CONSULTA PRELIMINAR

Contratação de Testes de Penetração e Red Teaming

CÂMARA MUNICIPAL DE LISBOA
Departamento de Sistemas de Informação

LISBOA

1. INDICE

2. ENQUADRAMENTO

O Município de Lisboa, na qualidade de Entidade Adjudicante e através do Departamento de Sistemas de Informação, realiza por via desta comunicação, uma consulta preliminar ao mercado, consulta essa que se fundamenta no artigo 35º-A do Código dos Contratos Públicos, na sua versão atual.

A consulta preliminar ao mercado é um processo fundamental no âmbito da contratação pública, que visa antecipar o procedimento formal de adjudicação e promover uma abordagem mais informada e estratégica.

Este mecanismo permite à entidade contratante obter uma visão detalhada sobre o mercado disponível, as alternativas técnicas, as soluções inovadoras e as estimativas de custos associadas aos bens ou serviços que pretende adquirir, antes de lançar o procedimento formal de contratação.

3. FORMA DA CONSULTA

É imperativo que esta consulta preliminar ao mercado seja conduzida com transparência, e não haja tratamento desigual de operadores económicos, conforme dispõe o artigo 35.º-A do Código dos Contratos Públicos. Com esse objetivo em vista, toda a informação da consulta preliminar é publicitada no portal Internet público da Câmara Municipal de Lisboa - https://www.lisboa.pt/.

A prestação voluntária e não vinculativa de informação pelos operadores económicos deverá ser feita através do endereço de e-mail dsi.cp@cm-lisboa.pt até às 18h do dia 08 de agosto de 2025.

4. OBJETO DA CONSULTA - ESPECIFICAÇÕES

Com vista à maximização da segurança dos nossos sistemas de informação, iniciamos uma consulta preliminar ao mercado para a contratação de serviços especializados em testes de penetração e Red Teaming a realizar entre 2026 e 2028 de acordo com o seguinte planeamento:

Plano anual mínimo para a CML:

Tipo de Teste	**Frequência**	**Observações**
Testes de Penetração	2 por ano – num total de 6	Uma vez em sistemas expostos, outra em internos.
Exercício de Red Teaming	3 testes (1 por ano)	Envolve coordenação e análise pós-evento.
Testes de engenharia social (phishing, etc.)	2x/ano (mínimo)	Pode ser incluído no Red Teaming ou realizado isoladamente.

Estes serviços são imprescindíveis para a identificação e mitigação de vulnerabilidades, garantindo a integridade, confidencialidade e disponibilidade dos nossos dados e sistemas.

4.1 Objetivo da Consulta

Necessidade: Identificar, avaliar e selecionar fornecedores qualificados e experientes para a execução de testes de penetração e Red Teaming.

Âmbito: os testes, devem incluir, mas não se limitar a: Sistemas e redes corporativas, Aplicações web e móveis, Infraestrutura em nuvem, Dispositivos IoT, redes sociais, Engenharia social.

4.2 Requisitos Técnicos

Experiência e Qualificações:

- Certificações mínimas: OSCP, CEH, GPEN, CISSP.
- Experiência comprovada em projetos similares, com preferência para empresas que possuam experiência em setores da Administração Pública ou em ambientes

de complexidade comparável.

- Demonstração de uma equipa técnica robusta e multidisciplinar, capaz de executar os diferentes tipos de testes propostos.

Metodologias:

- Utilização de frameworks reconhecidos como OWASP, NIST, PTES, ISO/IEC 27001:2022, ISO/IEC 42001:2023, CIS Controls, COBIT, MITRE ATT&CK, OSSTMM, Cyber Kill Chain.
- Abordagem sistemática: proposta de uma abordagem estruturada para a identificação, exploração, validação e mitigação de vulnerabilidades, que inclua fases claras de planeamento, execução e reporte.

Ferramentas:

Os fornecedores devem demonstrar proficiência e capacidade para utilizar um conjunto diversificado e atualizado de ferramentas que abranjam as seguintes categorias:

- Varredura e enumeração: Nmap, Nessus, OpenVas, Nikto, Masscan.
- Exploração: Metasploit, Burp Suite, SQLMap, Commix, Explot-DB.
- Pós-exploração: Mimikatz, BloodHound, Empire, PoshC2, PowerSploit.
- Ataque a redes: Aircrack-ng, Responder, Ettercap, Scapy, Bettercap.
- Quebra de senhas: John the Ripper, Hashcat, Ophcrack, Hydra, Medusa.

4.3 Requisitos de Segurança

Confidencialidade:

- Acordos de Confidencialidade (NDA): Obrigatoriedade de assinatura de NDAs robustos para proteger todas as informações sensíveis e proprietárias da organização.
- Medidas de Segurança de Dados: Detalhe das medidas de segurança implementadas para garantir a proteção dos dados (em trânsito e em repouso) durante e após a execução dos testes.

Relatórios:

- Relatórios Detalhados de Vulnerabilidades: Elaboração de relatórios técnicos completos e compreensíveis, com:
    - Descrição clara das vulnerabilidades encontradas.
    - Classificação de risco baseada em metodologias reconhecidas (CVSS ou similar).
    - Evidências e passos de reprodução para cada vulnerabilidade.
- Recomendações Práticas e Priorizadas: Fornecimento de recomendações de mitigação acionáveis e priorizadas, com base no risco e no impacto potencial.
- Relatórios Executivos: Apresentação de relatórios de alto nível, concisos e focados na gestão, que destaquem os principais achados, riscos globais e o progresso da postura de segurança.

4.4 Coordenação com o SOC e o CISO

A coordenação e comunicação eficazes com as equipas internas, nomeadamente o Centro de Operações de Segurança (SOC) e o Chief Information Security Officer (CISO), são mandatórias.

Integração de Procedimentos:

- Os fornecedores devem demonstrar como os testes serão alinhados e integrados com os processos e procedimentos operacionais existentes do SOC.

Monitorização e Deteção:

- Colaboração contínua com o SOC para:
    - Assegurar a monitorização das atividades de teste.
    - Analisar os alertas gerados e validar as capacidades de deteção do SOC.
    - Utilizar os testes para refinar e melhorar as regras de deteção.

Resposta a Incidentes:

- Estabelecimento de um plano de comunicação e resposta a incidentes em conjunto com o SOC para gerir e mitigar rapidamente qualquer descoberta crítica durante os testes. Poderão ser realizados exercícios de simulação de incidentes para treinar a equipa.

Definição de Objetivos Estratégicos:

- Colaborar com o CISO para garantir que os objetivos dos testes estejam perfeitamente alinhados com a estratégia global de segurança da organização.

Métricas e KPIs:

- Definição conjunta de métricas e Indicadores Chave de Desempenho (KPIs) para avaliar o sucesso dos testes em termos de melhoria da postura de segurança.

Relatórios e Comunicação Executiva:

- Assegurar que os relatórios sejam claros e apresentados de forma compreensível à alta administração, com reuniões regulares com o CISO para discussão de resultados e ações corretivas.

Conformidade e Regulamentação:

- Garantir que todos os testes estejam em conformidade com as políticas internas de segurança, regulamentações aplicáveis (ex: NIS2, GDPR/LGPD) e normas como a ISO 27001.

4.5 Feedback e Melhoria Contínua

Avaliação Pós-Teste:

- Realização de sessões de avaliação pós-teste com o SOC e o CISO para discutir resultados, lições aprendidas e identificar oportunidades de melhoria contínua nos processos de teste e na postura de segurança.

Formação e workshops:

- Proporcionar, quando apropriado, sessões de formação ou workshops para a equipa do SOC com base nas descobertas dos testes e nas melhores práticas identificadas. Colaborar com o CISO no desenvolvimento de programas de formação contínua.

5. INFORMAÇÃO PRETENDIDA

Solicitamos que os operadores económicos, voluntariamente, disponibilizem a seguinte informação em resposta a esta Consulta Preliminar;

5.1 Aquisição de serviços

Experiência Anterior:

- Histórico de projetos: apresentar um portfólio de projetos bem-sucedidos em testes de penetração e Red Teaming, com foco em resultados e benefícios para os clientes.
- Referências: fornecer referências de clientes anteriores que possam atestar a qualidade e a eficácia dos serviços prestados.

Capacidade de Resposta:

- Tempo de resposta; detalhar os tempos de resposta esperados para comunicação e intervenção em caso de descobertas críticas ou incidentes durante os testes.
- Disponibilidade; indicar a disponibilidade para testes de follow-up, reavaliações e suporte contínuo após a conclusão do projeto inicial.

Custo

Preenchimento da seguinte tabela.

Tipo de Teste	Quantidade Estimada	Preço Unitário (€)	Preço Total (€)	Observações Técnicas Relevantes
Testes de Penetração (incluindo trabalhos preparatórios, relatórios, aconselhamento, etc.)	6			Indicar se é por IP, por aplicação, por segmento de rede, etc.
Exercícios de Red Teaming (incluindo trabalhos preparatórios, relatórios, aconselhamento, etc.)	3			Indicar duração típica, nº de operadores, cobertura esperada.
Testes de Engenharia Social (phishing, vishing, etc.) (incluindo trabalhos preparatórios, relatórios, aconselhamento, etc.)	3			Indicar nº de alvos por campanha, métodos utilizados.
Outros Custos (discriminados por área, se possível)	—			Ex.: deslocações, retestes, relatórios adicionais, etc.

Notas Importantes:

1. **Preços apresentados devem incluir todos os encargos associados**, nomeadamente:
    - Planeamento e calendarização;
    - Reuniões preparatórias e de alinhamento;
    - Execução técnica do teste/exercício;
    - Reteste (se incluído);
    - Elaboração e apresentação de relatórios técnicos e executivos;
    - Sessões de esclarecimento e aconselhamento com as equipas técnicas da CML.
2. Devem ser discriminados, sempre que aplicável:
    - Custos de deslocação;
    - Custos por iteração adicional (retestes);
    - Custos de resposta fora do horário normal de trabalho;
    - Custos adicionais por personalização de relatórios ou dashboards.
3. A proposta deve indicar:
    - A **validação temporal dos preços apresentados** (mínimo 6 meses);
    - As **condições de faturação** (ex. por fase ou por entrega).
4. Incluir uma **nota metodológica** anexa à proposta, que detalhe:
    - As abordagens técnicas (ex.: OWASP, MITRE ATT&CK, PTES);
    - Ferramentas utilizadas (open source e comerciais);
    - Certificações das equipas (ex.: OSCP, OSCE, CRTO, etc.);
    - Estimativa de esforço e duração típica por tipo de serviço.

Prazos:

- Divisão de custos contabilizando 3 anos do serviço.
- Cronograma proposto; apresentar um cronograma detalhado para a execução dos testes, que inclua fases de planeamento, execução (com estimativa de duração por tipo de teste) e apresentação de relatórios.

Os operadores económicos poderão ainda apresentar outra informação que considerem relevante no âmbito da consulta.