

Aquisição de Sistema de Proteção Externo e Acesso Remoto

Caderno de Encargos

Aquisição de Sistema de Proteção Externo e Acesso Remoto

ÍNDICE

PARTE I – CLÁUSULAS GERAIS.....	4
CAPÍTULO I - DISPOSIÇÕES GERAIS.....	4
CLÁUSULA 1. ^a - OBJETO.....	4
CLÁUSULA 2. ^a - CONTRATO.....	4
CLÁUSULA 3. ^a - PRAZO.....	5
CAPÍTULO II - OBRIGAÇÕES CONTRATUAIS.....	5
SECÇÃO I -OBRIGAÇÕES DA ENTIDADE ADJUDICATÁRIA.....	5
<i>Subsecção I - Disposições gerais.....</i>	<i>5</i>
CLÁUSULA 4. ^a - OBRIGAÇÕES DA ENTIDADE ADJUDICATÁRIA.....	5
CLÁUSULA 5. ^a – CONFORMIDADE E OPERACIONALIDADE DOS BENS.....	6
CLÁUSULA 6. ^a – LOCAL DE ENTREGA DOS BENS E MONTAGEM.....	6
CLÁUSULA 7. ^a – PRAZO DE EXECUÇÃO.....	6
CLÁUSULA 8. ^a – INSPEÇÃO E TESTES.....	7
CLÁUSULA 9. ^a – INOPERACIONALIDADE, DEFEITOS OU DISCREPÂNCIAS.....	7
CLÁUSULA 10. ^a – ACEITAÇÃO DOS BENS.....	7
CLÁUSULA 11. ^a – GARANTIA DOS BENS.....	8
<i>Subsecção II - Dever de sigilo e proteção de dados.....</i>	<i>8</i>
CLÁUSULA 12. ^a - OBJETO DO DEVER DE SIGILO.....	8
CLÁUSULA 13. ^a – PRAZO DO DEVER DE SIGILO.....	9
CLÁUSULA 14. ^a – PROTEÇÃO DE DADOS.....	9
SECÇÃO II - OBRIGAÇÕES DA ENTIDADE ADJUDICANTE.....	9
CLÁUSULA 15. ^a – PREÇO BASE.....	9
CLÁUSULA 16. ^a - PREÇO CONTRATUAL.....	10
CLÁUSULA 17. ^a - CONDIÇÕES DE PAGAMENTO.....	10
CAPÍTULO III – PENALIDADES CONTRATUAIS.....	10
CLÁUSULA 18. ^a - PENALIDADES CONTRATUAIS.....	10
CLÁUSULA 19. ^a – FORÇA MAIOR.....	11
CAPÍTULO IV - CAUÇÃO E SEGUROS.....	12
CLÁUSULA 20. ^a - CAUÇÃO.....	12
CLÁUSULA 21. ^a – SEGUROS.....	12
CAPÍTULO V – GESTÃO DO CONTRATO.....	12
CLÁUSULA 22. ^a – SUPERVISÃO E CONTROLO.....	12
CAPÍTULO VI – RESOLUÇÃO DO CONTRATO.....	13
CLÁUSULA 23. ^a - RESOLUÇÃO POR PARTE DA ENTIDADE ADJUDICANTE.....	13
CLÁUSULA 24. ^a - RESOLUÇÃO POR PARTE DA ENTIDADE ADJUDICATÁRIA.....	13
CLÁUSULA 25. ^a – EXTINÇÃO DO CONTRATO.....	13
CLÁUSULA 26. ^a - FORO COMPETENTE.....	14
CAPÍTULO VII - DISPOSIÇÕES FINAIS.....	14
CLÁUSULA 27. ^a - COMUNICAÇÕES E NOTIFICAÇÕES.....	14
CLÁUSULA 28. ^a CONTAGEM DOS PRAZOS.....	14
<i>Cláusula 29.^a – Subcontratação e cessão da posição contratual.....</i>	<i>14</i>
CLÁUSULA 30. ^a - LEGISLAÇÃO APLICÁVEL.....	14
PARTE II - CLÁUSULAS RELATIVAS AOS ASPETOS DA EXECUÇÃO DO CONTRATO.....	15
CLÁUSULA 31. ^a - ASPETOS DA EXECUÇÃO DO CONTRATO NÃO SUBMETIDOS À CONCORRÊNCIA.....	15
PARTE III – CLÁUSULAS TÉCNICAS - ESPECIFICAÇÕES.....	16

Aquisição de Sistema de Proteção Externo e Acesso Remoto

CLÁUSULA 1. ^a - INTRODUÇÃO.....	16
CLÁUSULA 2. ^a - REQUISITOS GERAIS.....	16
CLÁUSULA 3. ^a ESPECIFICAÇÕES MÍNIMAS.....	17
FIREWALL – QUANTIDADE 1.....	17

Aquisição de Sistema de Proteção Externo e Acesso Remoto PARTE I – CLÁUSULAS GERAIS

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 ***Aquisição de Sistema de Proteção Externo e Acesso Remoto à Rede Informática Municipal***, a efetuar em conformidade com:

- a) Código dos Contratos Públicos;
- b) Documentos do Processo de Concurso;
- c) As normas técnicas, profissionais e deontológicas inerentes à atividade.

Cláusula 2.ª - Contrato

1 - O contrato é composto pelo respetivo clausulado contratual e os seus anexos.

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

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

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

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

5 - As normas constantes do Código dos Contratos Públicos relativas às fases de formação e de execução do contrato prevalecem sobre quaisquer disposições das peças do procedimento em elas desconformes.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

Cláusula 3.^a - Prazo

O contrato mantém-se em vigor até à entrega dos bens objeto do contrato e à verificação técnica do seu funcionamento, em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

Capítulo II - Obrigações contratuais

Secção I -Obrigações da entidade adjudicatária

Subsecção I - Disposições gerais

Cláusula 4.^a - Obrigações da entidade adjudicatária

1 - Sem prejuízo de outras obrigações previstas na legislação aplicável, no caderno de encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para a entidade adjudicatária as seguintes obrigações principais:

- a) Entregar os bens no prazo definido e em condições de utilização para os fins a que se destinam e de acordo com o estipulado em legislação própria;
- b) Manter atualizados todos os documentos de habilitação;
- c) Comunicar antecipadamente os factos que tornem total ou parcialmente impossível a prestação dos serviços objeto do presente procedimento, ou o cumprimento de qualquer outras das suas obrigações, logo que deles tomem conhecimento nos termos do contrato celebrado com a entidade adjudicante;
- d) Manter o sigilo e garantir a confidencialidade.

2 - A título acessório, a entidade adjudicatária fica ainda obrigada, designadamente, a recorrer a todos os meios humanos e materiais que sejam necessários e adequados ao fornecimento dos bens, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

3 - São da responsabilidade da entidade adjudicatária quaisquer encargos decorrentes da utilização de patentes, marcas registadas ou licenças. E, caso se verifique infração, a entidade adjudicatária terá de indemnizar em todas despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar, seja a que título for.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

Cláusula 5.ª – Conformidade e operacionalidade dos bens

- 1 - A entidade adjudicatária obriga-se a entregar os bens objeto do contrato com as características, especificações e requisitos técnicos adequados, **conforme definido na Parte III – CLÁUSULAS TÉCNICAS – ESPECIFICAÇÕES, do presente caderno de encargos.**
- 2 - A entidade adjudicatária obriga-se a disponibilizar, simultaneamente com a entrega dos bens objeto do contrato, todos os documentos em língua portuguesa/inglesa, que sejam necessários para a boa e integral utilização ou funcionamento daqueles.
- 3 - Com a entrega dos bens objeto do contrato, ocorre a transferência da posse e da propriedade daqueles para a entidade adjudicante, bem como do risco de deterioração ou perecimento dos mesmos, sem prejuízo das obrigações de garantia que impendem sobre a entidade adjudicatária.
- 4 - Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local de entrega são da responsabilidade da entidade adjudicatária.
- 5 - A entidade adjudicatária é responsável perante a entidade adjudicante por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que o bem é entregue.

Clausula 6.ª – Local de entrega dos bens e Montagem

Os bens objeto do presente caderno de encargos devem ser entregues no Complexo Logístico de Óbidos, sito Estrada da Arregaça n. 8, Pinhal, 2510-170 Óbidos, **no prazo proposto na sua proposta, em respeito pelo limite máximo estabelecido no presente caderno de encargos.**

Clausula 7.ª – Prazo de execução

- 1 - A entidade adjudicatária obriga-se a proceder à entrega de todos os bens objeto do contrato no prazo máximo de **90 (noventa) dias**, a contar da data da outorga do contrato e efetiva publicação no portal dos contratos públicos, em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.
- 2 - O presente contrato terminará quando se verificar uma das seguintes situações:
 - a) Atingido o prazo;
 - b) Celebração de Acordo de Revogação entre as partes.
- 3 - O disposto na presente cláusula não interfere com os prazos de garantia estipulados nas cláusulas seguintes.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

Cláusula 8.ª – Inspeção e testes

- 1 - Efetuada a entrega dos bens, a entidade adjudicante, por si ou através de terceiros por si designados, procede, no prazo de 24 horas, à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar, respetivamente, se estes correspondem às quantidades/solicitações efetuadas.
- 2 - É realizada uma Inspeção Técnica, para que sejam aferidos se os bens fornecidos se encontram em perfeitas condições de aceitação por parte da entidade adjudicante.
- 3 - Durante a fase de realização de testes, a entidade adjudicatária deve prestar toda a cooperação e todos os esclarecimentos necessários.

Cláusula 9.ª – Inoperacionalidade, defeitos ou discrepâncias

- 1 - No caso da inspeção prevista na cláusula anterior não comprovar a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente caderno de encargos, a entidade adjudicante deve disso informar, por escrito, a entidade adjudicatária.
- 2 - No caso previsto no número anterior, a entidade adjudicatária deve proceder, à sua custa e no prazo razoável que for determinado pela entidade adjudicante, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
- 3 - Após a realização das reparações ou substituições necessárias pela entidade adjudicatária, no prazo respetivo, a entidade adjudicante procede à realização de nova inspeção, nos termos da cláusula anterior.

Cláusula 10.ª – Aceitação dos bens

- 1 - Caso a inspeção a que se refere a cláusula nona comprove a total operacionalidade dos bens, objeto do contrato, bem como a sua conformidade com as exigências legais, e nela não seja detectada quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente caderno de encargos, deve ser emitido, no prazo máximo de 10 dias úteis, a contar do final da inspeção um Auto de Receção, assinado pelos representantes de ambas as partes.
- 2 - Com a entrega dos bens objeto do contrato, ocorre a transferência da posse e da propriedade daqueles para a entidade adjudicante, bem como do risco de deterioração ou perecimento dos mesmos, sem prejuízo das obrigações de garantia que impendem sobre a entidade adjudicatária.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

3 - A assinatura do Auto a que se refere o n.º 1 não implica a aceitação de eventuais defeitos ou de discrepâncias dos equipamentos objeto do contrato com as exigências legais ou com as características, especificações e requisitos técnicos previstos no presente caderno de encargos.

Cláusula 11.ª – Garantia dos bens

1 - Nos termos da presente cláusula e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, a entidade adjudicatária garante os mesmos, pelo prazo indicado na sua proposta, a contar da data da entrega dos bens contra quaisquer defeitos ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos dos mesmos, que se revelem a partir da respetiva aceitação.

2 - A garantia prevista no número anterior abrange:

- a) A substituição das peças, componentes ou bens defeituosos ou discrepantes;
- b) A desmontagem de peças, componentes ou bens defeituosos ou discrepantes;
- c) O fornecimento, a montagem ou instalação das peças, componentes ou bens reparados ou substituídos;
- d) A deslocação ao local da instalação/entrega;
- e) A mão-de-obra.

3 - A substituição prevista na presente cláusula deve ser realizada prazo de 24 horas e sem grave conveniente para a entidade adjudicante, tendo em conta a natureza do bem e o fim a que se destina.

4 - **A garantia mínima aceite é de 3 anos.**

Subsecção II - Dever de sigilo e proteção de dados

Cláusula 12.ª - Objeto do dever de sigilo

1 - A entidade adjudicatária deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.

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

Aquisição de Sistema de Proteção Externo e Acesso Remoto

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

Cláusula 13.ª – Prazo do dever de sigilo

O dever do sigilo mantém-se em vigor até ao termo do prazo de cinco anos a contar do cumprimento ou da cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Cláusula 14.ª – Proteção de dados

1 - O artigo 6.º do Regulamento Geral sobre a Proteção de Dados indica as situações em que o tratamento de dados é lícito, designadamente quando *“o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré – contratuais a pedido do titular de dados”, e “o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito”*.

2 - Sempre que sejam remetidos dados pessoais, nomeadamente em relação à equipa de trabalho proposta, os mesmos devam ser acompanhados de declaração de consentimento para o tratamento dos dados para esta finalidade, por parte dos seus titulares.

3 - Nos termos da alínea v) do n.º 1 do artigo 4.º da Portaria n.º 57/2018, de 26 de fevereiro, a publicitação do contrato, é feita no Portal BASE, incluindo anexos e aditamentos, **com exceção** das informações que se relacionem com segredos de natureza comercial, industrial ou outra e das **informações respeitantes a dados pessoais**.

Secção II - Obrigações da entidade adjudicante

Cláusula 15.ª – Preço base

1 - Nos termos do n.º 3 do artigo 47.º do CCP, o preço base fixado para o presente procedimento é de 12.058,00€ (doze mil e cinquenta e oito euros), valor ao qual acresce o IVA à taxa legal em vigor.

2 - Nos termos da alínea d) do n.º 2 do artigo 70.º do CCP são excluídas as propostas que apresentem preço contratual superior ao preço base.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

Cláusula 16.^a - Preço contratual

- 1 - Pelo fornecimento dos bens objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a entidade adjudicante deve pagar à entidade adjudicatária o preço da proposta adjudicada, acrescido de IVA à taxa legal em vigor.
- 2 - O preço contratual apresentado pelo concorrente contém todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, incluindo as despesas de alojamento, alimentação e deslocação dos seus meios humanos, bem como todas as despesas de aquisição, transporte, armazenamento e manutenção dos seus meios materiais.
- 3 - **Durante o contrato não haverá lugar a revisão de preços.**

Cláusula 17.^a - Condições de pagamento

- 1 - A quantia devida pela entidade adjudicante, nos termos da cláusula anterior, deve ser paga no **prazo máximo de 30 dias** após a receção desta das respetivas fatura(s), a(s) qual(ais) deve(m) ser emitida(s) após o fornecimento dos bens **e devem fazer sempre referência ao número de contrato e de compromisso.**
- 2 - Em caso de discordância, por parte da entidade adjudicante, quanto aos valores indicado(s) na(s) fatura(s), deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
- 3 - Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas através de transferência bancária.

Capítulo III – Penalidades contratuais

Cláusula 18.^a - Penalidades contratuais

- 1 - No caso de incumprimento dos prazos fixados no contrato e por causa imputável à entidade adjudicatária, pode ser aplicada uma penalidade, calculada de acordo com a seguinte fórmula:

$$P = V \cdot A / 500$$

Em que:

- **P:** corresponde ao montante da penalidade;
- **V:** é Igual ao valor do fornecimento; e
- **A:** é o número de dias em atraso.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

2 - A competência para decidir a aplicação da penalidade referida no número anterior é do Presidente da Câmara Municipal de Óbidos.

Cláusula 19.^a – Força Maior

1 - Não podem ser impostas penalidade à entidade adjudicatária, nem é havida com incumprimento, a não realização pontual das prestações contratuais a cargos de qualquer das partes que resulte de caso 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.

2 - Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greve, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

3 - Não constituem força maior, designadamente:

- a) Circunstâncias que não constituam força maior para os subcontratados da entidade adjudicatária, na parte em que intervenham;
- b) Greves ou conflitos laborais limitados às sociedades da entidade adjudicatária ou a grupo de sociedades em que esta se integre, bem como as sociedades ou grupos de sociedades dos seus subcontratados;
- c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de uma forma resultantes do incumprimento pela entidade adjudicatária de deveres ou ónus que sobre ela recaiam;
- d) Manifestações populares devidas ao incumprimento pela entidade adjudicatária de normas legais;
- e) Incêndios ou inundações com origem nas instalações da entidade adjudicatária 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 da entidade adjudicatária não devidas a sabotagem;
- g) Eventos que estejam ou devam estar cobertos por seguros;

4 - A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

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

Capítulo IV - Caução e seguros

Cláusula 20.^a - Caução

Considera-se que face ao valor, preço contratual inferior a 500.000,00€, não deve ser exigida caução nem deve proceder-se à retenção nos pagamentos, prevista no n.º 3 do artigo 88.º do Código dos Contratos Públicos.

Cláusula 21.^a – Seguros

- 1 - É da responsabilidade da entidade adjudicatária a cobertura, através de um contrato de seguro, da atividade que exerce.
- 2 - A entidade adjudicante pode, sempre que entender conveniente, exigir prova documental da celebração do contrato de seguro, devendo o adjudicatário fornecê-la no prazo um dia útil.

Capítulo V – Gestão do contrato

Cláusula 22.^a – Supervisão e controlo

- 1 - A identificação dos gestores do contrato designados pela entidade adjudicante, nos termos do artigo 290.º-A do Código dos Contratos Públicos fará parte do clausulado contratual.
- 2 - O adjudicatário deverá nomear um técnico que o represente em tudo o que concerne ao contrato, o qual servirá de interlocutor entre as partes para a resolução e/ou conhecimento de quaisquer assuntos inerentes ao objeto do contrato.
- 3 - Para efeitos do cumprimento do exercício das funções de gestão do contrato o adjudicatário deverá disponibilizar os contactos telefónicos e de endereço eletrónico do representante por si nomeado.
- 4 - O adjudicatário está sujeito à supervisão da execução do contrato, a qual será assegurada pelo gestor de contrato.
- 5 - Caso se verifiquem situações anómalas com base nos relatórios emitidos pelo gestor de contrato, será o adjudicatário notificado para regularização imediata das mesmas.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

Capítulo VI – Resolução do contrato

Cláusula 23.^a - Resolução por parte da entidade adjudicante

1 - Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a entidade adjudicante pode resolver o contrato, a título sancionatório, no caso da entidade adjudicatária violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente nos seguintes casos:

- a) Atraso, total ou parcial, na entrega dos bens objeto do contrato superior a cinco dias ou declaração escrita do fornecedor de que o atraso em determinada entrega excederá esse prazo;
- b) Fornecimento de bens com características técnicas diferentes.

2 - O direito de resolução referido no número anterior exerce-se mediante declaração enviada à entidade adjudicatária.

Cláusula 24.^a - Resolução por parte da entidade adjudicatária

1 - Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a entidade adjudicatária pode resolver o contrato quando qualquer montante que lhe seja devido esteja em dívida há mais de seis meses ou o montante em dívida exceda 25% do preço contratual, excluindo juros.

2 - O direito de resolução é exercido por via judicial.

3 - Nos casos previstos no n.º 1, o direito de resolução pode ser exercido mediante declaração enviada à entidade adjudicante, que produz efeitos 30 dias após a receção dessa declaração, salvo se o este último cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.

4 - A resolução do contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pelo fornecedor, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do Código dos Contratos Públicos.

Cláusula 25.^a – Extinção do Contrato

1 - O direito de extinguir o contrato poderá ser exercido por ambas as partes, nos termos previstos na Parte III do CCP.

2 - Para efeitos do disposto no número anterior, considera-se incumprimento definitivo, quando houver atraso no fornecimento, por um período superior a 5 dias úteis.

Aquisição de Sistema de Proteção Externo e Acesso Remoto

Cláusula 26.ª - Foro Competente

- 1 - Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Leiria, com expressa renúncia a qualquer outro.
- 2 - As partes podem derogar o disposto no número anterior por acordo escrito, decidindo submeter à arbitragem algum litígio específico.

Capítulo VII - Disposições finais

Cláusula 27.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 escritas e redigidas em português, conforme previsto no Código dos Contratos Públicos, através de correio eletrónico ou de outro meio de transmissão escrita e eletrónica de dados, ou por via postal, por meio de carta registada ou de carta registada com aviso de receção.
- 2 - Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 28.ª Contagem dos prazos

Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.

Cláusula 29.ª – Subcontratação e cessão da posição contratual

A subcontratação pelo adjudicatário e a cessão da posição contratual por qualquer uma das partes depende da autorização da outra, nos termos do Código dos Contratos Públicos.

Cláusula 30.ª - Legislação aplicável

- 1 - A tudo o que não esteja especialmente previsto no presente caderno de encargos, aplica-se o regime consagrado no Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual e demais legislação aplicável.
- 2 - Em respeito pelo n.º 2 do artigo 1.º-A do Código dos Contratos Públicos, o adjudicatário compromete-se a executar o contrato em respeito pelas normas aplicáveis em vigor em matéria social, laboral, ambiental, de igualdade de género e de prevenção e combate à corrupção, decorrentes do direito internacional, europeu, nacional ou regional.

Aquisição de Sistema de Proteção Externo e Acesso Remoto
PARTE II - CLÁUSULAS RELATIVAS AOS ASPETOS DA EXECUÇÃO DO
CONTRATO

Cláusula 31.^a - Aspectos da Execução do Contrato não Submetidos à Concorrência

Sem prejuízo dos limites resultantes das vinculações legais ou regulamentares aplicáveis, são aqui fixados, para cada um dos aspetos da execução do contrato não submetidos à concorrência, **os limites máximos/mínimos** a que a proposta está vinculada, determinando-se, consequentemente, a exclusão se os termos ou condições os ultrapassem:

a) Preço base

Limite máximo: 12.058,00€, acrescido de IVA à taxa legal em vigor.

b) Prazo de garantia/suporte dos bens;

Limite mínimo: 3 anos

c) Prazo de entrega

Limite máximo: 90 dias

Todos os restantes aspetos constantes do caderno de encargos.

Aquisição de sistema de proteção de rede e acesso remoto

PARTE III – CLÁUSULAS TÉCNICAS - ESPECIFICAÇÕES

Cláusula 1.ª - INTRODUÇÃO

Este documento visa caracterizar as soluções tecnológicas a adquirir para o Centro de Dados do Município de Óbidos sito no edifício dos Paços do Concelho.

Pretende-se o fornecimento de uma appliance NGFW de proteção periférica de rede com capacidade de inspeção e filtragem do tráfego, acessos VPN, reverse proxy de múltiplos sites através de um IP.

Cláusula 2.ª - REQUISITOS GERAIS

As propostas a apresentar têm de indicar explicitamente o período de garantia/suporte e de fornecimento de atualizações do software/firmware.

Considera-se manutenção, o conjunto de operações efetuadas pela entidade adjudicatária tendentes a repor e manter em boas condições de funcionamento a solução proposta, durante a vigência da Garantia/Suporte.

A reparação de hardware terá lugar sempre no local das instalações da entidade adjudicante, podendo ser retirado o equipamento quando não for viável a sua reparação no local, devendo neste caso ser substituído por outro idêntico ou superior, tendo em especial consideração a salvaguarda da informação e bom funcionamento do sistema global.

A entidade adjudicatária deve assegurar a continuidade de fabrico e do fornecimento de todas as peças, componentes ou equipamentos que integram os bens fornecidos no âmbito do contrato pelo prazo de 3 anos a contar da assinatura do auto de receção respetivo.

Todos os componentes da solução deverão ser novos e os sistemas com componentes reparados ou reconicionados não são aceites. **Deverá ser apresentada declaração da marca, atestando as condições dos equipamentos como novos.**

Os equipamentos propostos têm de contemplar suporte e garantia mínima de 3 anos, com atendimento 24/7, com nível de assistência no dia útil seguinte.

Há ainda que garantir o fornecimento de todas as atualizações e updates dos softwares / firmwares para as funcionalidades propostas, por um período de 3 anos.

Aquisição de sistema de proteção de rede e acesso remoto
Deverá ser apresentada declaração de fabricante atestando que o equipamento proposto não se encontra em final de vida (EOL).

Cláusula 3.^a ESPECIFICAÇÕES MÍNIMAS

FIREWALL – Quantidade 1

Identificação das características mínimas da Firewall a fornecer

Integração com redes de comunicações

As seguintes funcionalidades deverão ser suportadas:

- Servidor de DHCP, NTP e DNS incluído
- Funcionalidade de DNS Proxy
- Múltiplos modos de configuração de interfaces:
 - Sniffer
 - Agregação de portas (802.3ad)
 - Loopback
 - VLANs (802.1Q e trunk)
 - Software switch
- Routing estáticos e baseado em políticas (PBR - Policy Based Routing)
- SD-WAN
 - Application Awareness & Steering
 - Dynamic WAN Path Controller
 - NGFW with SSL Inspection
 - Dynamic failover times
 - Secure VPN Overlays
 - Single Management Console for Security & SD-WAN
 - Zero-touch provisioning
- Balanceamento e redundância de múltiplos links;
- Suporte para protocolos de routing dinâmico: RIPv1, RIPv2, RIPv6, OSPFv2 e OSPFv3, ISIS, BGP4+
- Suporte de tráfego multicast: PIM, sparse e dense mode
- Routing baseado em conteúdos: WCCP e ICAP
- Proxy explícito com suporte PAC e WPAD
- Suporte de IPv6
 - Gestão por IPv6
 - Protocolos de routing dinâmico com suporte para IPv6
 - Tunneling de IPv6
 - Processamento firewall e UTM de IPv6
 - NAT64

Aquisição de sistema de proteção de rede e acesso remoto

- NAT46
- VPN IPSec IPv6
- Suporte Dual Stack IPv4 e IPv6 em simultâneo
- Suporte VXLAN
- Controlador Switching integrado
- Virtualização da solução em contextos.

Identificação de utilizadores e dispositivos

As seguintes funcionalidades deverão ser suportadas:

- Base de dados local de utilizadores;
- Autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+
- Sistema de Single Sign-on de utilizadores:
 - Windows AD
 - Kerberos
 - Citrix e Terminal Server
 - Radius (accounting message)
 - Autenticação de utilizadores no acesso (802.1x, portal cativo)
- PKI e certificados:
 - Certificados X.509
 - Suporte SCEP
 - Criação de Certificate Signing Request (CSR)
 - Auto Renovação de certificados antes da data de expiração
 - Suporte OCSP
- Autenticação de 2 fatores
 - Servidor integrado de autenticação por tokens físicos, tokens por software e SMS
 - Integração com terceiras partes
- Identificação de dispositivos
 - Reconhecimento de dispositivo e sistema operativo
 - Classificação automática de dispositivos
 - Gestão de inventário de dispositivos
 - Suporte de autenticação e bypass feitos por MAC Address
- Implementação de políticas de segurança com base em utilizador ou dispositivos

Firewall

As seguintes funcionalidades deverão ser suportadas:

- Modos de operação NAT/route e transparente/bridge
- Agendamento de políticas: recorrentes ou apenas uma vez

Aquisição de sistema de proteção de rede e acesso remoto

- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, RTSP, SIP, TFTP, GTP-C, GTP-U, GTP-B, TNS (Oracle)
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pinhole
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por pares de interfaces
- Definição de objetos para utilização em políticas incluindo: pré-definidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia e FQDN
- Utilização de objetos de serviços Internet (ex: Azure, Office365) com atualização automática das gamas de IP e portos.
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT, STUN
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ)
- Processamento de tráfego de firewall IP4 e IPv6 feito em processador dedicado e desenhado para o efeito.

VPN

As seguintes funcionalidades deverão ser suportadas:

- IPSEC VPN:
 - Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico
 - Mecanismos de autenticação: certificados ou pre-shared key
 - IPSEC Phase 1 mode: aggressive e main (ID protection) mode
 - Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup
 - Suporte de IKEv1, IKEv2 (RFC 4306)
 - Suporte de IKE mode configuration (como servidor ou cliente), DHCP over IPSEC
 - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
 - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
 - Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
 - Suporte XAuth como cliente ou servidor
 - XAuth para clientes dialup: Server type option (PAP, CHAP, Auto), NAT Traversal option
 - Duração configurável da chave de encriptação IKE e da frequência do NAT traversal keepalive
 - Dead peer detection
 - Replay detection
 - Autokey keep-alive na Phase 2 SA

Aquisição de sistema de proteção de rede e acesso remoto

- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente
- Suporte ADVPN
- Suporte de configuração full-mesh VPN One-click
- Opções de configuração de VPNs IPsec: baseado em routing(route-based) ou baseado em políticas (policy-based)
- VPNs SSL
 - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente
 - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
 - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos
 - Gestão de atalhos (bookmarks) pessoais
 - Gestão de utilizadores concorrentes
 - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
 - Suporte de VPN SSL em modo web:
 - Para clientes remotos equipamentos apenas com um browser web
 - Disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix
 - Suporte para VPN SSL em modo túnel:
 - Para acesso a partir de computadores que necessitam utilizar qualquer software do tipo cliente-servidor.
 - Disponível para MAC OSX, Windows, IOS, Android e Windows Mobile
 - Suporte para VPN SSL em modo port-forwarding:
 - Utiliza uma applet Java para permitir uma utilização alargada de aplicações do tipo cliente-servidor
 - Validação da integridade do dispositivo cliente e do sistema operativo;
 - Opção para limpeza de cache aquando do termino da sessão VPN SSL
 - Opção de utilização de desktop virtual que permite isolar a sessão VPN SSL no ambiente de trabalho do computador cliente
- Monitorização de VPNs IPsec e SSL com diferentes níveis de detalhe
- Suporte para outras VPNs como L2TP (modo cliente e servidor), L2TP over IPsec, PPTP e GRE over IPsec
- Processamento de tráfego de IPsec feito em processador dedicado e desenhado para o efeito.

IPS - Detecção e prevenção de intrusões

As seguintes funcionalidades deverão ser suportadas:

- Suporte de IPS com mais de 12000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (push ou pull),

Aquisição de sistema de proteção de rede e acesso remoto

integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados

- Diferentes ações de IPS: monitorizar, bloquear, apagar sessão ou quarentena do IP de ataque com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS específicas com base em IPs
- Proteção DoS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer
- Possibilidade de criar novas assinaturas

Controlo de aplicações

As seguintes funcionalidades deverão ser suportadas:

- Detecção de mais de 3100 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas
- Controlo avançado de aplicações de IM e Facebook
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco, e/ou protocolo)
- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade
- Detecção de aplicações mesmo dentro de ligações proxy
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização ou aplicação de gestão de largura de banda
- Inspeção SSL (suporte TLS 1.3)

Proteção contra ameaças

As seguintes funcionalidades deverão ser suportadas:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, web filtering e DLP
- Capacidade de descriptação de sessões SSL com cópia de tráfego descriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Detecção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)

Aquisição de sistema de proteção de rede e acesso remoto

- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP
- Suporte de anti-vírus em modo proxy, incluindo:
 - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
 - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
 - Listas de ficheiros autorizados/negados
 - Opção de análise heurística
- Integração com solução de Sandboxing (cloud ou on-premises)
- Detecção de sites WEB (web filtering):
 - Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS)
 - Possibilidade de definição manual de filtros de sites com base em URL, conteúdo web e cabeçalho MIME
 - Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias
 - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
 - Deverá ser possível ter a opção para activar as seguintes funcionalidades:
 - Filtrar Java Applet, ActiveX e/ou cookies
 - Bloquear HTTP Post
 - Registar termos/palavras utilizados nas pesquisas em motores de busca
 - Identificar imagens pelo URL
 - Bloquear redirect de HTTP de acordo com a categoria
 - Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
 - Definição de quotas de utilização WEB com base em categorias
 - Definição de categorias customizadas e sobreposição de categorização
 - Mecanismos de exceção à utilização de perfis pré-definidos;
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Prevenção e proteção de fugas de informação - DLP
- Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Possibilidade de executar as acções: registar, bloquear, quarentena de utilizador/IP/Interface
- Filtros pré-difinidos incluindo cartões de crédito e número de segurança Social
- Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP

Aquisição de sistema de proteção de rede e acesso remoto

- Opções de filtro disponíveis: tipo de ficheiro, watermark, conteúdo e deteção de encriptação
- Utilização de mecanismos de DLP watermarking , com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
- Fingerprinting de ficheiros
- Armazenamento de ficheiros detetados para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB
- Integração nativa com plataformas externas de filtragem de email, sandbox e WAF
- Feeds de ameaças por Domain Name e/ou IP Address

Controlo de Endpoints

- Visibilidade centralizada sobre diversos elementos de rede, nomeadamente:
 - Vulnerabilidades nos endpoints
 - Indicadores de compromisso

Alta disponibilidade

As seguintes funcionalidades deverão ser suportadas:

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover)
 - Monitorização de portas e links (locais e remotos)
 - Sem perda de sessões
 - Failover em menos de 1 segundo
 - Notificações de eventos de failover
- Diferentes opções de arquitetura
 - HA com agregação de links
 - Full mesh HA
 - Suporte para HA com equipamentos geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou
- Cluster geográfico

Administração, Monitorização e Diagnósticos

As seguintes funcionalidades deverão ser suportadas:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica

Aquisição de sistema de proteção de rede e acesso remoto

- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: português, inglês, espanhol, francês, japonês, chinês simplificado, chinês tradicional e Coreano
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.
- Integração com outras soluções (externas) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções Openstack, VMWare NSX
- Automação, por exemplo para colocar em Quarentena um dispositivo com um elevado Indicador de Compromisso.

Registo de eventos e relatórios

As seguintes funcionalidades deverão ser suportadas:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória, disco rígido local, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195)
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless
- Opção para registo parcial ou completo de eventos
- Resolução de nomes de endereços IPs e protocolos
- Mecanismo nativo de visualização de eventos de forma estatística, com ferramentas de busca e drill-down disponível através de recurso com web browser.

Aquisição de sistema de proteção de rede e acesso remoto

Certificações

O equipamento deverá ter as seguintes certificações:

- Certificações ICSA de Firewall, SSL VPN, IPSEC VPN, AV e IPS
- FIPS 140-2 Validated (quando a operar em FIPS mode)
- USGv6 IPv6 Certified
- Licenciamento de todas as funcionalidades tais como GAV, IPS, Content Filtering, Application Control e Sandboxing, entre outras, para 3 anos e sem limite de utilizadores.
Este licenciamento deve ser transversal ao hardware e aplicável nomeadamente a todas as unidades físicas em cluster de garantia de políticas de alta disponibilidade;
- Licenciamento perpétuo para ipv6;
- Todo o licenciamento e garantia por um período mínimo de 3 anos (24h/7 dias por semana), incluindo atualizações de software, assinaturas e firmware.
- Em caso de substituição de hardware o período não deverá ultrapassar 24h (dias úteis).