

ESTUDO TÉCNICO PRELIMINAR

Objeto: Contratação de empresa especializada em Segurança da Informação para execução de serviços técnicos abrangendo: Análise de Vulnerabilidades, Testes de Intrusão (Pentest) e auditoria de segurança em infraestrutura de rede, servidores e aplicações. A solução inclui a avaliação do perímetro externo e a elaboração de Plano de Remediação com recomendações técnicas para correção de falhas.

Araraquara, 22 de Junho 2026

Histórico de Revisões

Data	Versão	Descrição	Autor
22/06/2026	1.0	Finalização da primeira versão do documento	David Wilian Quitério
12/08/2026	2.0	Revisão do documento.	Renildo Moreira de Almeida

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

Trata-se de estudo de viabilidade para contratação de consultoria especializada para diagnóstico e fortalecimento da infraestrutura tecnológica. O escopo compreende testes de intrusão (Pentest) e análises de vulnerabilidade em redes e aplicações, visando a identificação de riscos e a entrega de um plano estratégico de remediação e correção de incidentes.

1. NECESSIDADE DA CONTRATAÇÃO

A infraestrutura de TI constitui o alicerce das operações institucionais. Vulnerabilidades não mapeadas em ativos de rede e firewalls representam riscos críticos de interrupção de serviços e vazamento de dados. Esta necessidade surge da urgência em validar a eficácia dos controles implementados após atualizações estruturais recentes, tais como a atualização do modelo de firewall e a migração das regras de acesso. O objetivo é antecipar-se a ameaças por meio da identificação proativa de brechas exploráveis, assegurando a resiliência operacional e a integridade do patrimônio informativo.

O Problema: Embora ferramentas de varredura automática identifiquem falhas conhecidas, elas são incapazes de simular a criatividade de um invasor real ou a combinação lógica de vulnerabilidades que podem levar ao comprometimento total do ambiente.

A Solução: A execução de Testes de Intrusão (Pentest) para validar a robustez dos controles atuais e fornecer um plano de remediação estratégico, priorizado por riscos reais de negócio.

Os bens e serviços são considerados:

“comuns” pois se enquadram-se na classificação nos termos do inciso XIII do artigo 6º da Lei Federal nº 14.133/2021 “aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado”.

2. REQUISITOS DA CONTRATAÇÃO

O objeto a ser licitado, pelas suas características e com bases nas justificativas acima mencionadas, NÃO POSSUI NATUREZA CONTINUADA.

Para que o presente serviço seja contratado e corretamente prestado existem requisitos mínimo para sua satisfação, tais como:

- Escopo: Teste dos IPs da Sede do DAAE e das Unidades Anhumas I, II e Paiol que comunicam através de VPNs e do site www.daaeararaquara.com.br.
- Metodologia: Utilização de frameworks reconhecidos (PTES, OWASP, OSSTMM ou NIST).
- Modalidade Black Box: Sem conhecimento prévio da infraestrutura.
- Janelas de Execução: Testes devem ser realizados em horário comercial (8x5) e não serão realizados testes destrutivos, DoS, DDoS ou exploração massiva da infraestrutura interna;
- O DAAE deverá formalizar autorização para execução dos testes nos ativos envolvidos.
- 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.
- Entregáveis: Relatório Técnico detalhando as vulnerabilidades encontradas.
- Plano de Remediação com sugestões de correção.
- Reteste para validar as correções aplicadas, com período a ser definido com a contratante.

- A equipe responsável pela execução possui profissionais com certificações reconhecidas internacionalmente, incluindo: OSCP – OffSec Certified Professional, OSWE – OffSec Web Expert, CRT0 – Certified Red Team Operator, CEH Practical, eWPTX, eCPPT, eJPT, CISSP, DCPT, EXIN Ethical Hacking Foundation e LPIC-2 Linux Professional Institute.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

O objetivo central desta execução de Red Team (Pentest) é simular o comportamento de um adversário real de forma a avaliar, na prática, a resiliência dos ativos críticos da organização.

A solução consiste na execução de testes controlados que simulam ataques reais. O serviço deve ser executado de forma a não interromper as operações produtivas, com cronograma previamente acordado e comunicação direta com a equipe de infraestrutura.

A demanda fundamenta-se na necessidade imperativa de validar a eficácia dos controles de segurança implementados após atualizações críticas na infraestrutura. Mudanças estruturais recentes, como migrações de firewalls, exigem uma verificação rigorosa para assegurar que as novas camadas de proteção estejam operando conforme o planejado e sem brechas residuais.

Diferente de uma análise de vulnerabilidades convencional, esta abordagem estratégica tem como focos principais:

- Identificar brechas críticas que viabilizem a intrusão efetiva no ambiente corporativo;
- Medir a eficácia e a capacidade de resposta dos controles de segurança atuais;
- Revelar riscos reais e impactos de negócios antes que sejam explorados por cibercriminosos;

- Apoiar a priorização estratégica dos planos de remediação e correções;
- Fortalecer a postura de segurança e a maturidade tecnológica do DAAE Araraquara.

O escopo técnico das atividades foi estabelecido sob os seguintes critérios:

- Modalidade: Black Box (sem fornecimento prévio de informações sobre a infraestrutura).
- Abordagem: Focada estritamente na infraestrutura de borda da instituição.
- Alvos Principais: Firewalls, serviços publicados, aplicações web e quaisquer ativos críticos diretamente expostos à internet.

4. ESTIMATIVA DAS QUANTIDADES

ITEM	DESCRIÇÃO
1	PENTEST (CYBERSECURITY)

Cronograma	
Fase	Responsável
Descoberta e Exploração	Contratada
Execução do Pentest	Contratada
Relatório Executivo e Técnico	Contratada
Apresentação dos Resultados	Contratada
Correções	Contratante
Solicitação de Reteste	Contratante
Reteste	Contratada
Relatório Final	Contratada

4.1. RESULTADO PRETENDIDO COM A CONTRATAÇÃO

A contratação de Testes de Intrusão (Pentest) visa preencher essa lacuna de segurança, submetendo o ambiente a ataques controlados para validar a resiliência institucional contra ameaças externas e internas. O objetivo final é a obtenção de um Plano de Remediação detalhado, que forneça um roteiro técnico de correções priorizado por riscos reais, garantindo a continuidade dos serviços e a conformidade com as diretrizes de segurança da informação.

Os resultados esperados e benefícios pretendidos são os seguintes:

- Redução da Superfície de Ataque: Fechamento de portas e serviços desnecessários.
- Validação de Investimentos: Confirmar se os novos firewalls e soluções de backup estão configurados de forma estanque.
- Compliance: Atendimento às exigências de auditorias externas e da LGPD.
- Cultura de Segurança: Geração de conhecimento para a equipe interna de TI através do plano de remediação.
- Identificação e classificação de riscos (Crítico, Alto, Médio e Baixo).
- Subsídios técnicos para priorização de investimentos em segurança.
- Fortalecimento do perímetro de rede e das políticas de acesso.

5. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Com base na pesquisa realizada com empresas do ramo, verificou-se que o valor estimado da referida contratação é de R\$ 46.000,00.

6. LEVANTAMENTO DE MERCADO

Foram consideradas as seguintes alternativas para atendimento da necessidade administrativa:

- a) execução direta dos serviços pela equipe própria do DAAE;
- b) contratação separada de empresas distintas para auditoria externa, teste de intrusão, análise de vulnerabilidades e elaboração dos relatórios técnicos; e
- c) contratação de empresa especializada para execução integrada dos serviços de auditoria externa, teste de intrusão — Pentest Black Box —, análise de

vulnerabilidades, elaboração dos relatórios técnicos, apresentação das recomendações e realização de reteste.

A execução direta não se mostra adequada, em razão da necessidade de conhecimentos técnicos especializados, ferramentas próprias, metodologias específicas e atuação independente em segurança da informação.

A contratação de empresas distintas poderia ocasionar sobreposição de atividades, dificuldade de coordenação, fragmentação dos achados e risco de incompatibilidade entre as conclusões e recomendações apresentadas.

A contratação integrada de empresa especializada mostra-se adequada, pois permite a execução coordenada das etapas, a consolidação dos resultados em relatórios técnicos e executivos, a elaboração de plano de remediação e a realização de reteste vinculado aos achados inicialmente identificados.

Assim, a solução escolhida consiste na contratação de empresa especializada para execução integrada dos serviços previstos no Termo de Referência, por apresentar maior coerência técnica, melhor coordenação das atividades e maior potencial de aproveitamento dos resultados obtidos.

7. TRATAMENTO FAVORECIDO ÀS ME/EPP

O valor estimado da contratação é de R\$ 46.000,00, conforme pesquisa de preços e planilha de composição do valor estimado juntada aos autos.

Considerando que o valor da contratação é inferior a R\$ 80.000,00 e que o objeto consiste em serviço de natureza tecnológica, executado remotamente, sem necessidade de deslocamento ou prestação presencial nas instalações do DAAE, aplica-se ao certame a participação exclusiva de microempresas e empresas de pequeno porte, nos termos do art. 48, inciso I, da Lei Complementar nº 123/2006.

A pesquisa de preços foi realizada com quatro empresas, todas enquadradas como microempresa ou empresa de pequeno porte, conforme documentação de consulta cadastral juntada ao processo. Esse dado reforça a existência de fornecedores desse porte atuantes no segmento e aptos, em princípio, a apresentar proposta para o objeto.

Não foi identificada circunstância concreta que justifique o afastamento da exclusividade. A execução remota do serviço não exige estabelecimento, equipe ou estrutura física localizada na região do DAAE, sendo suficiente o atendimento aos requisitos técnicos, operacionais e de segurança previstos no Termo de Referência.

Dessa forma, o certame deverá ser destinado exclusivamente à participação de microempresas e empresas de pequeno porte, observados os requisitos de habilitação, qualificação técnica e demais condições estabelecidas no instrumento convocatório.

A justificativa anteriormente elaborada para a não exclusividade fica superada e não deverá fundamentar o procedimento licitatório.

8. JUSTIFICATIVA PARA O PARCELAMENTO (OU NÃO) DA SOLUÇÃO

Em regra, conforme § 2º do art. 40 da Lei n. 14.133/2021, os serviços/compra deverão ser divididos em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

O objeto será contratado em lote único, sem parcelamento, considerando a interdependência técnica entre a auditoria externa, o teste de intrusão, a análise de vulnerabilidades, a elaboração dos relatórios, o plano de remediação e o reteste.

O parcelamento poderia dificultar a responsabilização pelos resultados, fragmentar a avaliação dos ativos expostos à internet e comprometer a integração entre os achados, as recomendações e a posterior validação das correções implementadas.

A execução por uma única empresa também favorece a padronização metodológica, a compatibilidade dos relatórios e a atribuição de responsabilidade técnica integral pelo diagnóstico de segurança da informação.

Além disso, a divisão do objeto entre diferentes contratadas aumentaria os custos de gestão e fiscalização contratual, exigindo a coordenação de múltiplos contratos e podendo reduzir a eficiência da contratação.

Dessa forma, o não parcelamento mostra-se tecnicamente justificável e economicamente conveniente para a Administração, sem prejuízo da competitividade, desde que confirmada, no levantamento de mercado, a existência de empresas aptas a executar integralmente o objeto.

9. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não se verifica-se contratações correlatas nem interdependentes para a viabilidade e contratação desta demanda.

10. IMPACTOS AMBIENTAIS E MEDIDAS DE TRATAMENTO

A presente contratação não apresenta a possibilidade de ocorrência de impactos ambientais.

11. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO



Os estudos preliminares demonstraram a viabilidade técnica e a estrita necessidade da contratação da referida solução. Considerados os riscos mapeados e o imperativo de proteção dos ativos da entidade, a contratação alinha-se ao planejamento estratégico, atuando como uma auditoria técnica na infraestrutura de rede.

Araraquara, 22 de Junho de 2026

David Wilian Quitério
Chefe da Subdivisão de
Desenvolvimento, Infraestrutura e
Suporte

Renildo Moreira de Almeida
Chefe da Divisão de Tecnologia da
Informação