CONCURSO PÚBLICO – DEC 2/2020

Serviços de Suporte de Sistemas de Gestão e Assistência Técnica

CADERNO DE ENCARGOS

PARTE I - CLÁUSULAS GERAIS 3

CLÁUSULA 1.ª OBJETO 3

CLÁUSULA 2.ª CONTRATO 3

CLÁUSULA 3.ª DURAÇÃO DO CONTRATO 3

CLÁUSULA 4.ª PREÇO BASE 3

CLÁUSULA 5.ª CRITÉRIO DE ADJUDICAÇÃO 4

CLÁUSULA 6.ª CRITÉRIOS AMBIENTAIS 5

CLÁUSULA 7.ª OBRIGAÇÕES PRINCIPAIS DO ADJUDICATÁRIO 5

CLÁUSULA 8.ª CONFORMIDADE DO SERVIÇO 6

CLÁUSULA 9.ª ASSISTÊNCIA TÉCNICA 6

CLÁUSULA 10.ª INFORMAÇÃO E SIGILO 6

CLÁUSULA 11.ª PROTEÇÃO DE DADOS PESSOAIS E RGPD 6

CLÁUSULA 14.ª PRESTAÇÃO DA CAUÇÃO 8

CLÁUSULA 15.ª PENALIDADES CONTRATUAIS 8

CLÁUSULA 16.ª FORÇA MAIOR 9

CLÁUSULA 17.ª RESOLUÇÃO POR PARTE DA APDSE 9

CLÁUSULA 18.ª RESOLUÇÃO POR PARTE DO ADJUDICATÁRIO 10

CLÁUSULA 19.ª SUPERVISÃO E CONTROLO 10

CLÁUSULA 22.ª FORO COMPETENTE 12

CLÁUSULA 23.ª COMUNICAÇÕES E NOTIFICAÇÕES 12

CLÁUSULA 24.ª CONTAGEM DOS PRAZOS 12

CLÁUSULA 25.ª LEGISLAÇÃO APLICÁVEL 12

PARTE II – ESPECIFICAÇÕES TÉCNICAS 13

CLÁUSULA 1.ª ENQUADRAMENTO 13

CLÁUSULA 2.ª NOTAS PRÉVIAS 13

CLÁUSULA 3.ª ÂMBITO DA PRESTAÇÃO DE SERVIÇO 13

CLÁUSULA 4.ª ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO 14

CLÁUSULA 5.ª INSTALAÇÃO DA SOLUÇÃO 27

CLÁUSULA 6.ª MANUTENÇÃO E ASSISTÊNCIA TÉCNICA DA SOLUÇÃO 27

CLÁUSULA 7.ª DOCUMENTAÇÃO A APRESENTAR APÓS IMPLEMENTAÇÃO DA SOLUÇÃO 27

CLÁUSULA 8.ª PRAZO DE IMPLEMENTAÇÃO DA SOLUÇÃO 28

CLÁUSULA 9.ª QUANTIDADES MINIMAS 28

Parte 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, na sequência do procedimento pré-contratual, que tem por objeto principal a Prestação de Serviços Suporte de Sistemas de Gestão e Assistência Técnica, das Águas Públicas da Serra da Estrela E.I.M. S.A, adiante designada APdSE.

2. O objeto do contrato abrange ainda serviços de instalação, conversão, formação e licenciamento.

CLÁUSULA 2.ª CONTRATO

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

2. O contrato integra ainda os seguintes elementos:
   a) os suprimentos dos erros e omissões do Caderno de Encargos, identificados pelos concorrentes, desde que tais erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar.
   b) os esclarecimentos e as retificações relativos ao Caderno de Encargos.
   c) o presente Caderno de Encargos.
   d) a proposta adjudicada.
   e) os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3. Em caso de divergência entre os documentos referidos no número anterior, a 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. Além dos documentos indicados no n.º 2, o adjudicatário obriga-se também a respeitar, no que lhe seja aplicável, as normas europeias e portuguesas, as especificações e homologações de organismos oficiais e fabricantes ou entidades detentoras de patentes.

CLÁUSULA 3.ª DURAÇÃO DO CONTRATO

1. O contrato vigorará pelo período de 36 meses, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

CLÁUSULA 4.ª PREÇO BASE

1. O valor base para efeito de concurso é de € 94.225,00 (Noventa e Quatro Mil, Duzentos e Vinte e Cinco Euros), não incluindo o imposto sobre o valor acrescentado, ou seja, o valor máximo fixado no Caderno de Encargos, nos termos do n.º 1, do art. 47.º do Dec. Lei Nº 111-B/2017, de 31 de agosto.

2. O valor base do presente procedimento foi estabelecido após consulta ao portal base, e tendo em

consideração o que são os valores praticados no mercado para a prestação de serviços, em empresas análogas.

3. O preço base inclui todos os custos, encargos e despesas cuja responsabilidade não seja expressamente atribuída a entidade adjudicatária, nomeadamente os relativos ao transporte de bens e pessoas, alojamento, alimentação, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças, se aplicável.

CLÁUSULA 5.ª CRITÉRIO DE ADJUDICAÇÃO

1. A adjudicação será feita à proposta economicamente mais vantajosa, atendendo à melhor relação qualidade/preço, nos termos da alínea a), do n.º 1, do Artigo 74.º, do CCP, tendo em conta os seguintes fatores:

Critério Preço
P= Pontuação obtida de acordo com o preço da proposta do concorrente, conforme tabela:

Preço Total da Proposta	Pontos
Preço ≤ 78.500 €	10
78.500€ < Preço ≤ 82.000€	9
82.000€ < Preço ≤ 85.000€	8
85.000€ < Preço ≤ 87.500€	7
87.500€ < Preço ≤ 89.500€	6
89.500€ < Preço ≤ 92.000€	5
92.000€ < Preço < 94.225€	4
igual ao preço base	2
superior a preço base	0

Critério Distância:
D= Pontuação obtida de acordo com a distância das instalações do concorrente em relação à Sede da APdSE, conforme tabela:

Distância em Kms em relação à Sede APdSE	Pontos
Distância ≤ 30 Km	10
30 Km < Distância ≤ 100 Km	5
100 Km < Distância ≤ 200 Km	2,5
Distância > 200 Km	0

Sendo a Nota Final (NF):

$$NF = 0{,}60 \times P + 0{,}40 \times D$$

2. Critério de desempate: Serviço e assistência técnica pós-venda e condições de entrega, o menor prazo de entrega ou de execução e o menor tempo de prestação de assistência.

CLÁUSULA 6.ª CRITÉRIOS AMBIENTAIS

1. O presente procedimento utiliza critérios ambientais, na medida em que privilegia como critério de adjudicação a distância entre as instalações da APdSE e o prestador de serviços

2. A distância condiciona em grande medida o impacto ambiental da prestação de serviços, tendo em conta que quanto menor for a distância, menor será a emissão de gases com efeitos de estufa, fruto das deslocações para assistência técnica presencial que terá de ser efetuada.

CAPÍTULO II - OBRIGAÇÕES CONTRATUAIS

SECÇÃO I | OBRIGAÇÕES DO FORNECEDOR

CLÁUSULA 7.ª OBRIGAÇÕES PRINCIPAIS DO ADJUDICATÁRIO

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrerão para o fornecedor as seguintes obrigações principais de:
   a) Proceder à prestação de serviços identificadas na parte II do Caderno de Encargos, no prazo máximo de 7 dias de calendário a contar da data de celebração do contrato;
   b) prestar assistência técnica nos termos previstos na parte II do Caderno de Encargos;
   c) designar um interlocutor responsável pela prestação de serviços;
   d) dar resposta aos pedidos de intervenção, no prazo máximo previsto na parte II do Caderno de Encargos;
   e) no caso de não ser possível o cumprimento do prazo definido na alínea anterior, deverá o adjudicatário informar os serviços da APdSE, apresentado a devida justificação e proposta de calendarização alternativa;
   f) não ceder a sua posição contratual sem prévia autorização da entidade adjudicante;
   g) prestar de forma correta e fidedigna todos as informações referentes às condições em que é prestado o serviço, bem como ministrar todos os esclarecimentos que se justifiquem, de acordo com as circunstâncias;
   h) comunicar qualquer facto que ocorra durante a execução dos contratos e que altere, designadamente, a sua denominação social, os seus representantes legais com relevância para o fornecimento, a sua situação jurídica e a sua situação comercial;
   i) comunicar antecipadamente à entidade adjudicante os factos que tornem total ou parcialmente impossível a prestação de serviço, ou o cumprimento de qualquer outra das suas obrigações.
   j) comunicar antecipadamente à entidade adjudicante os factos que tornem total ou parcialmente impossível o fornecimento dos produtos, ou o cumprimento de qualquer outra das suas obrigações.

2. O prestador do serviço será responsável perante a APdSE por qualquer discrepância, vícios, inaptidão ou má execução dos serviços prestados, e pela inobservância das caraterísticas, especificações e requisitos técnicos previstos nas clausulas técnicas ao presente caderno de encargos, que venham a ocorrer no momento da execução dos trabalhos.

3. No caso previsto no número anterior, o fornecedor devera proceder a suas custas e segundo as indicações de prazo e modo que forem determinadas pela APdSE, aos trabalhos necessários para repor a conformidade dos serviços contratualizados ao cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.

4. A título acessório, o adjudicatário fica ainda obrigado, designadamente, a recorrer a todos os meios humanos e materiais que sejam necessários e adequados, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

CLÁUSULA 8.ª CONFORMIDADE DO SERVIÇO

1. O(s) fornecedor(es) obrigar-se-á a prestar os serviços ao contraente público objeto do contrato, com as características, especificações e requisitos técnicos previstos na parte II do presente Caderno de Encargos, que dele faz parte integrante.

2. O(s) fornecedor(es) será(ão) responsável(eis) perante a entidade adjudicante por qualquer defeito ou discrepância dos serviços objeto do contrato que existam no momento em que são concluídos.

CLÁUSULA 9.ª ASSISTÊNCIA TÉCNICA

O fornecedor ficará obrigado a prestar serviços de assistência técnica durante o período de contrato, a contar da data da entrada em funcionamento do sistema.

CLÁUSULA 10.ª INFORMAÇÃO E SIGILO

1. O prestador de serviços deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à APdSE, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.

2. A informação e a documentação cobertas pelo dever do 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.

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

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 fornecedor 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 11.ª PROTEÇÃO DE DADOS PESSOAIS E RGPD

1. O adjudicatário obriga-se, durante a vigência do contrato e mesmo após a sua cessação, a não ceder, revelar, utilizar ou discutir, com quaisquer terceiros, todas e quaisquer informações e ou elementos que lhe hajam sido confiados pela APdSE ou de que tenha tido conhecimento no âmbito do contrato ou por causa dele.

2. Os dados pessoais a que o prestador de serviços tenha acesso ou que lhe sejam transmitidos pela APdSE ao abrigo do contrato serão tratados em estrita observância das instruções desta empresa e da legislação de Proteção de Dados Pessoais, nomeadamente com o Regulamento Geral de Proteção de Dados Pessoais (RGPD – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016).

3. O prestador de serviços compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer forma colocar à disposição de terceiros os dados pessoais a que tenha acesso ou lhe sejam transmitidos pela APdSE ao abrigo do contrato, sem que para tal tenha sido expressamente instruída, por escrito, pela APdSE.

4. O prestador de serviços aceita que a APdSE recorra a outras entidades subcontratadas exclusivamente com o intuito de prestar serviços a que o prestador de serviços não consiga dar resposta, sempre no âmbito das atribuições definidas pela APdSE.

5. Caso o prestador de serviços subcontrate outras entidades (mediante prévia autorização escrita da

APdSE, nos termos previstos no CCP) para a prestação de serviços previamente definidos pela APdSE, o prestador de serviços será o único responsável pela escolha das empresas subcontratadas, bem como por toda a atuação destas.

6. O prestador de serviços obriga-se a garantir que as empresas por estas subcontratadas cumprirão o disposto na LPDP e na demais legislação aplicável, nomeadamente com o Regulamento Geral de Proteção de Dados Pessoais (RGPD – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016), devendo tal obrigação constar dos contratos escritos que celebra com outras entidades por si subcontratadas.

7. O prestador de serviços obriga-se a cumprir rigorosamente o disposto na LPDP e demais legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:
   a) Utilizar os dados pessoais a que tenha acesso ou lhe sejam transmitidos pela APdSE, única e exclusivamente para efeitos da prestação dos serviços objeto deste contrato;
   b) Observar os termos e condições constantes dos instrumentos de legalização respeitantes aos dados tratados;
   c) Manter os dados pessoais estritamente confidenciais, cumprindo e garantindo o cumprimento do dever de sigilo profissional relativamente aos mesmos dados pessoais;
   d) Cumprir quaisquer regras relacionadas com o tratamento de dados pessoais a que a APdSE, esteja especialmente vinculada, desde que tais regras lhe sejam previamente comunicadas;
   e) Pôr em prática as medidas técnicas e de organização necessárias à proteção dos dados pessoais tratados por conta da APdSE, contra a respetiva destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.
   f) Manter a APdSE, informada em relação ao tratamento de dados pessoais;
   g) Comunicar de imediato qualquer situação que possa afetar o tratamento dos dados em causa, ou que de algum modo possa dar origem ao incumprimento das disposições legais em matéria de proteção de dados pessoais ou dos termos do instrumento de legalização concedido pela Comissão Nacional de Proteção de Dados à APdSE.
   h) Prestar à APdSE, toda a assistência de que esta careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais, efetuado ao abrigo do contrato, no sentido de assegurar o cumprimento das obrigações no âmbito das notificações e comunicações em caso de Violação de dados pessoais.
   i) Assegurar que os seus colaboradores cumprem todas as obrigações previstas no contrato;
   j) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
   k) Adotar medidas de segurança previstas no artigo 32º do RGPD, que assegurem a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços que tratam dados pessoais e possuir um processo para testar, apreciar e avaliar regularmente a eficácia destas medidas;
   l) Prestar a assistência necessária à APdSE, no sentido de permitir que esta cumpra a obrigação de dar uma resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos Direitos previstos no RGPD, nomeadamente o direito de acesso do titular aos seus dados pessoais, direito de retificação e direito ao apagamento de dados.
   m) Garantir mecanismos de notificação efetivos em caso de violação de dados pessoais;
   n) Disponibilizar as informações necessárias para demonstrar o cumprimento do RGPD, bem como colaborar com auditorias ou inspeções, conduzidas pela APdSE, ou por outro auditor por este mandatado.

8. O prestador de serviços será responsável por qualquer prejuízo em que a APdSE, venha a incorrer em consequência do tratamento, por parte do mesmo e/ou dos seus colaboradores, de dados pessoais em violação das normas legais aplicáveis e/ou do disposto no contrato.

9. Para efeitos do disposto no nº 8 e alínea g) do nº 7 da presente cláusula, entende-se por "colaborador" toda e qualquer pessoa singular ou coletiva que preste serviços ao adjudicatário/prestador de serviços, incluindo, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido entre o

adjudicatário e o referido colaborador.

10. A obrigação de sigilo prevista na alínea d) do número 7 da presente cláusula mantém-se mesmo após a cessação do contrato, independentemente do motivo por que ocorra.

SECÇÃO II | OBRIGAÇÕES DA APdSE

CLÁUSULA 12.ª PREÇO CONTRATUAL

1. Pela prestação de serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a APdSE deverá pagar mensalmente ao fornecedor o serviço efetivamente prestado, nos termos das cláusulas da Parte II do Caderno de Encargos e de acordo com os preços constantes da lista de preços unitários da proposta adjudicada.

2. O valor total da proposta adjudicada não poderá ser superior ao preço máximo fixado no presente Caderno de Encargos, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

3. O preço referido no número anterior incluirá todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

CLÁUSULA 13.ª CONDIÇÕES DE PAGAMENTO

1. As quantias devidas pela APdSE, nos termos das cláusulas anteriores, serão pagas mensalmente no prazo de 60 dias.

2. As faturas deverão ser enviadas para a APdSE, Praceta os Doze de Inglaterra, Nº11 6270-465 Seia, com a indicação do número do cabimento.

3. Para os efeitos do disposto no n.º 1, a obrigação considerar-se-á vencida com a prestação de serviço.

4. Não poderão ser propostos adiantamentos por conta da prestação de serviço.

5. Em caso de discordância por parte da entidade adjudicante, quanto aos valores indicados nas faturas, deverá este comunicar ao prestador de serviços, por escrito, os respetivos fundamentos, ficando o fornecedor obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.

6. Para bom e pontual cumprimento das obrigações decorrentes do contrato, e no caso de não ser exigida a prestação da caução, poderá a entidade adjudicante, se o considerar conveniente, proceder à retenção de até 10% do valor dos pagamentos a efetuar, nos termos do n.º 3 do artigo 88.º do CCP.

CLÁUSULA 14.ª PRESTAÇÃO DA CAUÇÃO

No presente procedimento não haverá lugar a prestação de caução.

CAPÍTULO III - PENALIDADES CONTRATUAIS E RESOLUÇÃO

CLÁUSULA 15.ª PENALIDADES CONTRATUAIS

1. Pelo incumprimento de obrigações emergentes do contrato, a APdSE pode exigir ao adjudicatário o pagamento de uma sanção pecuniária, que não poderá exceder globalmente os 25% do valor contratual, nos seguintes termos:

a) Pelo incumprimento das datas e prazos de entrega dos bens e serviços objecto do contrato, calculado de acordo com a seguinte fórmula: P = PP x V x N, em que P corresponde ao valor da pena, PP

corresponde à percentagem da penalidade (1%), V corresponde ao valor contratual e N corresponde ao n.º de dias em atraso.

b) Pelo incumprimento do atraso na reposição do serviço de qualquer um dos itens do contrato de prestação de serviços fica a mensalidade sujeita a penalidades, de montante a fixar em função do tempo de atraso decorrido e de acordo com a seguinte fórmula: S = PP x M x H, em que S corresponde ao valor a descontar à mensalidade, PP corresponde à percentagem da penalidade (2%), M corresponde ao valor da mensalidade e H corresponde ao n.º de horas em atraso. O valor máximo da penalidade nunca poderá ser superior ao valor da mensalidade em questão.

2. O valor das sanções serão objeto de faturação por parte da APdSE, podendo ser objeto de encontro de contas com a entidade adjudicante.

CLÁUSULA 16.ª FORÇA MAIOR

1. Não podem ser impostas penalidades ao prestador de serviços, 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 prestador de serviços, na parte em que intervenham;
   b) Greves ou conflitos laborais limitados às sociedades do prestador de serviço ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
   c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;
   d) Manifestações populares devidas ao incumprimento pelo prestador de serviço de normas legais;
   e) Incêndios ou inundações com origem nas instalações do prestador de serviço 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 prestador de serviço não devidas a sabotagem;
   g) Eventos que estejam ou devam estar cobertos por seguros.
   h) A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
   i) A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

CLÁUSULA 17.ª RESOLUÇÃO POR PARTE DA APdSE

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a APdSE pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, nomeadamente:
   a) Se os serviços prestados não corresponderem às características e especificações técnicas estabelecidas neste Caderno de Encargos;
   b) Quando a demora da execução dos trabalhos exceder em 20 dias úteis o prazo fixado no contrato.

2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao prestador de serviço e não determina a repetição das prestações já realizadas, a menos que tal seja determinado

pelo contraente público.

3. A resolução do contrato não invalida o direito a qualquer ação que venha a ser interposta por parte da APdSE com vista à justa indemnização por perdas e danos eventualmente sofridos com incumprimento do contrato.

4. Em caso de resolução do contrato por incumprimento do fornecedor, a APdSE pode exigir-lhe uma pena pecuniária, que não poderá ser superior a 20% do preço contratual.

5. Ao valor da pena pecuniária prevista no número anterior, são deduzidas as importâncias pagas pelo fornecedor ao abrigo da alínea a), n.º 1, clausula 15.º, relativamente aos bens objecto do contrato cujo atraso na entrega tenha determinado a respetiva resolução.

6. Na determinação da gravidade do incumprimento, a APdSE terá a conta, nomeadamente, a duração da infracção, a sua eventual reiteração, o grau de culpa do fornecedor e as consequências do incumprimento.

CLÁUSULA 18.ª RESOLUÇÃO POR PARTE DO ADJUDICATÁRIO

1. O Adjudicatário pode resolver o contrato nos termos previstos no CCP.

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

3. 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 esta última 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 Adjudicatário, cessando, porém, todas as obrigações deste ao abrigo do contrato (com exceção daquelas a que se refere o artigo 444.º do CCP).

CAPÍTULO IV – GESTÃO DE CONTRATO

CLÁUSULA 19.ª SUPERVISÃO E CONTROLO

1. O contraente público designa como gestor do contrato nos termos do artigo 290.º -A, Sónia Alexandra da Conceição Geraldo Madeira, com a função de acompanhar permanentemente a execução do contrato.

2. O adjudicatário deverá nomear um técnico que o represente em tudo o que concerne aos serviços a prestar, o qual servirá de interlocutor entre a entidade adjudicante e o adjudicatário para a resolução e/ou conhecimento de quaisquer assuntos inerente ao objeto do contrato.

3. Para efeitos do cumprimento do exercício das funções de gestão do contrato, o adjudicatário deverá disponibilizar os contatos telefónicos e de endereço eletrónico do representante por si nomeado.

4. O adjudicatário estará sujeito à supervisão da execução do contrato, a qual será assegurada pelo

gestor de contrato.

5. Caso se verifiquem situações anómalas na prestação dos serviços, e com base nos relatórios emitidos pelo gestor de contrato, será o adjudicatário notificado para regularização imediata das mesmas.

CLÁUSULA 20.ª CESSÃO E SUBCONTRATAÇÃO DA POSIÇÃO CONTRATUAL POR INICIATIVA DO COCONTRATANTE

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

2. A cessão da posição contratual com iniciativa por parte do cocontratante depende da prévia apresentação dos documentos de habilitação relativos ao potencial cessionário que foram exigidos ao cedente na fase de formação do contrato.

3. A autorização da subcontratação depende da prévia apresentação dos documentos de habilitação relativos ao potencial subcontratado que foram exigidos ao subcontratante na fase de formação do contrato.

CLÁUSULA 21.ª CESSÃO DA POSIÇÃO CONTRATUAL POR INCUMPRIMENTO DO COCONTRATANTE

1. Em caso de incumprimento, pelo cocontratante, das suas obrigações, que reúna os pressupostos para a resolução do contrato, o adjudicatário cede a sua posição contratual ao concorrente do procedimento pré -contratual na sequência do qual foi celebrado o presente contrato, que venha a ser indicado pelo contraente público, pela ordem sequencial no referido procedimento.

2. Para o efeito previsto na parte final do número anterior, o contraente público interpela, gradual e sequencialmente, os concorrentes que participaram no procedimento pré - contratual original, de acordo com a respetiva classificação final, a fim de concluir um novo contrato para a adjudicação da conclusão dos trabalhos.

3. A execução do contrato ocorre nas mesmas condições já propostas pelo cedente no procedimento pré-contratual original.

4. A cessão da posição contratual opera por mero efeito de ato do contraente público, sendo eficaz a partir da data por este indicada.

5. Os direitos e obrigações do cocontratante, desde que constituídos em data anterior à da notificação do ato referido no número anterior, transmitem-se automaticamente para o cessionário na data de produção de efeitos daquele ato, sem que este a tal se possa opor.

6. As obrigações assumidas pelo cocontratante depois da notificação referida no n.º 4 apenas vinculam a entidade cessionária quando este assim o declare, após a cessão.

7. Quando há lugar a caução e a garantias prestadas pelo cocontratante inicial, estas são objeto de redução na proporção do valor das prestações efetivamente executadas e são liberadas seis meses após a data da cessão, ou, no caso de existirem obrigações de garantia, após o final dos respetivos prazos, mediante comunicação dirigida pelo contraente público aos respetivos depositários ou emitentes.

8. A posição contratual do cocontratante nos subcontratos por si celebrados transmite -se automaticamente para a entidade cessionária, salvo em caso de recusa por parte desta.

CAPÍTULO V - RESOLUÇÃO DE LITÍGIOS

CLÁUSULA 22.ª FORO COMPETENTE

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

CAPÍTULO VI - DISPOSIÇÕES FINAIS

CLÁUSULA 23.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 contato constantes do contrato deverá ser comunicada à outra parte.

CLÁUSULA 24.ª CONTAGEM DOS PRAZOS

1. À contagem dos prazos na fase de execução do contrato são aplicáveis as seguintes regras:
   a) Exceto quando dito expressamente que se trata de dias úteis, os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados;
   b) Quando o último dia do prazo for um sábado, domingo, feriado ou dia em que os serviços da entidade adquirente, por qualquer causa, se encontrem encerrados, passa o primeiro dia útil subsequente;
   c) O prazo fixado em semanas, meses ou anos, a contar de certa data, termina às 24 (vinte e quatro) horas do dia que corresponda, dentro da última semana, mês ou ano, a essa data, se no último mês não existir dia correspondente, o prazo finda no último dia desse mês.

CLÁUSULA 25.ª LEGISLAÇÃO APLICÁVEL

O contrato é regulado pela legislação em vigor.

Parte II – Especificações Técnicas

A Parte II elenca todas as funcionalidades, outputs de informação e características técnicas pretendidas por áreas.

CLÁUSULA 1.ª ENQUADRAMENTO

1. A APdSE tem um papel essencial no abastecimento de água aos municípios que abrangem. Torna-se assim, essencial, ter um sistema de gestão moderno, interoperável com as novas tecnologias de centralização de recursos e preparado para o futuro.
2. Será objeto deste procedimento a capacitação da APdSE com ferramentas capazes de promover este novo sistema.
3. A APdSE tem 4 edifícios, uma Sede e três Lojas. Nestes locais irá haver presença física da administração e colaboradores, que terão a necessidade de mobilidade pois a natureza deste sistema necessita que as contagens sejam efetuadas em diversos locais dos municípios abrangidos. Adicionalmente, e face à atual pandemia, o sistema também deverá ser capaz de suportar regime de teletrabalho.

CLÁUSULA 2.ª NOTAS PRÉVIAS

1. No presente documento são elencados os requisitos mínimos de cada uma das funcionalidades do sistema (de cada uma das especificações técnicas) que constituem o objeto do contrato a celebrar, sendo que os mesmos serão adiante abreviadamente designados por ET.
2. Todos os ET elencados no presente Caderno de Encargos estão numerados (n) e associados a um componente específico (ETn).
3. Todos os equipamentos/sistemas a adquirir têm que ser novos. Não serão aceites equipamentos/sistemas usados, reciclados ou remanufaturados.
4. A versão de firmware ou software instalada de base/fábrica no equipamento/sistema terá que suportar todas as funcionalidades requeridas.
5. Para efeitos do presente Caderno de Encargos, entende-se como fornecimento da solução: o fornecimento, a instalação, configuração, ensaios finais, formação e manutenção do sistema proposto.

   Nota: Quando utilizados os termos "deverá / suporta / possibilidade / permite / terá" e termos com significado semelhante, os requisitos devem ser considerados como requisitos obrigatórios se nada for dito em contrário e deverão ser fornecidos / instalados de base sem custo adicionais, sendo este requisito aplicável a todo o documento e pelo período de vigência do contrato.

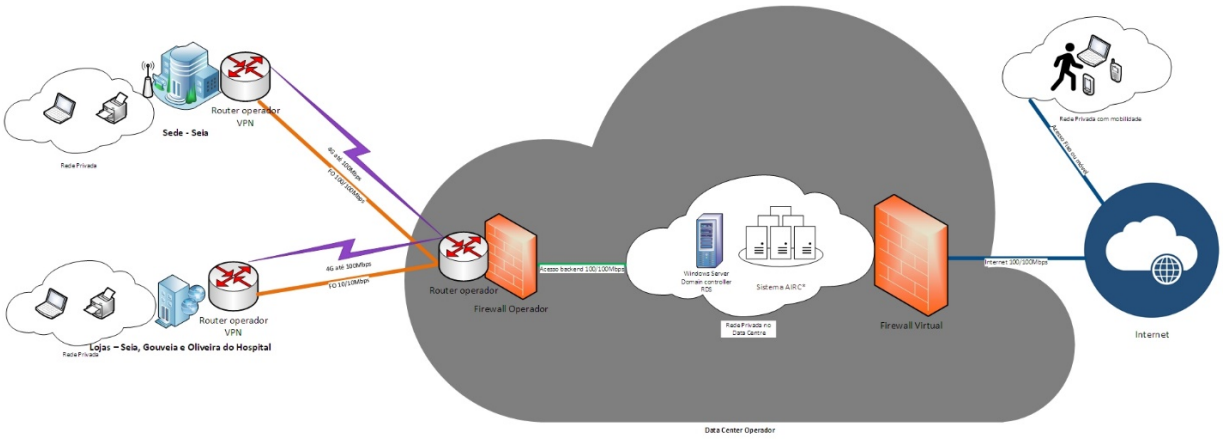
CLÁUSULA 3.ª ÂMBITO DA PRESTAÇÃO DE SERVIÇO

1. Pretende-se o fornecimento de um sistema de contagem do abastecimento de águas, sendo da responsabilidade do adjudicatário o dimensionamento e fornecimento de todos os componentes necessários para o correto funcionamento do sistema, conforme especificado no caderno de encargos.
2. Fazem parte integrante do fornecimento da solução as seguintes tarefas, que serão da responsabilidade do adjudicatário:
   a) Integração dos sistemas em data center;
   b) Fornecimento, instalação e montagem dos equipamentos/sistemas e acessórios em todos locais:

Sede, Lojas e Data Center;

c) Configuração, colocação em serviço, testes e formação on-job de toda a solução;

d) Manutenção e assistência técnica da solução.



CLÁUSULA 4.ª ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

Nesta secção são apresentadas funcionalidades/requisitos técnicos pretendidos para equipamentos e sistemas no âmbito deste procedimento.

Para comprovar as especificações técnicas da solução apresentada, os concorrentes terão obrigatoriamente de apresentar com a proposta, as fichas técnicas dos equipamento e sistemas (em língua portuguesa ou inglesa) que comprovem o cumprimento dos requisitos e especificações definidos neste procedimento

Nota: O não cumprimento de alguma destas especificações é critério de exclusão da proposta.

1.1. Requisitos da Solução Cloud

Esta componente deverá cumprir obrigatoriamente os seguintes requisitos:

ET 1	Solução de Servidores Virtuais IaaS;
ET 2	Conjunto de recursos virtuais dedicados para a criação, e gestão, dos seus próprios servidores, incluindo a disponibilização de processamento, memória, armazenamento e rede.
ET 3	Plataforma de serviço alojada em ambiente isolado e com redundância implementada, a todos os níveis: servidores, armazenamento, virtualização, switching e segurança.
ET 4	Consola para criação de servidores e configuração de recursos do ambiente virtual, incluindo funcionalidades de gestão de rede, segurança e organização lógica da arquitetura em self-service.
ET 5	Ter uma única interface para gerir o ambiente virtual, as aplicações ou os serviços, ajustar a capacidade contratada e efetuar o agendamento de tarefas automáticas.
ET 6	Garantir as seguintes funcionalidades:

ET 6.1 Visualizar os recursos alocados ao data center virtual – capacidade alocada vs disponível vs utilizada.

ET 6.2 Visualizar as operações efetuadas sobre o data center virtual.

ET 6.3 Criar / apagar servidores.

ET 6.4 Criação de servidores através de templates – sistema operativo pré-definido + recursos mínimos.

ET 6.5 Alterar recursos dos servidores (processamento, memória, disco, hostname, rede, grupo) dentro da quota de recursos disponível.

ET 6.6 Clonar servidor – permite duplicar um servidor.

ET 6.7 Criar cópias de segurança à imagem do servidor.

ET 6.8 Recuperar servidor a partir de uma cópia de segurança.

ET 6.9 Visualizar as operações efetuadas sobre cada servidor.

ET 6.10 Definir políticas de segurança – configuração da firewall e load balancer.

ET 6.11 Criar / apagar rede – criação de níveis de segurança (arquiteturas multicamada).

ET 6.12 Agrupar servidores de forma lógica, facilitando a organização da infraestrutura na Interface.

ET 7 Responda rapidamente a novos projetos, necessidades aplicacionais inesperadas ou alterações no negócio, ajustando a capacidade de TI de forma totalmente flexível e em tempo real, através de um portal web.

ET 8 Elevada agilidade e amplitude, na parametrização de recursos, permitindo aumentar e diminuir capacidade de forma precisa e rápida, sem obrigatoriedade de configurações predefinidas.

ET 9 Realização de cópias aos servidores virtuais, definindo a frequência e o período de retenção.

ET 10 Possibilidade de recuperação de toda a informação, restaurando qualquer cópia que tenha realizado.

ET 11 Possibilidade de definição de políticas de segurança entre aplicações, ou servidores, para permitir ou bloquear a comunicação na mesma rede local virtual, ou em redes locais virtuais distintas.

ET 12 A infraestrutura possuir regras para distribuir tráfego entre servidores, ou implementar mecanismos de failover.

ET 13 Acesso remoto aos servidores, sem utilizar a rede, simulando a ligação de um teclado e monitor ao servidor. Possibilidade de visualizar o servidor a reiniciar, alterar configurações de rede, ou realizar outras tarefas de gestão de forma sistemática.

ET 14 Partilhar um conjunto alargado de imagens, que abrangem sistemas operativos Microsoft e Linux, para a criação rápida de servidores.

ET 15 Monitorização do estado do servidor e dos seus recursos, permitindo ajustar a capacidade de forma proativa, com total controlo do impacto na despesa, sendo possível gerir o ciclo de vida dos recursos através de workflows automatizados.

ET 16 Interligação do ambiente virtual com a internet, com a rede privada empresarial, ou com outras infraestruturas TI através de conetividade ao data center.

ET 17 Transferência de servidores virtuais de outras infraestruturas para ambiente virtual e vice-versa, recorrendo a um servidor FTP como destino da exportação ou como origem da importação.

ET 18 Funcionalidades de gestão técnica que permitam fazer a gestão dos servidores, sem intervenção manual. Poder criar, iniciar, parar, escalar e apagar os servidores, de uma forma rápida e sem complicações.

ET 19 Processos, ferramentas e boas práticas:

ET 19.1 Um Hypervisor líder de mercado que garanta controlo proactivo sobre as atividades realizadas sobre a plataforma e que reflita a certificação da implementação das melhores práticas de segurança IT;

ET 19.2 Segregação da plataforma de serviço de outras plataformas existentes no Data Center – através de soluções de networking;

ET 19.3 Plataforma compatível com PCI 2.0;

ET 19.4 Isolamento do tráfego com VLANs dedicadas, por forma a inviabilizar a comunicação entre servidores de diferentes clientes;

ET 19.5 Isolamento de perímetro e de cliente, através de firewalls certificadas por entidade independente.

1.2. Requisitos do Data Center (DC)

Para o cumprimento dos objetivos e necessidades identificados, a entidade adjudicatária deverá disponibilizar os serviços pretendidos, em equipamentos alojados em DC com as seguintes características, sob pena de exclusão do concurso:

ET 20 Onde seja garantido o controlo das condições ambientais através de sistemas de ar condicionado redundantes, com controlo e regulação automática de qualidade do ar, temperatura e humidade, garantindo sempre a sua manutenção dentro dos parâmetros estabelecidos pelas melhores práticas da arte e recomendações internacionais;

ET 21 Onde seja garantida a existência de sistemas de deteção de gás e inundação, nas salas de TI & SIs em que estão alojados os servidores. Estes processos deverão ser complementados com sistemas de alarmista centralizada e controlada por operadores nas próprias instalações, para aumentar os níveis de eficiência e segurança;

ET 22 Onde seja garantida e protegida a integridade física dos equipamentos, com a presença de equipas de segurança (24hx365d por ano), por portas corta-fogo com controlo de acessos, por sistemas de deteção e extinção de incêndios, por sistemas de alarmística, circuitos fechados de videovigilância, sistemas diversos de deteção de intrusão, de movimento e de abertura e fecho de portas;

ET 23 Onde sejam garantidos pelo menos 4 perímetros de segurança física entre a entrada pública do complexo onde se integra o Data Centre e as infraestruturas de TIs na sala de alojamento. Todos estes perímetros de segurança deverão estar protegidos por portas blindadas, antifogo e com sistema de controlo de acessos biométrico;

ET 24 Onde seja garantida conectividade direta ao Backbone IP de Comunicações Nacional (Português), ao nível de acessos aos Servidores Virtuais via Internet, através de MPLS, bem como a redundância ao nível dos percursos de distribuição de comunicações por caminhos distintos;

ET 25 que seja garantida, entre o Cliente e os Servidores Virtuais do DC do adjudicatário, conetividade direta ponto-a ponto e sem sair do ambiente protegido do operador adjudicatário, ou seja, sem passar, nem a nível físico nem a nível lógico, pela Internet, permitindo estabelecer um ambiente protegido de rede privada exclusivamente com recurso a endereçamento por IPs Privados;

ET 26 Onde seja garantida redundância de sistemas ao nível do fornecimento da energia elétrica autossuficiente em regime de failover. Em caso de falha, cada sistema deverá dispor de equipamentos redundantes (UPS, Baterias e Geradores). As salas de quadros elétricos, Unidades de Energia Ininterrupta, geradores, ar condicionado e de rede devem ser de acesso restrito e isoladas por área funcional;

ET 27 Dispor de um centro de operação e supervisão que assegure toda a operação e supervisão das instalações numa base permanente (24hx365d por ano);

ET 28 Dispor de certificação Tier III (pelo Uptime Institute) em termos de conceção e instalação, o que implica garantir que todo o projeto de infraestrutura segue um princípio de redundância N+1, alimentado por 2 caminhos independentes e redundantes, permitindo à infraestrutura alcançar uma disponibilidade anual mínima de 99,98%. O adjudicatário deverá comprovar que o seu DC tem essa certificação.

ET 29 O DC deverá possuir as certificações:

ET 29.1 ISO 20000 (ITIL) - Serviços de Gestão de Tecnologias de Informação

ET 29.2 ISO 27001 - Gestão de Segurança da Informação

ET 30 No DC terão de ser seguidos todos os requisitos definidos na norma:

ET 30.1 ISO 14520 – norma para os sistemas de Deteção e Extinção de Incêndios.

ET 31 Deverá haver um documento emitido por auditores externos que garantam as seguintes normas de sustentabilidade ambiental do DC:

ET 31.1 Recurso a energias renováveis, aproveitamento de águas pluviais e refrigeração sustentável do DC.

O serviço de servidores privados que o adjudicatário garante prestar deverá, sob pena de exclusão do concurso:

ET 32 Permitir a disponibilização ágil e em tempo real de recursos lógicos computacionais com elevada segurança, escalabilidade e disponibilidade, a partir de uma interface de gestão web que seja simples e intuitiva;

ET 33 Permitir através de um ambiente virtual dedicado, constituído por recursos de processamento, memória, armazenamento e de rede totalmente flexíveis, para permitir acomodar diferentes tipos de aplicações e de forma automática;

ET 34 Permitir a virtualização de contextos de firewall, isolamento de rede, possibilidade de definição de políticas de segurança entre aplicações ou servidores para permitir ou bloquear comunicação na mesma rede local virtual ou em redes locais virtuais distintas. Permitir o controlo de acesso baseado em perfis de utilização e integração com redes privadas;

ET 35 Deverá garantir uma plataforma de serviço alojada em ambiente isolado e com redundância implementada a todos os níveis: servidores, armazenamento, virtualização, switching e segurança;

ET 36 A infraestrutura deverá permitir a implementação de regras para distribuição tráfego entre servidores ou para implementar mecanismos de failover.

ET 37 Deverá permitir a realização de cópias aos seus servidores virtuais, uma vez definidas a frequência e o período de retenção, em DC diferente e geograficamente separados em mais de 100 km. Possibilidade de recuperação de toda a informação, restaurando qualquer cópia que tenha realizado;

ET 38 Deverá incluir um conjunto alargado de imagens que abrangem sistemas operativos Microsoft e Linux para a criação rápida de servidores; os sistemas operativos suportados devem ser compatíveis com VMware;

ET 39 Deverá permitir a monitorização remota do estado dos servidores e dos seus recursos, permitindo ajustar a capacidade de forma proactiva;

ET 40 Deverá garantir a transferência de servidores virtuais de outras infraestruturas para ambiente virtual e vice-versa, recorrendo a servidor FTP como destino da exportação ou como origem da importação (em formato *.ova compatível);

ET 41 Deverá disponibilizar ferramentas – API – que permitam a gestão de servidores sem intervenção manual;

ET 42 Deverá garantir disponibilidade de serviço dos servidores privados mínimo de 99,95%; suporte telefónico especializado em língua portuguesa (24hx365d por ano); suporte telefónico comercial (7hx5dias úteis por semana);

ET 43 Embora fora do âmbito do concurso, o adjudicatário deverá declarar garantir estar preparado para permitir, se as APdSE assim o pretenderem, serviço de Disaster Recovery, suportado em Data Center secundário geograficamente redundante, com garantia de conetividade do tipo das definidas nos parágrafos I) e II); neste caso, o DC Produtivo e o DC Disaster Recovery deverão estar a mais de 200Km distância, e pelo menos um deles deverá estar a mais de 50km de distância do litoral.

ET 44 Embora fora do âmbito do concurso, o adjudicatário deverá declarar garantir estar preparado para permitir, se as APdSE assim o pretenderem, serviço de Housing, suportado em Data Center com as caraterísticas exigidas neste documento, dando a possibilidade às APdSE de, a qualquer momento, poder optar por uma solução adicional de alojamento de máquinas físicas, propriedade das APdSE, em condições adequadas de alojamento, de conetividades de dados, de alimentação elétrica, refrigeração, de segurança (física e lógica) e ambiental; para este efeito, o DC do adjudicatário deverá ser identificado e estar localizado em território português.

Ao nível da conetividade o adjudicatário deverá garantir

ET 45 Entre as APdSE e os Servidores Virtuais do DC do adjudicatário, conetividade direta ponto-a ponto e sem sair do ambiente protegido do operador adjudicatário, ou seja, sem passar, nem a nível físico nem a nível lógico, pela Internet, permitindo estabelecer um ambiente protegido de rede privada exclusivamente com recurso a endereçamento por IPs Privados;

ET 46 Conectividade direta ao Backbone IP de Comunicações Nacional (Português), ao nível de acessos aos Servidores Virtuais via Internet, bem como a redundância ao nível dos percursos de distribuição de comunicações por caminhos distintos;

1.2.1. Requisitos Firewall Front-End

Esta componente deverá cumprir, obrigatoriamente, os seguintes requisitos:

ET 47 Firewall de Front-End em formato appliance virtual com suporte e licenciamento por 3 anos com:

ET 47.1 Gestão local e que perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa

ET 48 Performance:

ET 48.1 Performance da appliance virtual com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) >= 2,0 Gbps

ET 48.2 Performance da appliance virtual com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) >= 1 Gbps

ET 48.3 Performance da appliance virtual com a funcionalidade de VPN IPSec >= 1 Gbps

ET 48.4 Número de novas sessões por segundo >= 15000

ET 49 Gestão:

ET 49.1 Gestão e administração da própria máquina através de interface web, linha de comandos e API XML

ET 49.2 Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance virtual, com diferentes níveis de privilégio

ET 49.3 Possibilidade de editar configurações pendentes que ainda não foram aplicadas

ET 49.4 Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas

ET 49.5 Possibilidade de descartar alterações à configuração realizadas

ET 49.6 Possibilidade de armazenar diferentes versões da configuração

ET 49.7 Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento

ET 49.8 Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça

ET 49.9 Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade

ET 50 Rede:

ET 50.1 As interfaces de rede da appliance virtual deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3

ET 50.2 Suporte de IEEE 802.1Q

ET 50.3 Suporte de iEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo

ET 50.4 Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP

ET 50.5 Suporte de routing estático

ET 50.6 Suporte de DHCP, NAT e PAT

ET 50.7 Capacidade de deteção de falhas bidirecionais entre a appliance virtual e router para aplicar a protocolos de routing dinâmico ou rotas estáticas

ET 50.8 Capacidade de realizar policy based routing através do IP ou rede de origem

ET 50.9 Capacidade de realizar policy based routing através do tipo de aplicação

ET 50.10 Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo

ET 50.11 Permitir a criação de clusters de alta disponibilidade até 6 membros

ET 50.12 Suporte para TLS 1.3 e capacidade de desencriptar este tráfego

ET 51 Identificação de Utilizadores:

ET 51.1 Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP

ET 51.2 Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory

ET 51.3 Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores

ET 51.4 Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores

ET 51.5 Possibilidade de gerir utilizadores através de API XML

ET 51.6 Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local

ET 51.7 Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing

ET 52 Funcionalidades Gerais de Segurança:

ET 52.1 Possibilidade de agrupar interfaces da appliance virtual em conjuntos independentes, formando diferentes zonas de segurança

ET 52.2 Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança

ET 52.3 Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino

ET 52.4 Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas

ET 52.5 Capacidade de identificação de subfunções dentro de uma aplicação

ET 52.6 Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7

ET 52.7 Possibilidade de agrupar aplicações por categorias de forma a que as políticas de segurança sejam aplicadas por categorias de aplicações

ET 52.8 Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP

ET 52.9 Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP

ET 52.10 Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL

ET 52.11 Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling)

ET 52.12 Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego

ET 52.13 Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança

ET 52.14 Capacidade de forçar o uso de MFA para acesso a aplicações internas

ET 52.15 Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes

ET 53 IDS/IPS:

ET 53.1 Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças

ET 53.2 Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas

ET 53.3 Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos

ET 53.4 As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma a que a aplicação de perfis de proteção se possam realizar com base nestas categorias

ET 53.5 Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades

ET 53.6 Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis

ET 53.7 Deve ser possível converter assinaturas snort e suricata para dentro da plataforma

ET 54 Antivírus & Anti-Malware:

ET 54.1 Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C

ET 54.2 Capacidade de habilitar mecanismos de DNS sinkholing que permitam intercetar pedidos de resolução de nomes para domínios comprometidos com malware

ET 54.3 Capacidade de definir políticas de antivírus, de forma a que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso

ET 54.4 Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs)

ET 54.5 Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance virtual possam tomar uma ação no caso de um ficheiro malicioso

ET 54.6 Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações

ET 54.7 Capacidade de identificar ficheiros não através das suas extensões, mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros

ET 54.8 Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente

ET 54.9 Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro

ET 54.10 Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança

ET 54.11 Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados

ET 54.12 Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing.

ET 54.13 Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças

ET 55 URL Filtering:

ET 55.1 Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir mas advertir, etc)

ET 55.2 Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud

ET 55.3 Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação)

ET 55.4 Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web

ET 55.5 A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet

ET 55.6 A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.

ET 56 DNS Security:

ET 56.1 A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos

ET 56.2 Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes

ET 56.3 A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling).

ET 56.4 A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS.

ET 56.5 Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente.

ET 56.6 A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente

ET 56.7 Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas.

ET 56.8 Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos

ET 56.9 Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains

ET 56.10 A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças.

ET 56.11 A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas.

ET 57 Sandboxing:

ET 57.1 Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma a que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)

ET 57.2 Perante uma análise por parte do serviço de Sandboxing na cloud que categorize a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)

ET 57.3 O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios

ET 57.4 A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP

ET 57.5 A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.

ET 57.6 Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux

ET 57.7 O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida.

ET 57.8 Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10

ET 57.9 Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS),

ET 57.10 Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)

ET 57.11 Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.

ET 57.12 Capacidade de desencriptar malware (unpacker) para utilização na análise estática e machine learning.

ET 58 IoT Security:

ET 58.1 A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT.

ET 58.2 A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede.

ET 58.3 A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses.

ET 58.4 O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilância), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo

ET 58.5 Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também.

ET 58.6 Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal.

ET 58.7 A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas.

ET 58.8 Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos,etc.

ET 58.9 O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas ao uso/configuração incorrecta dos mesmos. Exemplo: uso de credenciais default.

ET 58.10 Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB(Cloud Access Security Broker).

ET 59 Data Loss Prevention:

ET 59.1 A plataforma deve disponibilizar um módulo completo de Data Loss Prevention

ET 59.2 Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação

pessoal,etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio.

ET 59.3 Este serviço deverá permitir proteger estes documentos das seguintes formas:

ET 59.4 Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização

ET 59.5 Monitorizar o upload de documentos para aplicações externas permitidas pela organização

ET 59.6 O serviço deve disponibilizar out-of-the-box pelo menos 380 “data patterns” e deve também disponibilizar perfis que agrupam determinados padrões de forma a simplificar a criação de políticas. Por exemplo, deverá existir um perfil associado com o GDPR de forma a facilitar a monitorização de documentos que possam contêm informação pessoal de utilizadores.

ET 59.7 Deverão existir os seguintes perfis out-of-the box: Bulk CCN, CCPA, Corporate FInancial docs, Financial information, GDPR, GLBA, Healthcare, Intellectual Property, Legal, Malware, Personally-Identifiable Information, Profanity, Self Harm e Sensitive content

ET 59.8 A solução deverá ser constantemente atualizada com novos padrões e perfis.

ET 59.9 De forma a melhorar o rácio de deteção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou “weighted”.

ET 59.10 Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE(Secure Access Service Edge), CASB(Cloud Access Security Broker) e CSPM(Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização.

ET 60 Relatórios e Logs:

ET 60.1 A appliance virtual deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais

ET 60.2 Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas

ET 60.3 Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf

ET 60.4 Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets

ET 60.5 Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende

ET 60.6 Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento

ET 60.7 Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a largo prazo

ET 60.8 Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance virtual com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema

ET 60.9 Capacidade de de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas,

equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos

ET 60.10 Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance virtual de forma a que a partir dos logs criados se possa obter informações de alto nível

ET 61 Outras funcionalidades:

ET 61.1 Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade

ET 61.2 Possibilidade de decifrar tráfego SSL e SSH de forma a que se possa estabelecer políticas de desencriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados

ET 61.3 Capacidade de criar exceções à desencriptação para determinado tipo de tráfego

ET 61.4 Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC)

ET 61.5 Possibilidade de enviar tráfego após desencriptação para uma interface de port mirror para análise de terceiras partes

ET 61.6 Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego

ET 61.7 Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção

1.3. Requisitos de Rede Privada e Acessos

Esta componente deverá cumprir obrigatoriamente os seguintes requisitos:

ET 62 Firewall de Back-End com suporte e licenciamento por 3 anos

ET 63 Acesso internet Data Center Back-End e Front End a 100 Mbps simétricos, sem contenção, com possibilidade de upgrade até 1Gbps em ambas;

ET 64 Solução VPN IP em Rede MPLS, com ligação 100/100 Mbps (simétrica), a partir de acesso com tecnologia de acesso baseada em Fibra Ótica, com capacidade de upgrade até 1Gbps/1Gbps, em ambiente seguro e isolado do ambiente público (Internet), com possibilidade de ativação de funcionalidades de QOS IP para soluções multimédia como o VoIP (Voz sobre IP), com tráfego ilimitado;

ET 65 Ligação dos locais remotos ao Site Sede em Seia, com conectividade VPN IP simétrica de 10/10Mbps. Ligação da Sede ao DC e restantes locais via VPN IP 100/100Mbps. Infraestrutura suportada em fibra óptica em todos os locais e nível de serviço de 4 horas lineares também para todos os locais;

ET 66 Arquitetura para suporte ao serviço VPN assente em rede de acesso integralmente suportada em Fibra Ótica, desde os equipamentos localizados em central do operador até ao terminador de rede ótica;

ET 67 Acesso permanente à VPN IP em fibra ótica, em FTTH, ligando as instalações das APdSE ao Backbone Empresarial MPLS;

ET 68 Possibilidade de interligação de locais geograficamente dispersos com topologia de rede implementada em estrela, em que todos os locais da empresa comunicam entre si em ambiente privado, com tráfego ilimitado;

ET 69 Crescimento flexível dos serviços, sem perturbação na infraestrutura física instalada, quer em termos de débito, quer em QoS;

ET 70 Utilização ilimitada de tráfego para a VPN IP, independentemente do tempo de utilização e do volume de dados, com Multi-QoS;

ET 71 Plataforma online de reporting para aceder em tempo real ao Desempenho e Qualidade de Serviço das componentes de Networking, nomeadamente os Registos de Avaria e estado em tempo real, Estado da Solução, Parque de Serviços Contratos, Gráficos de ocupação LB e delay/jitter, Gráficos em tempo real com atualização de 1 seg. e Estado dos SLAs com registos de avarias/IP SLA.

ET 72 Suporte de avaria até 4 horas Lineares;

ET 73 Redundância de conectividade nas instalações em 4G, com ativação automática, até 100 Mbps com Router e Antena Exterior 4Ge c/ routing c/ nível de serviço até 4 horas lineares;

1.4. Requisitos dos ativos LAN e WLAN

O controlador Wi-Fi deverá cumprir obrigatoriamente os seguintes requisitos:

ET 74 Controlador WLAN (Wi-Fi) na cloud em data centers alojados na União Europeia, cumprindo o RGPD.

Os Access Points (APs) de interior deverão ter as seguintes características:

ET 75 Compatível com protocolos IEEE 802.11a/b/g/n/ac wave 2.

ET 76 MIMO 2x2

ET 77 Capacidade de funcionar em modo autónomo e como controlador local

ET 78 Pelo menos 100 utilizadores concorrentes por AP

ET 79 Pelo menos 4 portas 10/100/1000, tendo pelo uma com saída PoE.

ET 80 Pelo menos uma porta USB A 2.0

ET 81 Ganho de antena integrada no máximo de 1dBi

ET 82 Débito agregado de pelo menos 1167 MBps

ET 83 Compatível com IEEE 802.3af/at.

ET 84 Certificado pela Wi-Fi Alliance com Passpoint®

ET 85 Suportar Beamforming.

ET 86 Ser adequado para montagem em parede.

Os Access Points (APs) de exterior deverão ter as seguintes características:

ET 87 Compatível com protocolos IEEE 802.11a/b/g/n/ac wave 2.

ET 88 MIMO 2x2

ET 89 Capacidade de funcionar em modo autónomo e como controlador local

ET 90 Proteção IP67

ET 91 Pelo menos 512 utilizadores concorrentes por AP

ET 92 Pelo menos 1 porta 10/100/1000

ET 93 Ganho de antena integrada no máximo de 3dBi

ET 94 Débito agregado de pelo menos 1167 MBps

ET 95 Compatível com IEEE 802.3af/at.

ET 96 Certificado pela Wi-Fi Alliance com Passpoint®

ET 97 Suportar Beamforming.

O switch PoE deverá cumprir obrigatoriamente os seguintes requisitos:

ET 98 Pelo menos 24 portas 10/100/1000 compatíveis com IEEE 802.3af/at

ET 99 Pelo menos 4 portas SFP+

ET 100 Pelo menos uma porta de consola RJ45

ET 101 Montagem em rack 19" ocupando 1RU, no máximo.

ET 102 Armazenamento flash de com pelo menos 16 MB
ET 103 Temperatura de funcionamento de pelo menos -20ºC a +60ºC
ET 104 Relógio de CPU de pelo menos 800MHz
ET 105 Pelo menos 512MB de memória RAM
ET 106 Fonte de alimentação interna de pelo menos 500W

1.5. Requisitos da Consultoria e Serviços de TI

Esta componente deverá cumprir obrigatoriamente os seguintes requisitos:

ET 107 Recurso técnico com formação de engenharia informática, telecomunicações ou similar.
ET 108 Disponibilidade do recurso supramencionado, de pelo menos 20h semanais, durante toda a vigência do contrato, num dos locais das APdSE.
ET 109 Serviço de resolução de problemas ou avarias (helpdesk) até 1h por acesso remoto e até 4h para deslocações on-site. Devendo ser asseguradas numa bolsa de 10h/semana.

CLÁUSULA 5.ª INSTALAÇÃO DA SOLUÇÃO

1. O adjudicatário tem de executar o serviço de instalação cumprindo as melhores práticas técnicas, de acordo com a especificação dos vários componentes do sistema.

2. Qualquer tipo de licenciamento necessário para garantir o correto funcionamento de todo dos equipamentos e/ou sistemas propostos, devem ser previstas e incluídas pelo concorrente.

CLÁUSULA 6.ª MANUTENÇÃO E ASSISTÊNCIA TÉCNICA DA SOLUÇÃO

1. Após o fornecimento e instalação da solução, o adjudicatário terá de garantir a Manutenção e Assistência Técnica da Solução fornecida por um período de 3 anos.
2. A manutenção terá de incluir a extensão do período da garantia dos equipamentos/sistemas pelo mesmo período da manutenção.
3. Durante o período contratual o adjudicatário estará obrigado a:

   a) Repor o Serviço de acordo com o SLA 24hx7dx4h;
   b) Prestar Suporte telefónico, gratuito, por email ou fax 24h x 7d x 365d;
   c) Atualizar os sistemas sempre que se justificar (após aprovação);
   d) Correção de falhas de segurança conhecidas (após aprovação);
   e) Reparar ou substituir a totalidade ou parcial dos equipamentos danificados;
   f) Garantir as peças de reserva para a substituição de quaisquer equipamentos danificados. A substituição destes equipamentos é da responsabilidade do adjudicatário e não implica qualquer custo adicional para a entidade adjudicante.

CLÁUSULA 7.ª DOCUMENTAÇÃO A APRESENTAR APÓS IMPLEMENTAÇÃO DA SOLUÇÃO

Após a instalação da solução e antes da aceitação do projeto, o adjudicatário tem de apresentar relatório completo com a documentação do projeto, que inclui um mapa de testes de aceitação descritos de seguida, nomeadamente:

a) Arquitetura da solução instalada.

b) Marcas, modelos, números de série e enderençamento IP de cada um dos equipamentos de rede.
c) Credenciais de acesso

CLÁUSULA 8.ª PRAZO DE IMPLEMENTAÇÃO DA SOLUÇÃO

O prazo máximo para a implementação do projeto é de 7 dias de calendário a contar a partir da data de assinatura do contrato.

CLÁUSULA 9.ª QUANTIDADES MINIMAS

A solução a fornecer requer que sejam cumpridos os requisitos funcionais, técnicos, de densidade e de qualidade pretendidos, obrigando a um número mínimo de equipamentos para se conseguir respeitar esses parâmetros.

Nesse sentido, são apresentados nesta seção, as quantidades mínimas de material/equipamento que a entidade adjudicante considera necessárias para cumprir os parâmetros supramencionados, sendo, no entanto, da responsabilidade dos concorrentes garantir o funcionamento da solução proposta de acordo com os parâmetros especificados. Como tal, sempre que considerem necessário, devem estes, propor os materiais e/ou equipamentos adicionais que considerem essenciais para salvaguardar o correto funcionamento da solução.

De seguida estão indicadas as quantidades mínimas estimadas pela entidade adjudicante, devendo as quantidades finais apresentadas por cada concorrente resultar do planeamento detalhado levado a cabo após a visita aos locais.

item	Descrição	Quantidades mínimas	Mensalidades
1	VCPUs	46	36
	RAM	92 GB	
	Discos SSD	400 GB	
	Discos SAS	1370 GB (1,370 TB)	
	Licenciamento Windows Server 2019	8	
	Licenças RDS	30	
	Firewall back-end	1	
	Firewall front-end	1	
	Rede Privada e Acessos	1	
2	Controlador Wi-Fi cloud	1	36
	AP de interior	9	
	AP de exterior	1	
	Switch PoE	1	
3	Helpdesk (remoto ou on-site)	10h/semana	36
4	Horas semanais para consultoria e serviços TI on-site	20h/semana	6

Seia, 16 de dezembro de 2020

O Vice-Presidente do Conselho de Administração
Carlos Filipe Camelo Miranda de Figueiredo