CONSULTA PRELIMINAR

Aquisição de serviços de Implementação do **Centro de Operações de Segurança (SOC)**

LISBOA

CÂMARA MUNICIPAL DE LISBOA
Departamento de Sistemas de Informação

1. Conteúdo

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 16:00h do dia 27 de junho de 2025.

4. OBJETO DA CONSULTA - ESPECIFICAÇÕES

A Câmara Municipal de Lisboa (CML), através do seu Departamento de Sistemas de Informação (DSI), pretende recolher informações do mercado relativas à prestação de serviços especializados de cibersegurança através de uma **Aquisição de Serviços de Implementação do Centro de Operações de Segurança (SOC)**, **num modelo gerido,**

com supervisão e acompanhamento pela CML, garantindo cobertura contínua, especialização técnica e integração com as equipas municipais.

4.1 Infraestrutura da CML a considerar

Dados de referência	Fontes de dados
1. Cloud services: Azure 2. Universo de utilizadores dos domínios: 11.000 3. Número de domínios: 2 4. Número de domínios de parceiros/fornecedores por VPN: 70 5. Ativos e passivos de rede e equipamentos atualizados. 6. Necessidade de acesso ao SOC para 5 utilizadores. 7. Fontes de dados a monitorizar: • WindowsServers: 262 • LinuxServers: 198 • Firewalls: 2 • VPNGateways: 1 • DDoSProtection: 1 • LoadBalancers: 5 • IDS/IPSSensors: 1 • InternetProxies: 7 • WebServersIIS: 20 • OutrosWebServers: 30 8. A integração eficaz de várias ferramentas de segurança é essencial para o funcionamento do SOC. Algumas dessas ferramentas incluem:	1. DomainControllers: 8 2. FileServers: 1 3. Hypervisors(VMware,etc.): 22 4. DNSServers: 2 5. Databases: 15x OracleServers+10xMSSQL+3xpostgresql 6. BackupSolutions: 3 7. EDR/XDR(numberofendpoints): 1 8. AuthenticationSystems(Radius,SSO): 2 9. IBMPower9: 2

1. Firewall e IDS/IPS (Intrusion Detection and Prevention Systems): Para monitorizar e bloquear tráfego malicioso. 2. Soluções EDR (Endpoint Detection and Response): Para detectar e responder a ameaças em endpoints, como computadores, dispositivos móveis e servidores. 3. NDR (Network Detection and Response): Para monitorizar e responder a ameaças dentro da rede.Threat Intelligence: 4. Plataformas de inteligência de ameaças que fornecem dados sobre as últimas ameaças e ataques conhecidos, ajudando a antecipar possíveis incidentes.	

4.2 Serviços a Prestar

Domínio funcional	Serviço a prestar pelo SOC	Papel da CML
1. Monitorização e Deteção	- Monitorização contínua 24/7 de logs de rede, endpoints, sistemas, cloud, aplicações e dispositivos IoT - Deteção de comportamentos anómalos (com recurso a SIEM e UEBA) - Integração de fontes de threat intelligence	- Validar o âmbito e as fontes a monitorizar - Acompanhar relatórios e reuniões de alinhamento
2. Gestão de Alertas e	- Triagem automática e manual de eventos - Correlacionamento e classificação de	- Definir critérios de escalonamento

Domínio funcional	Serviço a prestar pelo SOC	Papel da CML
Incidentes	alertas por criticidade - Escalonamento à CML apenas quando necessário	- Intervir apenas em incidentes críticos
3. Resposta a Incidentes	- Contenção inicial (isolamento de dispositivos, bloqueio de IPs, etc.) - Erradicação com base em procedimentos definidos - Apoio à recuperação e reposição de serviço	- Disponibilizar contactos técnicos - Acompanhar planos de resposta e recuperação
4. Análise Forense	- Análise pós-incidente (linhas cronológicas de logs, origem do ataque, impacto) - Preservação de evidência digital	- Validar relatórios e coordenar contacto com entidades externas (ex: CNCS, PJ)
5. Gestão de Vulnerabilidades	- Inventariação contínua de ativos - Execução regular de varrimentos de vulnerabilidades - Priorização de riscos e recomendações de mitigação	- Garantir aplicação de correções com as equipas internas de IT
6. Threat Intelligence (Inteligência de Ameaças)	- Fornecimento contínuo de indicadores de ameaça - Alertas sobre campanhas direcionadas ao setor público/autárquico	- Acompanhar reuniões de análise de risco
7. Automatização (SOAR)	- Implementação de procedimentos automáticos (ex: resposta a phishing, brute force, beaconing) - Criação de tickets automáticos	- Aprovar fluxos e validar respostas automáticas
8. Conformidade e Auditoria	- Apoio ao cumprimento da NIS2, RGPD e ISO 27001 - Registo de logs e evidência de resposta	- Participar em auditorias e assegurar articulação com os

Domínio funcional	Serviço a prestar pelo SOC	Papel da CML
	- Suporte a auditorias	serviços jurídicos e de compliance
9. Relatórios e Dashboards	- Dashboards em tempo real acessíveis à CML - Relatórios semanais, mensais e trimestrais - Indicadores operacionais e estratégicos	- Analisar relatórios e partilhar informação relevante com a gestão autárquica
10. Capacitação e transferência de conhecimento	- Formação periódica - Documentação de processos - Simulações de incidentes (exercícios tabletop)	- Indicar os recursos a formar e promover a retenção de conhecimento

4.3 Modelo de relacionamento com a CML

Atividade / Entrega	**Periodicidade sugerida**
Reuniões técnicas operacionais	Semanal
Reuniões de coordenação e estratégia	Mensal
Relatórios de alertas e eventos	Semanal e ad hoc
Relatórios executivos e dashboards	Mensal ou trimestral
Exercícios de simulação de incidentes	Semestral
Atualização de playbooks e procedimentos	Trimestral ou contínua
Sessões de formação internas	Trimestral ou semestral

4.4 Principais Indicadores de desempenho pretendidos

Requisito	**Nível mínimo esperado**
Tempo de resposta a incidentes críticos	≤ 15 min (Tier 1)
Tempo de mitigação ou contenção inicial	≤ 1h
Disponibilidade do serviço SOC	99.9% (24/7/365)

4.5 Outros requisitos

Relatórios de atividade	Semanais + Mensais
Auditorias e testes de eficácia	Trimestrais
Confidencialidade de dados	Conformidade com RGPD
Interface técnica com DSI	Portal ou API + contacto dedicado

O fornecedor deverá operar num ambiente certificado (preferencialmente ISO 27001 e/ou ENS).

O SOC deverá garantir redundância e continuidade operacional (Disaster Recovery)

Todo o tráfego de comunicação entre o SOC e a CML deverá ser cifrado.

Os dados da CML não deverão sair da União Europeia sem autorização expressa.

5. INFORMAÇÃO PRETENDIDA

De seguida são apresentadas algumas orientações gerais para que, voluntariamente, os interessados em responder à presente Consulta Preliminar, possam disponibilizar as seguintes informações.

Os interessados deverão apresentar, informação detalhada da solução proposta tendo em conta os capítulos seguintes.

5.1 Proposta Técnica

- Metodologia de trabalho: Descrição da abordagem proposta para a realização dos serviços, incluindo técnicas, frameworks e ferramentas a utilizar.
- Plano e faseamento dos trabalhos: Definição das principais fases do projeto, com identificação de atividades, entregáveis e estimativa de prazos para cada etapa.
- Tempo estimado de implementação (onboarding) e maturação do serviço.
- Modelo de arquitetura aplicacional: Proposta preliminar da abordagem arquitetónica a adotar, considerando a integração com os sistemas existentes e as melhores práticas de interoperabilidade.
- Estratégia de gestão da mudança: Recomendações sobre como garantir a adoção eficaz da nova arquitetura dentro da CML.
- Localização do SOC e da infraestrutura.
- Escalabilidade da solução;
- Capacidade de integração com ambientes Microsoft, Google Cloud, firewalls, e outros SIEM's existentes.
- Modelos de escalonamento e contacto.
- Exemplo de relatório técnico e executivo.
- Materiais de apoio (brochuras técnicas, vídeos demonstrativos, etc.).

5.2 Equipa Técnica Envolvida

- Perfil da equipa: Identificação dos perfis técnicos da equipa de projeto, com apresentação das certificações dos analistas.

5.3 Experiência e Projetos Anteriores

- Portfólio de projetos semelhantes: Descrição de trabalhos realizados anteriormente na implementação de Sistemas de Operações de Cibersegurança (SOC) em Entidades públicas ou autárquicas que já utilizem o serviço.
- Casos de sucesso: Exemplos concretos de implementação de Sistemas de Operações de Cibersegurança (SOC).
- Referências: Contactos de clientes anteriores que possam validar a experiência da empresa.

5.4 Estimativa de Custos

- Orçamento preliminar: Indicação do custo estimado para a prestação dos serviços, tendo em conta o cenário de 36 meses de serviço SOC efetivo, tendo em conta as diferentes fases até à entrada em produção do SOC.
- Capacidade de o licenciamento ser ajustado consoante a implementação do projeto.
- Forma de licenciamento: por volume de logs, número de activos, flat fee, etc.

5.5 Conformidade e Requisitos Legais

- Certificações e normas aplicáveis: Indicação de certificações e outras normas aplicáveis.