CONSULTA PRELIMINAR

Contratação de serviços de CISO

(Chief Information Security Officer)

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 31 de julho de 2025.

4. OBJETO DA CONSULTA - ESPECIFICAÇÕES

A Câmara Municipal de Lisboa (CML), no âmbito da sua estratégia de reforço da maturidade em cibersegurança, pretende auscultar o mercado quanto à viabilidade, soluções existentes e boas práticas associadas à prestação de um serviço externo de **CISO as a Service**. Esta função deverá assegurar a governação estratégica e operacional da segurança da informação e da cibersegurança em toda a organização, em alinhamento com a legislação em vigor e os referenciais normativos aplicáveis.

A presente consulta visa recolher contributos que apoiem a definição do procedimento de contratação a lançar futuramente, nomeadamente quanto à estruturação técnica do serviço, competências exigidas e indicadores de desempenho a considerar.4.1 Contexto e Enquadramento

A CML é uma organização pública de grande dimensão e complexidade, com uma infraestrutura tecnológica híbrida (on-premises e cloud), múltiplos fornecedores de serviços TIC e uma crescente dependência digital para a prestação de serviços aos cidadãos. Neste contexto, torna-se fundamental dispor de uma função de CISO com capacidade de articulação transversal, visão estratégica, domínio normativo e competência técnica para gerir riscos, assegurar conformidade e desenvolver uma cultura organizacional de cibersegurança.

4.2. Âmbito e Responsabilidades do Serviço de CISO

O serviço de CISO a contratar deverá garantir a execução contínua e articulada das seguintes **funções e responsabilidades**:

A. Governação e Estratégia de Segurança

- Definir e manter a **estratégia de cibersegurança da CML**, alinhada com os objetivos estratégicos da organização.
- Estabelecer a **Política de Segurança da Informação**, e apoiar a sua aprovação e divulgação interna.
- Desenvolver políticas e normas complementares (controlo de acessos, gestão de incidentes, classificação da informação, etc.).

B. Gestão de Risco e Conformidade

- Implementar um processo contínuo de **gestão de riscos de segurança da informação**.
- Assegurar a conformidade com os requisitos legais e regulamentares aplicáveis: **RGPD, NIS2, ENS, CCP, normas ISO/IEC 27001 e 22301**.
- Apoiar auditorias internas e externas em matéria de segurança.

C. Continuidade de Negócio e Resiliência

- Coordenar e atualizar os seguintes documentos:
  - **Análise de Impacto no Negócio (BIA)**;
  - **Plano de Continuidade de Negócio (PCN)**;
  - **Plano de Recuperação de Desastres (DRP)**.

D. Gestão e Resposta a Incidentes

- Desenvolver e manter o **Plano de Resposta a Incidentes**, com foco nos requisitos da Diretiva **NIS2**.
- Definir procedimentos para deteção, comunicação, contenção, resposta e lições aprendidas.
- Estabelecer canais de reporte à **CNCS** e outras entidades relevantes.

E. Formação e Sensibilização

- Conceber e implementar um **Plano de Sensibilização e Formação em Cibersegurança**, com ações dirigidas a diferentes perfis: técnicos, chefias, dirigentes e utilizadores em geral.
- Promover exercícios práticos (ex: simulações de phishing, testes de resposta a incidentes).

F. Segurança na Cadeia de Fornecimento

- Criar um **Programa de Gestão de Segurança de Fornecedores**, que inclua critérios de avaliação, cláusulas contratuais padrões e mecanismos de monitorização contínua.
- Apoiar os serviços adjudicantes na incorporação de requisitos de segurança nos contratos TIC.

G. Segurança no Ciclo de Vida do Software

- Definir **procedimentos e boas práticas para o desenvolvimento de software seguro**, tanto em projetos internos como externos.
- Promover a integração de práticas **DevSecOps**, e o uso de ferramentas de análise de vulnerabilidades.

H. Monitorização e Melhoria Contínua

- Estabelecer **métricas e indicadores de desempenho da função de cibersegurança**.
- Produzir relatórios regulares para as chefias e órgãos executivos da CML.

4.3. Tarefas Prioritárias na Fase Inicial da Prestação de Serviços

A entidade contratada deverá, logo no início da prestação de serviços, desenvolver, propor para aprovação e apoiar a implementação dos seguintes **documentos estruturantes**:

1. **Política de Segurança da Informação**
2. **Plano de Continuidade de Negócio (PCN)**
3. **Análise de Impacto no Negócio (BIA)**
4. **Plano de Recuperação de Desastres (DRP)**
5. **Plano de Resposta a Incidentes (em conformidade com a NIS2)**
6. **Plano de Sensibilização e Formação em Cibersegurança**
7. **Programa de Gestão de Segurança de Fornecedores**
8. **Procedimentos para Desenvolvimento Seguro de Software**

A validação e aprovação destes documentos pelas áreas executivas da CML constitui um marco fundamental para o sucesso da função de CISO.

4.4. Indicadores de Desempenho (KPIs) Propostos

A avaliação do desempenho do serviço de CISO será feita com base em indicadores objetivos, a definir no procedimento de contratação. De forma indicativa, apresentam-se os seguintes:

Indicador	Descrição	Meta Indicativa
% de documentos estruturantes desenvolvidos e aprovados no prazo	Percentagem de entregas realizadas nos prazos definidos no plano inicial	≥ 90%
N.º de ações de sensibilização realizadas	Contabiliza sessões por público-alvo e taxa de participação	≥ 4 por ano
% de incidentes registados com resposta em conformidade com o plano	Medido por tempo médio de deteção e resolução vs. o definido	≥ 95%
Grau de conformidade com NIS2 e ISO 27001	Avaliado por auditoria interna ou externa	≥ 80%
N.º de fornecedores avaliados quanto à cibersegurança	Inclui análise de risco e aplicação de critérios	≥ 10 por ano
Aderência aos procedimentos de desenvolvimento seguro	Verificada por amostras em projetos TIC	≥ 90%

4.5. Participação na Consulta

As entidades interessadas deverão apresentar contributos e propostas relativamente a:

- Modelos de prestação de serviço de CISO (dedicado, partilhado, híbrido);
- Recursos e perfis mínimos recomendados;
- Ferramentas e metodologias que considerem mais adequadas;
- Riscos associados à contratação externa desta função;
- Sugestões adicionais de indicadores de desempenho.

5. INFORMAÇÃO PRETENDIDA

De seguida são apresentadas algumas orientações gerais para o que, voluntariamente, solicitamos que os operadores económicos nos disponibilizem em resposta à Consulta Preliminar.

5.1 Aquisição serviço de CISO

- **Metodologia de Trabalho:** Solicitamos sugestões sobre abordagens, metodologias e boas práticas para os serviços requeridos. Os operadores económicos devem descrever detalhadamente as metodologias que utilizam para a monitorização, deteção e resposta a incidentes de segurança, incluindo as melhores práticas adotadas e como estas se alinham com normas e regulamentações aplicáveis.

- **Estimativa de Custo:** Pretendemos obter uma noção de custos baseada na dimensão e complexidade do projeto ou volume de horas a contratar. Solicitamos que os custos sejam discriminados por itens sempre que possível, incluindo honorários dos consultores, custos de ferramentas e software, e quaisquer outras despesas associadas.

- **Prazos e Cronogramas de Execução:** Os operadores económicos devem apresentar um cronograma detalhado que inclua todas as fases do projeto, desde a análise inicial até à implementação e testes finais, indicando os prazos esperados para cada fase.

- **Casos de Estudo ou Referências:** Solicitamos exemplos de projetos semelhantes realizados anteriormente pelos operadores económicos. Devem ser fornecidos casos de estudo ou referências que demonstrem a experiência e competência na prestação de serviços de CISO.

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