



“Aquisição de solução de segurança para perímetro público”

Consulta Prévia N.º 31/2022

Consulta Prévia nos termos da alínea c) do n.º 1 do artigo 20.º do Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua atual redação
(doravante designado por CCP))

TÍTULO I – CLÁUSULAS GERAIS

CAPÍTULO I – Disposições Gerais

Cláusula 1.^a

Objeto

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar entre o Município de Mira, adiante abreviadamente designado por Entidade Adjudicante, na sequência do procedimento pré-contratual de consulta prévia nos termos da alínea c) do n.º 1 do artigo 20.º do Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, que tem por objeto a aquisição de solução de segurança para perímetro público, CPV 30230000-0 Equipamento Informático.
2. As características, as especificações e os requisitos técnicos do bem objeto do contrato são os que constam na Cláusula 31.^a - Cláusulas Técnicas do presente caderno de encargos.

Cláusula 2.^a

Contrato

1. Nos termos do disposto no n.º 1 do art.º 94º do Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, doravante designado por CCP, o contrato será reduzido a escrito e composto pelo respetivo clausulado contratual e seus anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
 - a) Os suprimentos dos erros e omissões do Caderno de Encargos identificados, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) Os esclarecimentos e as retificações relativas ao Caderno de Encargos;
 - c) O presente Caderno de Encargos;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos sobre a proposta vencedora 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 quando os 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.

Cláusula 3.ª

Preço Base

1. Pelo fornecimento do bem objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o preço base é de 30.000,00€ (trinta mil euros), valor a acrescer de IVA à taxa legal em vigor, se legalmente devido, correspondendo ao preço máximo que a entidade adjudicante se dispõe a pagar, pela execução de todas as prestações que constituem o objeto do presente contrato.
2. Nos termos da alínea d), n.º 2, artigo 70.º do CCP, são excluídas as propostas cujos preços sejam superiores aos preços base referidos nos números anteriores.
3. Os preços referidos nos números anteriores incluem todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, incluindo eventuais despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, recursos humanos, fiscalidade, cotações, propostas metodológicas e/ou reformulação das mesmas, bem como quaisquer encargos decorrentes da utilização de direitos de propriedade industrial ou intelectual, seguros ou de quaisquer licenças.

Cláusula 4.ª

Duração do Contrato

1. O contrato a celebrar mantém-se em vigor até à conclusão de todas as ações previstas em conformidade os prazos de execução previstos nas especificações técnicas previstas na Parte II do presente caderno de encargos, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.
2. Sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato, o prazo de entrega do bem objeto do presente procedimento é de 30

(trinta) dias a contar da data da celebração do contrato, conforme previsto nas especificações técnicas do presente caderno de encargos.

CAPÍTULO II

Obrigações Contratuais

Secção I – Obrigações do Adjudicatário

Cláusula 5.ª

Obrigações principais do Adjudicatário

1. Sem prejuízo de outras obrigações prevista na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o prestador de serviços as seguintes obrigações principais:
 - a) Proceder à entrega do bem, conforme especificações técnicas constantes do presente caderno de encargos;
 - b) Obrigação de garantia dos bens;
 - c) Obrigação de continuidade de fabrico dos bens;
 - d) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato.
 - e) Cumprir as orientações e diretrizes técnicas do contratante público relativamente aos procedimentos e ações a considerar, nos termos da legislação aplicável;
2. A título acessório, o fornecedor fica ainda obrigado, designadamente, a realizar todas as tarefas solicitadas pela entidade adjudicante e abrangidas pelo contrato a celebrar, com a diligência e qualidade requeridas pelo tipo de trabalho em causa mesmo que para tal tenha de recorrer aos meios humanos, materiais e informáticos que entenda necessários e adequados ao fornecimento de eletricidade e à complexa execução das tarefas ao seu cargo.

Cláusula 6.ª

Conformidade e operacionalidade dos bens

1. O fornecedor obriga-se a entregar onde o contraente público informar os bens objeto do contrato com as características, especificações e requisitos técnicos previstos no presente caderno de encargos, e de acordo com a proposta adjudicada;
2. Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento;
3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens;
4. O fornecedor é responsável perante a entidade adjudicante por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Cláusula 7.ª

Entrega dos bens objeto do contrato

1. O fornecedor obriga-se a entregar os bens objeto no local a designar pelo Município de Mira do contrato com as características, especificações e requisitos técnicos previstos no presente caderno de encargos, e de acordo com a proposta adjudicada.
2. Para efeitos do disposto no número anterior, o fornecedor obriga-se a fornecer o bem objeto do contrato, no escrupuloso cumprimento deste caderno de encargos, e da proposta adjudicada, no prazo máximo de 60 dias, contado da data de adjudicação.

Cláusula 8.ª

Inspeção e trabalhos/testes

1. Efetuada a entrega e instalação dos bens objeto do contrato, o Município de Mira, por si, ou através de terceira entidade por ela indicada, procede, no prazo máximo de 15 (quinze) dias de calendário, a contar da respetiva entrega dos bens, à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar se os mesmos correspondem quer às quantidades estabelecidas, quer às características, especificações e requisitos previstos, em especial técnicos e operacionais, nos termos e condições das cláusulas técnicas do presente caderno de encargos, que

- dele fazem parte integrante, e de acordo com a proposta adjudicada, bem como outros requisitos exigidos por lei.
2. A inspeção qualitativa a que se refere o número anterior incide sobre os bens, sendo efetuada através da verificação das características, especificações e requisitos mínimos previstos nas cláusulas técnicas do presente caderno de encargos, mediante a realização dos trabalhos e ou testes definidos para o efeito.
 3. Durante a fase de realização dos trabalhos e ou testes, o fornecedor deve prestar ao Município de Mira toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a realização daqueles, através de pessoas devidamente credenciadas para o efeito, assegurando sempre, porém, tal acompanhamento por técnicos devidamente habilitados e competentes para o efeito.
 4. O Município de Mira comunica ao fornecedor todas as irregularidades encontradas no prazo referido no número anterior, findo o qual, não havendo qualquer comunicação de irregularidade detetada, considera-se que há aceitação definitiva dos mesmos, produzindo-se os efeitos previstos na cláusula 10.º Aceitação bens do presente caderno de encargos, em especial a validação, na respetiva fatura, da conformidade do fornecimento dos bens pelo Município de Mira
 5. As deficiências de fabrico ou quaisquer outras anomalias detetadas após o período de aceitação definitiva dos bens devem ser solucionadas pelo fornecedor, designadamente ao abrigo das condições de garantia.

Cláusula 9.ª

Inoperacionalidade, defeitos ou discrepâncias

1. No caso de os trabalhos e ou testes previstos na cláusula anterior não comprovarem a total conformidade e ou operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, ou no caso de existirem discrepâncias com as características, especificações e requisitos técnicos definidos no presente caderno de encargos e seus anexos, a Entidade Adjudicante deve informar, por escrito, o fornecedor.
2. No caso previsto no número anterior, o fornecedor deve proceder, à sua custa e no prazo razoável que for determinado pela Entidade Adjudicante, às alterações e complementos necessários para garantir o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.

3. Após a realização das alterações e complementos necessários pelo fornecedor, no prazo respetivo, a Entidade Adjudicante procede a nova análise, nos termos da cláusula anterior.

Cláusula 10.^a

Aceitação dos bens

1. Caso os testes a que se refere a cláusula 8.^a do presente caderno de encargos comprovem a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, e neles não sejam detetados quaisquer defeitos e ou desconformidades e ou discrepâncias com as características, especificações e requisitos definidos no presente caderno de encargos, em especial nas cláusulas técnicas, deve ser expressa na respetiva fatura a validação da conformidade do referido fornecimento, devidamente assinada pelo representante do Município de Mira.
2. Pela cessão dos direitos a que se refere o número anterior não é devida qualquer contrapartida para além do preço contratual a pagar nos termos do presente caderno de encargos.

Cláusula 12.^a

Conformidade e Garantia Técnica

O adjudicatário fica sujeito, no que se refere aos elementos entregues ao Município de Mira em execução do contrato, às exigências legais, obrigações do fornecedor e prazos previstos no Código dos Contratos Públicos e demais legislações aplicáveis.

Cláusula 13.^a

Garantia da continuidade de fabrico

1. O fornecedor deve assegurar, à luz do estabelecido na alínea c) do n.º 1 da cláusula 5.^a do presente caderno de encargos, que o fabricante se compromete a garantir a continuidade de fabrico e de fornecimento de todas as peças, componentes e equipamentos que integram os bens objeto do contrato pelo prazo estimado da respetiva vida útil;
2. Sem prejuízo do disposto no número anterior, sempre que se verifique a descontinuidade de um bem, ou linha de bens, o fornecedor deve proceder à sua

substituição, submetendo essa atualização ao Município de Mira juntamente com uma declaração que confirme a descontinuidade, emitida pelo fabricante do bem/produto ou pelo representante oficial em Portugal

Cláusula 14.^a

Patentes, Licenças e Marcas registadas

1. São da responsabilidade da entidade adjudicatária quaisquer encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças.
2. Caso a entidade adjudicante venha a ser demandado por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, a entidade adjudicatária indemnizá-lo-á de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

Cláusula 15.^a

Objeto do dever de sigilo

1. O Adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica ou 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. O Adjudicatário deverá garantir rigoroso sigilo quanto a informações de que os seus técnicos e demais colaboradores venham a ter conhecimento relacionadas com este empreendimento e demais atividades da Entidade Adjudicante.
3. 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.
4. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo Adjudicatário 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.

Cláusula 16.^a

Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor até ao termo do prazo de 5 anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou de credibilidade, de prestígio ou da confiança devidos às pessoas coletivas.

Secção II

Obrigações da Entidade Adjudicante

Cláusula 17.^a

Preço Contratual

1. Pelo fornecimento do bem objeto do Contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a Entidade Adjudicante deve pagar ao Adjudicatário o preço constante da proposta adjudicada, acrescido e IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à Entidade Adjudicante, (incluindo despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças).

Cláusula 18.^a

Condições de Pagamento

1. A(s) quantia(s) devidas pela Entidade Adjudicante, nos termos da cláusula anterior devem ser pagas no prazo de 60 dias após a receção pela Entidade Adjudicante das respetivas faturas, emitidas mensalmente, as quais devem cumprir com o disposto no artigo 36.º CIVA¹ e só podem ser emitidas após o vencimento das obrigações respetivas, e após a prestação dos serviços,

¹Código do Imposto sobre o Valor Acrescentado

devendo ainda cumprir com as exigências impostas pelo artigo 9.º, n.º 1, da LCPA²², aprovada pela Lei n.º 8/2012, de 21 de fevereiro, na redação atual.

2. As faturas devem ser emitidas em nome do Município de Mira NIF: 506724530, sito na Praça da República, 3070-304 MIRA, com referência aos documentos que lhes deram origem, isto é, devem especificar o n.º da encomenda e o respetivo número sequencial de compromisso.
3. Desde que devidamente emitidas e observado o disposto no n.º 1 e 2, as faturas são pagas através de transferência bancária.

CAPÍTULO III

Penalidades Contratuais, Incumprimento de Contrato e Resolução

Cláusula 19.^a

Penalidades contratuais

1. Concretizada a adjudicação, nos casos em que se verifique atraso nos prazos de execução definidos para os serviços a realizar identificados na Parte II do presente caderno de encargos, por razões imputáveis à adjudicatária, que não resultem de força maior, poderá ser aplicada uma penalidade a deduzir ao valor da fatura da prestação de serviços, calculada de acordo com a seguinte fórmula:
 - a) 5% do preço contratual por cada semana de atraso na entrega dos bens;
2. As penalidades referidas no presente artigo não eximem em caso algum a entidade adjudicatária da responsabilidade pela indemnização dos danos causados pelo incumprimento no âmbito da prestação de serviços objeto do contrato, nos termos previstos no artigo anterior.
3. A aplicação das penalidades previstas nos números anteriores é da competência da entidade adjudicante.
4. O contraente público reserva-se o direito de deduzir nos pagamentos a efetuar à entidade adjudicatária as importâncias correspondentes ao valor das penalidades aplicadas nos termos dos números anteriores, sem prejuízo da possibilidade de, por acordo entre as partes, se estipular outra forma de pagamento.
5. O valor acumulado das sanções pecuniárias não poderá exceder 20% do preço contratual, sem prejuízo do poder de resolução do contrato, quando este limite seja atingido e a Câmara Municipal de Mira decida não proceder à resolução do contrato,

²² *Lei dos Compromissos e Pagamentos em Atraso*

- por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%, de acordo com o definido pelo artigo 329.º do CCP.
6. Para além das referidas sanções, poderá ser aplicado o regime contraordenacional previsto na Parte IV, Cláusulas 455.º a 464.º, do CCP, caso o comportamento do adjudicatário seja considerado demasiado lesivo ou prejudique o regular funcionamento da entidade adjudicante.
 7. Na determinação da gravidade do incumprimento, a Câmara Municipal de Mira tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.
 8. A Câmara Municipal de Mira pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.
 9. As penas pecuniárias previstas na presente cláusula não obstam a que a Câmara Municipal de Mira exija uma indemnização pelos danos decorrentes do incumprimento do adjudicatário.

Cláusula 20.ª

Prestações Acessórias Objeto do Contrato

Quaisquer atividades diretamente relacionadas com o objeto dos documentos contratuais, que decorram da normal execução do contrato, mas que não estejam especialmente previstas, e que venham a ser aconselhadas por força das circunstâncias, consideram-se como prestações acessórias, não dando lugar a qualquer pagamento para além do que ficar contratado.

Cláusula 21.ª

Força Maior

1. Não podem ser impostas penalidades ao Adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo 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,

greves, 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 do Adjudicatário, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades em que o Adjudicatário 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 ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente ao impedimento resultante da força maior.

Cláusula 22.^a

Resolução por parte da Entidade Adjudicante

Sem prejuízo de outros fundamentos de resolução previstos na lei, nomeadamente indemnizações legais e contratuais devidas, a Entidade Adjudicante pode resolver o contrato, a título sancionatório, no caso de o Adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem,

Cláusula 23.^a

Resolução por parte do Adjudicatário

1. O Adjudicatário pode resolver o Contrato nos termos e nos casos previstos nos artigos 332.º n.º1 e 406.º do CCP.
2. O direito de resolução é exercido por via judicial, com exceção dos casos previstos na alínea c) do n.º 1 do artigo 332.º do Código dos Contratos Públicos, nos quais o direito de resolução pode ser exercido mediante declaração à Entidade Adjudicante produzindo efeitos 30 (trinta) dias após a receção dessa declaração, salvo se a Entidade Adjudicante cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.
3. A resolução do Contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pelo Adjudicatário, 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 24.ª

Gestor de Contrato

1. Na outorga contratual, o contraente público designará o gestor do contrato, com a função de acompanhar permanentemente a execução deste.
2. Sem prejuízo de outras obrigações constantes do presente caderno de encargos, competirá ao gestor do contrato:
3. A representação do contraente público no âmbito da execução contratual, salvo indicação daquele em contrário;
4. A coordenação das reuniões com o(s) representantes do cocontratante, salvo se houver indicação do contraente público em contrário.
5. Comunicar ao órgão competente pela decisão de contratar, ou a quaisquer entidades a quem este o incumba, quaisquer desvios, defeitos ou outras anomalias na execução do contrato; propondo em relatório fundamentado as medidas corretivas que, em cada caso, se revelem adequadas;
6. Visar a(s) fatura(s) através de assinatura/carimbo de modo a confirmar a correta execução contratual;
7. As funções de gestão do contrato extinguir-se-ão quando todas as prestações, principais ou acessórias de todas as Partes do contrato tiverem sido executadas.
8. A extinção referida no número anterior não isenta o gestor do contrato de quaisquer responsabilidades, designadamente de prova judicial, seja testemunhal ou documental.

9. Havendo necessidade de substituição, durante a vigência do contrato, deve o contraente público designar o novo gestor do contrato através de um despacho assinado pelo representante designado para a assinatura do contrato pelo órgão competente para a decisão de contratar; devendo notificar o cocontratante e o gestor cessante através dos meios de comunicação utilizados no presente contrato.

CAPÍTULO IV

Seguros

Cláusula 25.^a

Disposições gerais

1. É da responsabilidade do Adjudicatário a cobertura, através de Contratos de seguro da atividade que exerce.
2. A Entidade Adjudicante pode, sempre que entender conveniente, exigir prova documental da celebração dos Contratos de seguro referidos no número anterior, devendo o prestador de serviços providenciá-la no prazo de 5 dias úteis.

CAPÍTULO V

Resolução de Litígios

Cláusula 26.^a

Foro competente

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

CAPÍTULO VI

Disposições Finais

Cláusula 27.^a

Subcontratação e cessão da posição contratual

1. A subcontratação pela entidade adjudicatária e a cessão da posição contratual depende da autorização da entidade adjudicante, nos termos do Código dos Contratos Públicos.
2. O prestador de serviços pode subcontratar as entidades identificadas na fase de formação do Contrato, desde que se encontrem cumpridos os requisitos constantes dos n.ºs 3 e 6 do artigo 318.º do CCP.
3. A responsabilidade pelo exato e pontual cumprimento de todas as obrigações contratuais é do exclusivamente do prestador de serviços, ainda que as mesmas sejam cumpridas por recurso a subcontratos.
4. A cessão da posição contratual é em qualquer caso vedada nas situações previstas no n.º 1 do artigo 317.º do CCP.
5. O prestador de serviços tomará as providências indicadas pelo contraente público para que este, em qualquer momento, possa distinguir o pessoal do prestador de serviços do pessoal dos subcontratados.

Cláusula 28.^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 29.^a

Contagem de prazos

Os prazos previstos no contrato são contínuos, correndo sábados, domingos e dias feriados, conforme previsto no artigo 471.º do CCP.

Cláusula 30.^a

Legislação aplicável

A tudo o que não esteja previsto no Caderno de Encargos aplica-se o regime previsto no Código dos Contratos Públicos, aprovado pelo Decreto-lei n.º 18/2008, de 29 de janeiro na sua atual redação, bem como as disposições legislativas e regulamentares aplicáveis, de acordo com a natureza do serviço a contratar.

Cláusula 31.^a

Cláusulas Técnicas

Pressupostos Técnicos

O Município de Mira tem neste momento uma solução de perímetro baseada em *Fortinet*. O propósito deste fornecimento é substituir esta solução por uma mais atual, migrando todas as regras e configurações atualmente existentes, com o menor impacto possível, seja através de caminhos alternativos, seja em horário que não afete os serviços.

O equipamento será para ligar ao *switch* de core do fabricante Aruba, utilizando a funcionalidade de agregação de portas SFP+, devendo ser previsto o fornecimento de 2 unidades Direct Attach Copper de 3 metros para este fim, compatível com a firewall fornecida e o equipamento de switching mencionado.

Especificações Técnicas

1. Solução de autenticação e gestão de identidades com tokens para duplo fator de autenticação

Pretende-se a implementação de uma solução de autenticação segura e gestão de identidades centralizada, que permita o acesso seguro e controlado dos utilizadores à infraestrutura de rede.

1.1. Funcionalidades principais

As seguintes funcionalidades deverão ser suportadas:

- Autenticação segura baseada em protocolos standard de autenticação como RADIUS e LDAP
- Funcionalidade de autenticação forte através da utilização de tokens por aplicações móveis com suporte a sistemas iOS, Android e Windows Phone, SMS e email, certificados digitais e chaves FIDO sem password
- Diretório local de utilizadores e Integração com sistemas de diretórios externos incluindo LDAP e Active Directory de forma a reutilizar credenciais existentes
- Políticas de sincronização para importação de utilizadores em diretórios externos
- Portais de registo e self-service customizáveis que permitam o registo automatizado e gestão de passwords pelos próprios utilizadores e integração com dispositivos externos
- A solução deverá ter a capacidade de funcionar como entidade certificadora, fazendo a emissão e gestão do ciclo de vida dos certificados digitais, usados para autenticação segura de dispositivos ou utilizadores em redes com e sem fios e acessos VPN
- Gestão de certificados para registo automático de dispositivos em ambientes BYOD (Bring Your Own Device)
- A solução deverá suportar o standard IEEE 802.1X de forma a permitir a autenticação de nível corporativo de dispositivos e utilizadores em redes com e sem fios. Deverão ser suportados entre outros os protocolos PEAP, EAP-MD5, EAP-TTLS, EAP-TLS e EAP-GTC. A solução deverá ainda suportar autenticação baseada no macaddress dos dispositivos
- Identificação dos utilizadores de forma transparente através de pelo menos os seguintes métodos
 - Integração com controladores de domínio de Active Directory de forma a captar as credenciais dos utilizadores

- Agente externo para instalação nas máquinas dos utilizadores com capacidade para detetar eventos e informação de login e logout e alteração de endereços IP
- Portais disponibilizados pela própria solução para autenticação e rastreio dos utilizadores de forma a reduzir a necessidade de autenticações repetidas
- Monitorização dos registos de login dos acessos baseados no protocolo RADIUS
- A solução deverá disponibilizar uma API REST de autenticação para integração com sistemas terceiros
- A solução deverá suportar o standard de autenticação e autorização SAML SP/IdP de forma a garantir mecanismos de single sign-on para acesso a aplicações através de browser

1.2. Requisitos gerais

As seguintes características deverão ser asseguradas:

- Consola de gestão com acesso via browser e protocolo seguro HTTPS ou CLI via SSH
- A solução deverá permitir a implementação em cenário de alta disponibilidade
- Deverá permitir a utilização do protocolo SNMP para queries ou envio de traps com informação do sistema
- A solução deverá ter a capacidade de mostrar graficamente, na consola de gestão, as tentativas de autenticação com e sem sucesso num período de tempo configurável
- A solução deverá ter a capacidade de guardar os logs de autenticação localmente ou enviar para um repositório externo via Syslog
- Deverá permitir o backup de toda a configuração a partir da consola de gestão e suportar calendarização e envio do ficheiro de backup para um repositório externo

1.3. Requisitos da componente de tokens para duplo fator de autenticação

As seguintes funcionalidades deverão ser suportadas:

- Gerador OATH compatível com OTP baseada em tempo (TOTP) ou eventos (HOTP) para gerar passwords de utilização única
- Detalhes do login enviados por PUSH para o telemovel com a possibilidade de aprovar ou rejeitar
- Utilização de PIN/Impressão digital/reconhecimento facial para proteger a aplicação
- Permissão para copiar OTP (One time Password) para o clipboard
- Exibição do tempo de validade da OTP
- Gestão de tokens e da aplicação
- Remoção automática de tokens em caso de ataques brute-force
- Compatibilidade com iOS (iPhone, iPod Touch, iPad, Apple Watch), Android, Windows Phone 8, 8.1, Windows 10 e Windows Universal Platform
- Licenciamento perpetuo e transferências entre dispositivos ilimitadas
- Ativar tokens over-the-air (Apenas disponível para dispositivos com WIFI)
- Especificações da OTP (RFC 6238, RFC 4226)

1.4. Especificações técnicas

As seguintes características mínimas deverão ser asseguradas:

- Suporte para no mínimo 100 utilizadores
- Suporte para no mínimo 200 tokens para dispositivo móvel iOS, Android ou Windows Phone
- Dispositivos NAS: 33
- Grupos de utilizadores: 10
- Certificados CA: 5

- Certificados de utilizador: 100
- Solução em appliance virtual com suporte nas seguintes plataformas: VMware ESX/ESXi 4 / 5 / 6, Microsoft Hyper-V Server 2010, 2012 R2 e 2016, KVM, Xen, Amazon Web Services (AWS), Microsoft Azure, Oracle OCI, Alibaba Cloud
- Virtual CPUs (máximo): 64
- Virtual NICs (mínimo/máximo): 1 / 4
- Storage (mínimo/máximo): 60 GB / 16 TB
- Memória RAM (mínimo/máximo): 2 GB / 1 TB
- Alta disponibilidade: Ativo-Passivo e Config Sync

2. Web Application Firewall (WAF)

2.1. Especificações técnicas

As seguintes características mínimas deverão ser asseguradas:

Sistema Virtual

- Hypervisores suportados: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, Virtualbox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Oracle Cloud.
- vCPUs suportados (Máximo): 2
- vNICs suportados (Máximo): 10
- Armazenamento interno (Mínimo / Máximo): 40 GB / 2 TB
- Memória suportada (Mínimo / Máximo): 1.024 MB / Unlimited for 64-bit
- Alta-Disponibilidade: Ativo/Standby, Ativo/Ativo

Desempenho do sistema

- Débito HTTP: 100 Mbps
- Domínios de Administração (Máximo): 64
- Licenciamento ilimitado de aplicações: SIM

Modos de integração em rede

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

As seguintes funcionalidades deverão ser suportadas:

- AI-based Machine Learning
- Profiling automático (white Lists)
- Assinaturas de servidor web e aplicações (black list)
- Reputação de IPs
- Geolocalização de IPs
- Validação de compliance com RFC de HTTP
- Suporte nativo para HTTP/2
- Verificação de OpenAPI 3.0
- Proteção de WebSocket e enforcement de assinaturas
- Proteção de ataques do tipo Man in the Browser (MiTB)
- Proteção contra os seguintes ataques aplicacionais
 - OWASP Top 10
 - Cross Site Scripting
 - SQL Injection
 - Cross Site Request Forgery
 - Session Hijacking

- Built-in Vulnerability Scanner
 - Integração com Third-party scanner (virtual patching)
 - Análise de ficheiros com antivírus e sandbox
- Serviços de segurança
 - Assinaturas de serviços Web
 - Conformidade de protocolos XML e JSON
 - Detecção de malware
 - Patching virtual
 - Validação de protocolos
 - Proteção contra ataques do tipo Brute force
 - Assinatura e encriptação de cookies
 - Pontuação e ponderação de ameaças
 - Detecção de ataques SQLi baseados na syntax
 - Segurança dos headers de HTTP
 - Gestão de mensagens e códigos de erro customizados
 - Assinaturas de deteção de Sistema operativo
 - Proteção contra ataques conhecidos e do tipo zero-day
 - Stateful Firewall L4
 - Prevenção de ataques DoS
 - Mecanismos de proteção avançada com recurso a múltiplos elementos de segurança
 - Proteção contra fugas de informação
 - Proteção contra web defacement

- Balanceamento aplicacional
 - Balanceamento de servidores L7
 - Reescrita de URLs
 - Routing aplicacional baseado em conteúdos
 - Offloading de HTTPS/SSL
 - Compressão de HTTP
 - Caching de conteúdos
- Autenticação
 - Autenticação ativa e passiva
 - Publicação de sites e SSO (Single sign-on)
 - Acesso RSA para autenticação de 2 fatores
 - Suporte para LDAP, Radius e SAML
 - Suporte para certificados SSL de cliente
 - CAPTCHA e Real Browser Enforcement (RBE)
- Gestão e Reporting
 - Acesso de gestão através de interface 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
 - Ferramentas gráficas de análise e reporting
 - Suporte para gestão centralizada de múltiplos equipamentos
 - Suporte para Alta Disponibilidade Ativo/Ativo
 - REST API

- Suporte para Logging e Reporting centralizado
- Identificação e rastreamento de utilizadores/dispositivos
- Dashboards para visualização de informação em tempo real
- Dashboards para Bots
- Categorização de ataques OWASP Top 10
- Análítica de informação de geolocalização de IPs
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, Syslog e Email (Logging e monitorização)
- Suporte de domínios administrativos com controle de acesso baseado em funções (RBAC)
- Integração em redes
 - VLANs (802.1Q) e agregação de portas(802.3ad)
 - Support de IPv6
 - Alta disponibilidade activo-passivo e activo-activo
 - Tradução de HTTP/2 para HTTP 1.1
 - Integração com plataformas HSM
 - Integração simplificada com plataformas PKI
 - Análise de anexos em aplicações ActiveSync/MAPI, Outlook Web Access e FTP
 - Alta disponibilidade com sincronização de configurações entre múltiplos dispositivos ativos
 - Deve permitir a configuração automatizada e incluir definições por defeito para instalação simplificada
 - Deve incluir wizards de configuração para aplicações e bases de dados comuns
 - Mecanismos de auto-aprendizagem

- Deve incluir por defeito alguns perfis de inspeção e proteção
- Pré-configurado para aplicações Microsoft, como Exchange, OWA e Sharepoint
- Deve incluir políticas de segurança pré-definidas para aplicações Drupal e Wordpress
- Suporte de OpenStack
- Suporte de Websockets

3. Firewall de Próxima Geração (NGFW)

3.1. Especificação técnica

- Conectividade
 - Interfaces 10/100/1000 RJ45 Aceleradas ASIC: 16x GE RJ45
 - Interfaces GbE SFP ou 10/100/1000 Aceleradas ASIC: 8x GE SFP
 - Interfaces 10GbE SFP+ Aceleradas ASIC: 4x 10GE SFP+
 - Interfaces de Gestão: 1x GE RJ45
 - Interfaces de HA: 1x GE RJ45
 - Interface USB: 1
 - Interface de Consola (RJ45): 1
 - Bluetooth Low Energy (BLE): 1
- Sistema
 - Disco interno: 1x 480 GB SSD
 - Trusted Platform Module (TPM): 1
- Desempenho
 - Aceleração do tráfego de Firewall, SSL e IPSec por hardware: Hardware dedicado
 - Aceleração de tráfego NGFW por hardware: Hardware dedicado

- Débito firewall (pacotes UDP de 1518 / 512 / 64 bytes): 27 / 27 / 11 Gbps
- Latência de firewall (pacotes UDP de 64 bytes): 4.78 μ s
- Débito firewall (pacotes por segundo): 16.5 Mpps
- Sessões TCP concorrentes: 3 Milhões
- Novas sessões/segundo (TCP): 280000
- Políticas de firewall: 10000
- Débito VPN IPSec (pacotes 512 bytes): 13 Gbps
- Túneis IPsec Gateway-to-Gateway: 2000
- Túneis IPsec cliente remoto: 16.000
- Débito VPN SSL: 2 Gbps
- VPN SSL - Máximo RECOMENDADO de utilizadores simultâneos: 500
- Débito IPS: 5 Gbps
- Débito de inspeção SSL: 4 Gbps
- Débito de Application Control: 13 Gbps
- Débito NGFW: 3.5 Gbps
- Débito Threat Protection: 3 Gbps
- Domínios Virtuais (por defeito / máximo): 10 / 10
- Máximo de FortiAPs controlados (Total / Tunnel Mode): 256 / 128
- Máximo de FortiSwitch controlados: 64
- Máximo de FortiTokens: 5000
- Licenciamento ilimitado de utilizadores: SIM
- Energia e Alimentação
 - Alimentação AC: 100–240V AC, 50–60 Hz
 - Consumo de energia médio: 104.52 W

- Consumo de energia máximo: 121.94 W
 - Dissipação Térmica: 436.98 BTU/h
 - Fonte de alimentação redundante: Sim
- Condições ambientais
 - Temperatura de funcionamento: 0 - 40 °C
 - Humidade: 20 a 90% sem condensação
 - Compliance: FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI
 - Certificações: ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, IPv6
- Dimensões
 - Altura: 44 mm (1RU)
 - Largura: 432 mm
 - Profundidade: 342 mm
 - Peso: 4.6 KG

As seguintes funcionalidades deverão ser suportadas:

Integração com redes de comunicações

- 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 (3000+ Applications Supported), 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;

- Protocolos de routing dinâmico: RIPv1, RIPv2, RIPv3, OSPFv2 e OSPFv3, ISIS, BGP4+
- Tráfego multicast: PIM, sparse e dense mode
- Routing baseado em conteúdos: WCCP e ICAP
- Proxy explícito com suporte PAC e WPAD
- IPv6: Gestão por IPv6, Protocolos de routing dinâmico com IPv6, Tunneling de IPv6, Processamento firewall e UTM de IPv6, NAT64, NAT46, VPN IPSec IPv6
- Dual Stack IPv4 e IPv6 em simultâneo
- VXLAN
- Controlador Wireless integrado
- Controlador Switching integrado
- Virtualização da solução em contextos.

Identificação de utilizadores e dispositivos

- 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; Novell eDirectory FortiClient; 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; Autenticação e bypass feitos por MAC Address

- Implementação de políticas de segurança com base em utilizador ou dispositivos

Firewall

- Modos de operação NAT/route e transparente/bridge
- Agendamento de políticas: recorrentes ou apenas uma vez
- 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)
- Tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pinhole
- 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: predefinidos, 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
- 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, 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

- IPSEC VPN: 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, IKEv1, IKEv2 (RFC 4306) , 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
- 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
- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente
- ADVPN
- 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
 - 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
 - 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
 - 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
 - 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 da terminação 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
 - 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

- IPS com mais de 12000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados

- Diferentes ações de IPS: definido por defeito na assinatura, monitorizar, bloquear, reset de sessão ou quarentena (IP do atacante, IP de atacante e vítima, interface de entrada) 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

- 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, aplicação de gestão de largura de banda

- Inspeção SSL (suporte TLS 1.3)

Proteção contra ameaças

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, filtragem WEB 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
- Anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- 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
- Anti-vírus em modo proxy, incluindo: Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP; 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):
 - diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS)
 - Possibilidade de definição manual de filtragem 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 ativar as seguintes funcionalidades: Filtrar Java Applet, ActiveX e/ou cookies; Bloquear HTTP Post; Registrar termos/palavras utilizados nas pesquisas em motores de busca; Identificar imagens pelo URL; Bloquear redireccionamentos 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 customizada 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 redireccionamentos 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
 - protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP: Possibilidade de executar as ações: registar, bloquear, quarentena de utilizador/IP/Interface; Filtros pré-definidos incluindo cartões de crédito e número de segurança Social
 - protocolos na análise de ficheiros: HTTP-POST, HTTP=GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP: Opções de filtragem disponíveis, tais

como tamanho, 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
- Arquivamento 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 e Indicadores de compromisso

Alta disponibilidade

- 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 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 HÁ; HA com equipamento geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

Administração, Monitorização e Diagnósticos

- 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
- múltiplas linguagens de administração no acesso gráfico, incluindo: português, inglês, espanhol, francês, japonês, chinês simplificado, chinês tradicional e Coreano
- Gestão local e gestão centralizada em simultâneo
- 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 (incluído de terceiras partes) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções Openstack, VMWare NSX, e Cisco ACI.
- Automação, por exemplo para colocar em Quarentena um dispositivo com um elevado Indicador de Compromisso.

Registo de eventos e relatórios

- 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: enviado, bloqueado, sessões violadas, 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 encurtado 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.

4. Serviços de Implementação

4.1. Estratégia de Serviços

- Preparação/Kickoff
 - Definição de tarefas, requisitos, responsabilidades e agendamento
 - Levantamento da informação necessária à implementação da solução pretendida
 - Especificação do modo de proteção da componente WAF e das proteções a implementar para cada uma das 10 aplicações web a proteger;

- Validação dos requisitos
- Instalação, Configuração e Testes
 - Gestão de identidade e acesso com tokens para duplo fator de autenticação
 - Instalação e configuração inicial da nova plataforma para a ligação à rede
 - Ligação da nova plataforma à rede
 - Adição da AD local como servidor de autenticação remoto
 - Registo e mapeamento dos novos tokens aos utilizadores da AD
 - Verificação do funcionamento esperado da nova plataforma
 - Backup da configuração criada e testada com sucesso
 - Formação On-Job nas configurações realizadas a dois elementos da equipa de TI do Município de Mira
 - Firewall de Aplicações Web (WAF)
 - Instalação e configuração inicial da solução para a ligação à rede
 - Ligação à rede da plataforma adquirida
 - Configuração da solução para updates periódicos
 - Configuração das proteções especificadas
 - Verificação do funcionamento esperado das proteções implementadas.
 - Configuração da solução para utilização da solução de gestão de identidade e acesso implementada na autenticação do acesso aos websites protegidos

- Verificação do funcionamento do 2FA na autenticação do acesso aos websites protegidos com esperado
- Backup da configuração criada e testada com sucesso.
- Formação On-Job nas configurações realizadas a dois elementos da equipa de TI do Município de Mira
- Firewall de Próxima Geração
 - Registo da nova plataforma para ativação dos serviços UTP do fabricante
 - Migração da configuração da atual solução para a nova plataforma
 - Instalação e ligação à rede da nova plataforma
 - Verificação do funcionamento esperado da nova plataforma
 - Configuração das novas plataformas de firewall para utilização da nova solução de gestão de identidade e acesso como servidor de autenticação
 - Verificação do funcionamento do 2FA no acesso VPN
 - Backup da configuração criada e testada com sucesso
 - Formação On-Job nas configurações realizadas a dois elementos da equipa de TI do Município de Mira
- Fecho
 - Documentação da solução implementada
 - Entrega da documentação
 - Fecho

As eventuais referências a marcas nas peças/especificações técnicas acima mencionadas, deverão ser sempre interpretadas como contendo a expressão prévia “tipo ou equivalente”, nos termos legalmente exigidos.