Caderno de Encargos

PROCEDIMENTO POR CONCURSO PÚBLICO N.º 14/2024

(Nos termos do disposto na al. a), b), c) ou d), do n.º 1 do art.º 20.º do CCP)

Capítulo I
Disposições Gerais

Cláusula 1.ª
Objeto

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto principal a **prestação de serviços para a proteção da cibersegurança.**

Cláusula 2.ª
Preço base

1 – Pela prestação de serviços, objeto do presente procedimento de aquisição, o Município da Lousã dispõe-se pagar um valor global máximo de **71.000,00€ (setenta e um mil euros),** não incluindo o imposto sobre o valor acrescentado.

2 - O preço base definido tem por fundamento o valor obtido através da consulta preliminar ao mercado prevista no art.º 35.º-A do CCP.

Cláusula 3.ª
Contrato

1 - O contrato é composto pelo respetivo clausulado contratual e os seus anexos. O clausulado do contrato deverá conter os seguintes elementos:

a) A identificação das partes e dos respetivos representantes, assim como do título a que intervêm, com indicação dos atos que os habilitem para esse efeito;

b) A indicação do ato de adjudicação e do ato de aprovação da minuta do contrato;

c) A descrição do objeto do contrato;

d) O preço contratual ou o preço a receber pela entidade adjudicante ou, na impossibilidade do seu cálculo, os elementos necessários à sua determinação;

e) O prazo de entrega;

f) Os ajustamentos aceites pelo adjudicatário;

g) A referência à caução prestada pelo adjudicatário;

h) Se for o caso, a classificação orçamental da dotação por onde será satisfeita a despesa inerente ao contrato, a realizar no ano económico da celebração do mesmo ou, no caso de tal despesa se realizar em mais de um ano económico, a indicação da disposição legal habilitante ou do plano plurianual legalmente aprovado de que o contrato em causa constitui execução ou ainda do instrumento, legalmente previsto, que autoriza aquela repartição de despesa;

i) A identificação do gestor do contrato em nome da entidade adjudicante, nos termos do artigo 290.º-A;

j) As eventuais condições de modificação do contrato expressamente previstas no caderno de encargos, incluindo cláusulas de revisão ou opção, claras, precisas e inequívocas.

2 - O contrato a celebrar integra ainda os seguintes elementos:

a) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;

b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;

c) O presente Caderno de Encargos;

d) A proposta adjudicada;

e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3 - Em caso de divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem pela qual são indicados nesse número.

4 - Em caso de divergência entre os documentos referidos no nº 2 e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101º desse mesmo diploma legal.

Cláusula 4.ª

Período de vigência

O contrato mantém-se em vigor pelo período de 3 (três) anos.

Capítulo II

Obrigações Contratuais

Secção I

Obrigações do Adjudicatário

Subsecção I

Disposições Gerais

Cláusula 5.ª

Especificações Técnicas

O contrato a celebrar terá de obedecer às especificações técnicas constantes do **Anexo I** ao presente documento.

Subsecção II

Dever de sigilo

Cláusula 6.ª

Objeto do dever de sigilo

1 – O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à Câmara Municipal, de que possa ter conhecimento por conta da execução do contrato.

2 - A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem ser objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.

3 - Exclui-se do dever de sigilo previsto, a informação e a documentação que fossem comprovadamente do domínio público, à data da respetiva obtenção pelo prestador de serviços, ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

4 - O cocontratante deve prestar ao contraente público todas as informações que este lhe solicitar e que sejam necessárias à fiscalização do modo de execução do contrato, devendo o contraente público satisfazer os pedidos de informação formulados pelo cocontratante e que respeitem a elementos técnicos na sua posse, cujo conhecimento se mostre necessário à execução do contrato.

5 - Salvo quando, por força do contrato, caiba ao cocontratante o exercício de poderes públicos, compete exclusivamente ao contraente público a satisfação do direito à informação, por parte de particulares, sobre o teor do contrato e quaisquer aspetos da respetiva execução.

6 - O contraente público e o cocontratante guardam sigilo sobre quaisquer matérias sujeitas a segredo nos termos da lei às quais tenham acesso por força da execução do contrato.

Capítulo IV

Disposições finais

Cláusula 7.ª

Casos fortuitos ou de força maior

1 - Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior – entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar – for impedido de cumprir as obrigações assumidas no contrato.

2 - A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

3 - Não constituem força maior, designadamente:

a) Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;

b) Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;

c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;

d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;

e) Incêndios ou inundações com origem nas instalações do adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;

f) Avarias nos sistemas informáticos ou mecânicos do adjudicatário não devidas a sabotagem;

g) Eventos que estejam ou devam estar cobertos por seguros.

4 - A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 8.ª

Cessão da posição contratual

O adjudicatário não poderá ceder a sua posição contratual, ou qualquer dos direitos e obrigações decorrentes do contrato, sem autorização da entidade adjudicante.

Cláusula 9.ª

Comunicações e notificações

1 - Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do

Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no Contrato.

2 - Qualquer alteração das informações de contacto constantes do Contrato deve ser comunicada à outra parte.

Cláusula 120ª

Contagem dos prazos na fase de formação dos contratos e da execução dos contratos

A contagem dos prazos na fase de formação dos contratos e da execução dos contratos, far-se-á nos termos respetivamente do artigo 470º e do artigo 471º do CCP.

Cláusula 11.ª

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal do Coimbra, com expressa renúncia a qualquer outro.

Cláusula 12.ª

Legislação aplicável

Em tudo o que for omisso no presente Caderno de Encargos, observar-se-á o disposto no Código dos Contratos Públicos, na redação atual, e demais legislação portuguesa em vigor.

ANEXO I

ESPECIFICAÇÕES TÉCNICAS

A Câmara Municipal da Lousã, pretende, adquirir uma solução a 3 anos, que contemple o fornecimento, instalação, configuração e formação *onsite* de todos as soluções propostas deste caderno de encargos.

Estas soluções têm de cumprir ou exceder as características técnicas abaixo descritas, devem ser obrigatoriamente ser todas do mesmo fabricante e incluir bolsa de 100 horas de suporte às soluções.

Deverá também ser remetida declaração do fabricante informando em como o concorrente está autorizado a vender e instalar as soluções.

1. Antimalware, Vulnaribilty e Patch Management

1. Proteção de Endpoints

A proteção de endpoints deve cumprir obrigatoriamente os seguintes requisitos mínimos:

Para proteção dos endpoints será necessário considerar o licenciamento de uma solução de Endpoint, com licenciamento para 225 dispositivos, com gestão na Cloud, com os seguintes requisitos mínimos:

a) Deve emular ameaças simulando a execução de ficheiros desconhecidos num ambiente isolado para detetar comportamentos maliciosos e prevenir violações, bem como extrair ameaças como conteúdos ativos dos documentos acedidos pelos utilizadores, entregando ficheiros limpos sem qualquer perigo;

b) Deve incorporar uma proteção Anti-Ransomware que interrompa o Malware desde o primeiro momento e repare automaticamente o dano (restaurando cópias criptografadas pelo Ransomware);

c) Deve utilizar uma tecnologia que funcione sem assinaturas e não seja baseada em atualizações constantes, funcionando tanto online quanto offline, colocando infeções em quarentena automaticamente com base na sua análise forense, bem como restaurando automaticamente ficheiros criptografados por Ransomware ao seu estado antes do ataque;

d) Deve ser capaz de prevenir erros humanos e detetar Phishing de Zero-Day, bloqueando proactivamente o acesso a sites novos e desconhecidos, bem como salvaguardar as credenciais dos utilizadores e impedir o uso de senhas corporativas em sites externos;

e) Deve fornecer relatórios forenses de ameaças, coletando continuamente todos os eventos relevantes do sistema, e fornecer pesquisa proativa de incidentes e análises para entender rapidamente o ciclo de vida completo do ataque, fornecer maior visibilidade do ataque e vetores de danos do ataque para

maximizar a produtividade da equipa de resposta e minimizar a exposição organizacional;

f) Os relatórios forenses devem oferecer uma visão do ataque representando os dados de acordo com um padrão de segurança de acordo com a Matriz MITRE ATT & CK;

g) A solução deve fornecer visibilidade total com recursos forenses, monitorizando e registando todos os eventos que ocorrem nos terminais: ficheiros afetados, processos iniciados, alterações no registo do sistema e atividade de rede. Esta monitorização deve garantir que os dados estejam disponíveis, mesmo se o ataque for bem-sucedido, mesmo se ele remover ficheiros ou outros indicadores de comprometimento que foram deixados no sistema;

h) A solução deve incorporar mecanismos de análise comportamental que usem análise forense para identificar de forma eficaz e exclusiva comportamentos de Malware desconhecidos e classificar com precisão o Malware na categoria apropriada;

i) Deve ter mecanismos de segurança de navegação incorporados aos principais navegadores da web que sejam capazes de extrair ameaças e reconstruir ficheiros acedidos pelos usuários em poucos segundos, eliminando possíveis ameaças e entregando rapidamente uma versão segura ao utilizador. Além disso, deve incorporar mecanismos de emulação de ameaças que detetam comportamento malicioso e evitam infeções por Malware de dia zero e ataques direcionados, inspecionando ficheiros em um ambiente de Sandbox virtual. A filtragem de navegação é necessária usando a Filtragem de URL para garantir uma navegação segura;

j) A solução deve proteger os utilizadores de ameaças que chegam por meio de downloads da Internet usando técnicas como Phishing, conteúdo malicioso copiado para dispositivos de armazenamento removíveis, infeções causadas por movimento lateral de dados e Malware entre sistemas em segmentos específicos da rede, bem como infeções por meio de conteúdo criptografado;

k) A solução deve incluir proteção Anti-Bot, continuamente atualizada com os dados de inteligência de ameaças mais recentes, identificando e bloqueando as comunicações de Botnet com servidores de comando e controlo (C&C), contendo e colocando em quarentena os dispositivos infetados;

l) O instalador da solução deve ser capaz de desinstalar agentes antivírus de terceiros e a solução deve ser capaz de ser implementada de forma fácil com administração local ou na Cloud;

m) A solução deve ter uma consola central para definir políticas, criar grupos de sistema/utilizadores, registar, implementar atualizações, gerar relatórios com acesso baseado em funções e oferecer suporte ao uso de autenticação de sistemas de terceiros;

n) A solução forçará as estações de trabalho a cumprir as regras de segurança definidas pela organização. Aqueles que não cumprirem serão mostrados como não conformes e políticas restritivas devem ser aplicadas;

o) Deve ter um cliente de VPN integrado no próprio Endpoint, e permitir a ligação nativamente com a firewall;

p) A solução deve incluir módulos de análise forense, criando automaticamente uma análise de incidentes para cada deteção/prevenção que ocorrer;

q) A solução deve incluir módulos Threat Hunting que permitem a pesquisa de vários tipos de dados de sensor não detetados, incluindo ficheiros, processos, rede, registo, injeção e dados do utilizador;

r) A solução deve permitir a correção de qualquer ficheiro ou processo encontrado através do Threat Hunting;

s) A solução deve permitir análises forenses e relatórios de qualquer indicador encontrado por meio do Threat Hunting. A solução enriquecerá automaticamente seus resultados de pesquisa confiáveis;

t) A solução deve incluir um módulo de Gestão de Postura do Endpoint que permita a gestão de vulnerabilidades e a correção dessas mesmas vulnerabilidades;

u) A solução deve ajudar a identificar vulnerabilidades e ameaças potenciais nos Endpoints e a garantir uma postura de segurança consistente em todos eles;

v) O módulo de gestão de postura deve fornecer deteção automatizada de vulnerabilidades, priorização e correção para reduzir o risco de violação de dados ou outro incidente de segurança e proteger os ativos digitais da organização;

w) A solução deve gerar relatórios periódicos sobre tipos de Malware, tipos de vulnerabilidades exploradas, etc.

- A solução deve ter a capacidade de gerar relatórios visuais;
- A solução deve mostrar o processo afetado, as chaves de registo afetadas e os ficheiros afetados no ambiente do sistema operativo. A solução deve mostrar capturas de ecrã e vídeo da emulação de ficheiros maliciosos no ambiente de Sandbox. A solução deve ser capaz de registar a comunicação C&C do ficheiro BOT emulado;
- A solução deve ser gerida e apresentar os relatórios numa página web, juntamente – de forma integrada – com a solução de proteção de Email e de dispositivos móveis.

x) A solução tem de trabalhar e oferecer suporte em ambiente virtualizado –VDI Horizon do fabricante Omnissa.

2. Proteção de E-mail para M365

A proteção de email deve cumprir obrigatoriamente os seguintes requisitos mínimos:

Para proteção das contas de email e aplicações que estão incluídas na suite do Office365 será necessário considerar o licenciamento para 160 contas de uma

solução de proteção de email. Esta deve oferecer segurança contra ameaças cibernéticas à plataforma de email Office 365 da Microsoft.

A solução deve fornecer proteção contra os seguintes ataques cibernéticos:

- Deteção de Malware (em ficheiros anexados a e-mails, ficheiros enviados para aplicações de compartilhamento de ficheiros, etc.);
- Ataques de Phishing;
- Ataques de Spoofing;
- Ataques de Spam;
- Uso de aplicações SaaS não autorizadas, também conhecidos como Shadow IT;
- Login não autorizado (indicando uma aquisição de conta);
- A solução deve oferecer suporte à proteção de aplicações SaaS executando ações de segurança online, ou seja, intercetação de emails ou ações SaaS antes que eles cheguem às aplicações;
- A solução deve detetar anomalias no comportamento do utilizador, por exemplo, geolocalização (o utilizador que se ligou em locais distantes num curto período de tempo);
- A solução deve ser capaz de se integrar a um provedor de identidade (OKTA, Centrify, Azure AD, etc...) para evitar a aquisição de conta e fornecer uma camada de segurança de proteção de identidade adicional;
- A solução deve ser capaz de colocar em quarentena o e-mail/conteúdo malicioso e deve fornecer ao utilizador opções para remover ou restaurar os recursos em quarentena;
- A solução deve ter integração direta com a Microsoft, sem que seja necessário alterar os Mx Records;
- A solução deve fornecer relatórios ao administrador, indicando pelo menos: Resumo de eventos maliciosos detetados para cada aplicação compatível;
  - Detalhes de eventos maliciosos para cada aplicação separadamente;
  - Capacidade de exportar relatórios para ficheiros CSV;
  - Capacidade de criar relatórios PDF de estilo executivo para eventos por aplicações SaaS.
- A solução deve ser gerida e apresentar os relatórios numa página web, juntamente – de forma integrada – com a solução de proteção de Endpoint e de dispositivos móveis.

3. Proteção de dispositivos móveis

Para proteção dos dispositivos móveis será necessário considerar o licenciamento de uma solução de proteção de dispositivos móveis para 10 dispositivos, pelo menos, as seguintes funcionalidades:

- Deteção de Malware;
- Deteção de ataques de Phishing ou links maliciosos;

- Deteção de ameaças à rede;
- Deteção de alterações nas políticas do dispositivo;
- Impedir o acesso a links maliciosos conhecidos do próprio dispositivo;
- A solução deverá detetar vulnerabilidades conhecidas e explorações de dispositivos, bem como detetar dispositivos com Jailbreak e Rootkit
- A solução deve suportar dispositivos móveis Android e iOS;
- A consola de gestão deverá fornecer avaliações completas de risco do dispositivo (correlacionar dispositivo, aplicativo e atividade da rede);
- A consola de gestão deverá fornecer ao administrador de segurança um painel visível para mostrar o estado de risco dos dispositivos, o estado de proteção e os registos contínuos de eventos e alertas;
- A consola de gestão deverá fornecer opções de correção e mitigação no caso de ameaça real detetada;
- A solução deve ser gerida e apresentar os relatórios numa página web, juntamente – de forma integrada – com a solução de proteção de Endpoint e de email.

4. Serviço de Deteção e Resposta gerida (MDR)

O presente concurso deve incluir, para a totalidade dos dispositivos considerados (Endpoints equipamentos fixos e moveis) e da firewall atualmente em produção – do fabricante Check Point – um serviço de Deteção e resposta gerida, com, pelo menos, as seguintes funcionalidades:

1. Requisitos Gerais

a) O serviço de Managed Detection and Response (MDR) deve ser prestado pelo mesmo fabricante das soluções de segurança já implementadas, de Endpoints e Firewalls.

b) O serviço deve fornecer atualizações contínuas, ações de prevenção automatizadas, configurações ideais, recomendações e melhores práticas de forma a melhorar as defesas e prevenir ataques futuros.

c) O serviço deve ser prestado por especialistas no setor e por tecnologias baseadas em Inteligência Artificial para prevenir, monitorizar, detetar, investigar, responder e remediar ataques nos diferentes ambientes: Cloud, Network, Mobile, Endpoint, IoT e Email.

d) O serviço deve monitorizar toda a infraestrutura: Cloud, Network, Mobile, Endpoint, IoT e Email, 24 horas por dia, 7 dias por semana e tomar decisões informadas para impedir ataques e melhorar as defesas para evitar ataques futuros.

2. Componentes do serviço

O serviço deve fornecer acesso a um portal baseado em Cloud, com alertas fornecidos por e-mail, telefone e portal do cliente, acesso direto ao chat com a

equipa de resposta a incidentes e analistas, notificações de remediação: manuais ou automatizadas e SLA de 30 minutos para todos os eventos críticos.

➢ **Monitorização**

a) O serviço deve monitorizar as ameaças em toda a infraestrutura e correlacionar ameaças entre domínios com acesso imediato a especialistas em ameaças que validam os incidentes, emitem alertas e gerem os falsos positivos, utilizando plataformas de enriquecimento de inteligência em ameaças;

b) O serviço deve efetuar validação de alertas – removendo a taxa de falsos positivos ao monitorizar os dados e agregar, analisar e normalizar todos os logs em conjuntos de produtos utilizando dados forenses das diferentes plataformas, enriquecidos, normalizados e contextualizados, que permitem escalar e obter correlações.

➢ **Investigação**

a) O serviço deve investigar e pesquisar ameaças em toda a infraestrutura utilizando recursos avançados de deteção, utilizando Machine Learning (ML) e inteligência artificial (IA), manuais automatizados (automated playbooks) e Threat Hunting.

b) O serviço deve procurar atividades suspeitas, baseadas em comportamentos estranhos, e não apenas em alertas ou eventos acionados e examinar o ambiente e procurar proactivamente padrões de ataque.

➢ **Resposta**

a) O serviço deve efetuar a análise de Root Cause do comprometimento, revisão completa dos logs de auditoria, revisão das políticas, recomendações pós-comprometimento, análise de rede e dos principais indicadores de comprometimento;

b) O serviço deve proceder à identificação de sistemas comprometidos facultando um relatório completo da atividade do invasor, análise e revisão da ameaça;

c) O serviço deve fornecer um briefing completo às equipas técnicas e de gestão sobre o impacto do comprometimento, identificação do paciente zero e ajuda para restaurar os serviços;

d) O serviço deve tomar medidas automáticas e proativas para remediar um o ataque, usando um conjunto de playbooks/manuais e SLAs;

e) O serviço deve ser capaz de permitir interação em tempo real com os especialistas e analistas, ajudando na tomada de decisões após análise de um incidente;

f) O serviço deve efetuar notificação imediata de um incidente, com respostas automatizadas, e fornecer acesso em tempo real a especialistas e

analistas 24 horas por dia, 7 dias por semana, 365 dias por ano, com cobertura global em suporte em diferentes idiomas.

3. Equipa de resposta a incidentes (Incident Response Team)

a) O serviço deve incluir uma equipa de resposta a incidentes para ajudar na preparação, resposta e recuperação de qualquer violação de segurança com especialistas dedicados 24 horas por dia, 7 dias por semana;

b) O serviço deve responder em trinta (30) minutos após contacto com a equipa de resposta a incidentes e estabelecer uma teleconferência privada para avaliar e fazer a análise do evento. Os logs devem ser analisados e as recomendações e soluções documentadas no Relatório de Incidentes;

c) O serviço deve fornecer um relatório completo das circunstâncias do Incidente, que deve ser composto pelo seguinte:

- Visão geral do incidente e informações de resumo executivo;
- Descrição e comportamento do evento;
- Detalhes do registo das chamadas e trabalho realizado;
- Análise e comportamento de dados de sistema/rede;
- Recomendação e análise.

Lousã, 18 de dezembro de 2024

O Presidente da Câmara