propostos, sendo os valores expressos em Reais.

7.2 - Nos preços propostos deverão estar inclusos, além do lucro, todas as despesas e custos, como por exemplo: mão de obra especializada, materiais, equipamentos, encargos, leis sociais, BDI, transportes, tributos de qualquer natureza e todas as despesas, diretas ou indiretas, relacionadas com a prestação dos serviços, objeto desta licitação.

7.3. Os preços contratados poderão ser reajustados após o interregno mínimo de 12 (doze) meses, contado da data do orçamento estimado, mediante aplicação da variação acumulada do IPCA/IBGE, ou de outro índice que venha a substituí-lo.

7.4. O reajuste incidirá somente sobre os valores correspondentes ao período posterior ao implemento do interregno mínimo de 12 (doze) meses.

7.5. A data do orçamento estimado será aquela formalmente indicada na Planilha de Composição do Valor Estimado da Contratação e nos documentos que integram a pesquisa de preços.

7.6. Não se aplica ao contrato o regime de repactuação, por não se tratar de serviço com dedicação exclusiva ou predominância de mão de obra.

7.7 - A Nota Fiscal Eletrônica/Fatura deverá ser emitida em nome da Licitante Vencedora e acompanhar a execução do material, destacando em seu corpo o número de contrato/empenho, a modalidade licitatória e o número da licitação.

7.8 – A Nota Fiscal Eletrônica deverá ser encaminhada para os seguintes e-mails: gti@daaeararaquara.com.br / nfe@daaeararaquara.com.br.

7.9 - Também vinculada à fatura, a licitante vencedora deverá destacar no corpo da Nota Fiscal as seguintes retenções: **ISSQN, INSS e IRPJ**, quando estas forem obrigatórias. Em caso negativo, a licitante vencedora deverá apresentar declaração formal de que é beneficiária de tais isenções.

7.10 – Os pagamentos serão efetuados no 5º (quinto) dia útil após a aprovação da Nota Fiscal/Fatura pelo Ordenador de Despesas.

7.11 – O pagamento será efetuado mediante crédito em conta corrente, devendo a licitante vencedora informar o número do banco, da agência e da conta bancária, ou através de banco credenciado.

7.12 – Correrão por conta da CONTRATADA todas as despesas relativas à execução do presente Contrato, cabendo ao CONTRATANTE exclusivamente o pagamento da importância contratada.

7.13 – No caso de atraso no pagamento, por culpa exclusiva da contratante, sendo este superior a 30 (trinta) dias, o valor devido será corrigido com base na variação do IPCA/IBGE.

7.14 – A CONTRATADA terá o prazo de até 15 (quinze) dias úteis, contado da assinatura do contrato, para mobilização e preparação do início dos serviços.

As atividades principais deverão ser concluídas em até 90 (noventa) dias úteis, contados do início efetivo da execução, após a mobilização, a disponibilização das informações necessárias e a emissão das autorizações pertinentes.

O reteste deverá ser solicitado pela CONTRATANTE em até 180 (cento e oitenta) dias após a entrega do relatório do Pentest e será limitado à revalidação dos achados identificados na execução inicial, sem cobrança adicional.

A vigência contratual será de 12 (doze) meses, contados da assinatura do contrato.

O pagamento será realizado em duas parcelas:

- a) 50% do valor contratual após a entrega e aprovação dos relatórios iniciais previstos no Termo de Referência;
- b) 50% do valor contratual após a realização do reteste, quando solicitado pela CONTRATANTE no prazo contratual, e a entrega e aprovação do respectivo relatório.

Caso a CONTRATANTE não solicite o reteste no prazo de até 180 (cento e oitenta) dias após a entrega do relatório do Pentest, a segunda parcela será paga após o decurso desse prazo, desde que os demais entregáveis tenham sido aprovados.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

8.1 - Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.2 - Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

- a) Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;
- b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

c) Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

8.3 – Dos tipos de multa:

a) **MORATÓRIA:** Pelo atraso injustificado, a critério da Administração, na execução do contrato/ata, a multa será de 0,2% (dois décimos por cento) por dia até 30 (trinta) dias e 0,4% pelo que exceder a 30 dias até 60 (sessenta) dias, calculados sobre o valor do contrato/ata.

b) **COMPENSATÓRIA:** Pela inexecução total ou parcial do contrato/ata, a multa será de 10% (dez por cento) do valor correspondente à parte não cumprida do contrato/ata.

8.4 - A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

8.5 - Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

8.6 - Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.7 - Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será cobrada judicialmente.

8.8 - A multa poderá ser recolhida administrativamente no prazo máximo de 20 (vinte) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.9 - A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.9.1 - Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial.

8.9.2 - Os endereços de e-mail informados na proposta comercial serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

8.10 - Na aplicação das sanções serão considerados:

8.10.1 - a natureza e a gravidade da infração cometida;

8.10.2 - as peculiaridades do caso concreto;

8.10.3 - as circunstâncias agravantes ou atenuantes;

8.10.4 - os danos que dela provierem para o Contratante; e

8.10.5 - a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.11 - Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definido na referida Lei.

8.12 - A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para

provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.13 - O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade na relação de Apenados do Tribunal de Contas do Estado de São Paulo.

8.14 - As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

9.1 – O Fornecedor será selecionado por meio de realização de procedimento de LICITAÇÃO, com adoção do critério de julgamento pelo MENOR PREÇO.

9.2 - REGIME DE EXECUÇÃO

9.2.1 – O regime de execução do objeto será de empreitada por preço global.

9.3 – O valor estimado da presente contratação é de R\$ 46.000,00 (quarenta e seis mil reais).

10. DISPOSIÇÕES FINAIS

10.1 – As informações contidas neste Termo de Referência não são classificadas como sigilosas.

11. DOS ANEXOS

11.1 – ANEXO I – TERMO DE REFERÊNCIA

11.1.1 – Apêndice do Anexo I – Estudo Técnico Preliminar;

11.2 – Anexo II – Planilha de Composição de Preços;

11.3 – Anexo III – Planilha Estimativa de Preços;

11.4 – Anexo IV – Análise de Risco;

Demais anexos que a gerência achar necessário.

DEPARTAMENTO AUTÔNOMO DE ÁGUA E ESGOTOS DE ARARAQUARA, 27 DE AGOSTO DE 2026

David Wilian Quitério
Subdivisão de Desenvolvimento, Infraestr. e Suporte

Renildo Moreira de Almeida
Chefe da Divisão de Tecnologia da Informação