

Caderno de Encargos

Aquisição do Equipamento Solução Data Center com hardware e licenciamento, firewall de perímetro e hardware diverso e solução de storage

Consulta Prévia Simplificada N.º CPR/1/2021



Associação para o Desenvolvimento do Centro Académico de Investigação e Formação Biomédica do Algarve, AD-ABC

Cofinanciado por:



ÍNDICE

CAPÍTULO I	5
Disposições gerais	5
Cláusula 1. ^a	5
Objeto do Contrato.....	5
Cláusula 2. ^a	5
Entidade Adjudicante.....	5
Cláusula 3. ^a	5
Forma e documentos contratuais.....	5
Cláusula 4. ^a	6
Gestor do Contrato.....	6
Cláusula 5. ^a	6
Prazo de vigência do Contrato	6
CAPÍTULO II	7
Obrigações contratuais.....	7
Secção I	7
Obrigações do Adjudicatário	7
Cláusula 6. ^a	7
Obrigações gerais do Adjudicatário	7
Cláusula 7. ^a	8
Conformidade e garantia técnica.....	8
Cláusula 8. ^a	8
Aceitação do equipamento.....	8
Cláusula 9. ^a	9
Dever de sigilo.....	9
Cláusula 10. ^a	9
Proteção de dados pessoais	9
Secção II	10

Obrigações da AD-ABC.....	10
Cláusula 11. ^a	10
Preço contratual.....	10
Cláusula 12. ^a	11
Preço Base do Procedimento.....	11
Cláusula 13. ^a	11
Condições de pagamento.....	11
CAPÍTULO III	12
Penalidades contratuais e resolução	12
Cláusula 14. ^a	12
Penalidades contratuais.....	12
Cláusula 15. ^a	12
Força maior	12
Cláusula 16. ^a	13
Resolução por parte da AD-ABC.....	13
Cláusula 17. ^a	13
Resolução por parte do Adjudicatário	13
CAPÍTULO IV	14
SEGUROS.....	14
Cláusula 18. ^a	14
Seguros.....	14
CAPÍTULO V	14
Caução.....	14
Cláusula 19. ^a	14
Caução.....	14
CAPÍTULO VI.....	14
Disposições finais	14
Cláusula 20. ^a	14

Resolução de litígios - Foro competente	14
Cláusula 21.ª	15
Cessão da posição contratual	15
Cláusula 22.ª	15
Comunicações e notificações	15
Cláusula 23.ª	15
Contagem dos prazos	15
Cláusula 24.ª	15
Direito aplicável.....	15
ANEXO I	16
ESPECIFICAÇÕES TÉCNICAS	16

CAPÍTULO I

DISPOSIÇÕES GERAIS

Cláusula 1.^a

Objeto do Contrato

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 aquisição de Solução Data Center com hardware e licenciamento, firewall de perímetro e hardware diverso e solução de storage doravante, “equipamento” ou “bem”, conforme descrito no **Anexo I** (Especificações Técnicas).
2. De acordo com a nomenclatura de referência aplicável aos Contratos Públicos, CPV (Vocabulário Comum para os Contratos Públicos) adotada pelo Regulamento (CE) n.º 2195/2002, alterado pelo Regulamento (CE) n.º 213/2008 de 28 de novembro de 2007, o presente procedimento tem as seguintes classificações: 72500000-0, Serviços relacionados com a informática; 72511000-0, Serviços de software de gestão de rede; 72541000-9, Serviços de expansão informática; 30210000-4, Máquinas de processamento de dados (hardware); 30213100-6, Computadores portáteis e 30213300-8, Computadores de secretária (desktop computers).

Cláusula 2.^a

Entidade Adjudicante

A Entidade Adjudicante é a Associação para o Desenvolvimento do Centro Académico de Investigação e Formação Biomédica do Algarve, AD-ABC, associação de direito privado sem fins lucrativos, de índole académica e científica com o NIF 514 997 133, sita na Universidade do Algarve, Campus Gambelas – Edifício 2, 8005-139 Faro, com o número de telefone (+ 351) 289 244 476 e com o endereço eletrónico: abc@abcmedicalg.pt.

Cláusula 3.^a

Forma e documentos contratuais

1. O contrato será reduzido a escrito nos termos do n.º 1 do artigo 95.º do Código dos Contratos Públicos.
2. O Contrato é composto pelo respetivo clausulado contratual e seus anexos.
3. Fazem parte integrante do Contrato os seguintes documentos:
 - a. Os suprimimentos dos erros e omissões do Caderno de Encargos identificados pelo adjudicatário, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;

- b. Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c. O presente Caderno de Encargos e anexos;
 - d. A Proposta Adjudicada;
 - e. Os esclarecimentos à Proposta Adjudicada, prestados pelo Adjudicatário.
4. Em caso de divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem pela qual aí são indicados.
5. Em caso de divergência entre os documentos referidos no n.º 2 e as cláusulas do Contrato, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos (doravante designado abreviadamente de CCP), e aceites pelo Adjudicatário nos termos do disposto no artigo 101.º deste mesmo código.

Cláusula 4.ª

Gestor do Contrato

1. O acompanhamento da execução do contrato a celebrar, será efetuada pelo Presidente da Direção da AD-ABC Nuno Silva Marques.
2. O gestor do contrato tem por função o acompanhamento e avaliação do bom cumprimento do contrato nos termos do artigo 290.º A do CCP.

Cláusula 5.ª

Prazo de vigência do Contrato

O contrato produz efeitos, vinculando as partes, até à conclusão do fornecimento do bem adjudicado em conformidade com os respetivos termos e condições previstos no Caderno de Encargos e o disposto na Lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato, nomeadamente no que se refere ao dever de sigilo e, em especial, à obrigação pós-contratual de assistência técnica ao equipamento objeto do contrato no período pós-garantia e ao preço constante da proposta adjudicada.

CAPÍTULO II

OBRIGAÇÕES CONTRATUAIS

Secção I

Obrigações do Adjudicatário

Cláusula 6.ª

Obrigações gerais do Adjudicatário

1. O Adjudicatário obriga-se a executar o objeto do Contrato com absoluta subordinação aos princípios de ética profissional, isenção, independência, zelo e competência, de acordo com a adjudicação.
2. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas do contrato, decorre para o Adjudicatário a obrigação de fornecer o bem de acordo com as condições de fornecimento definidas nas cláusulas técnicas do presente caderno de encargos.
3. Constituem ainda obrigações do Adjudicatário:
 - a. Apresentar os documentos de habilitação a que está obrigado, nos termos do artigo 81.º do CCP;
 - b. Fornecer o equipamento conforme os requisitos técnicos, funcionais e ambientais mínimos, níveis de serviço e condições do fornecimento definidos neste Caderno de Encargos e demais documentos contratuais;
 - c. Obrigação de prestar assistência técnica sem quaisquer encargos adicionais para a entidade adjudicante, com as deslocações ou mão-de-obra, durante o prazo da garantia;
 - d. Fornecer o equipamento adjudicado nas instalações da AD-ABC, a indicar oportunamente, no prazo de 60 (sessenta) dias;
 - e. Obrigação de montar, instalar em condições de pleno funcionamento e demonstrar o equipamento identificado na sua proposta nas instalações da AD-ABC;
 - f. Obrigação de formação do pessoal técnico, tanto no que respeita ao seu funcionamento como no que respeita à sua conservação e reparação de avarias elementares, devendo apresentar um Plano de Formação que especifique o tipo de formação que entendam conveniente;
 - g. Comunicar antecipadamente à entidade adjudicante os factos que tornem total ou parcialmente impossível o fornecimento do equipamento ou o cumprimento de qualquer outra das suas obrigações, nos termos do contrato celebrado com a entidade adjudicante;
 - h. Não alterar as condições do fornecimento do equipamento previsto neste Caderno de Encargos;
 - i. Comunicar qualquer facto que ocorra durante a execução do contrato 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.

Cláusula 7.ª

Conformidade e garantia técnica

1. O equipamento objeto do contrato deve ser entregue em perfeitas condições de ser utilizado para os fins a que se destina e dotado de todo o material de apoio necessário à sua entrada em funcionamento.
2. O Adjudicatário é responsável perante a AD-ABC por qualquer defeito ou discrepância do equipamento objeto do contrato que existam no momento em que os mesmos lhe são entregues.
3. Nos termos da presente cláusula e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, o Adjudicatário garante os bens objeto do contrato, pelo prazo mínimo de 2 anos, contra quaisquer defeitos ou discrepâncias com as exigências legais e com características, especificações e requisitos técnicos definidos no Anexo I ao presente Caderno de Encargos.
4. Imediatamente após a AD-ABC ter detetado qualquer defeito ou discrepância do equipamento, deve notificar o Adjudicatário, para efeitos da respetiva reparação.
5. A reparação ou substituição previstas na presente cláusula devem ser realizadas dentro de um prazo razoável fixado pela AD-ABC e sem grave inconveniente para este último, tendo em conta a natureza do bem e o fim a que o mesmo se destina.
6. Durante o período de garantia do equipamento, o Adjudicatário fica ainda obrigado à realização do serviço de manutenção e de conservação (manutenção preventiva e corretiva) do mesmo, garantindo a sua atualização e operacionalidade, assumindo todos os custos associados.
7. O fornecedor deve também assegurar todas as obrigações relativas à manutenção e conservação dos equipamentos adicionais e de substituição, caso necessários, sem custos para a AD-ABC.

Cláusula 8.ª

Aceitação do equipamento

1. Caso o equipamento objeto do contrato, esteja em conformidade com as exigências do Caderno de Encargos e disposições gerais, e neles não sejam detetados quaisquer defeitos ou discrepâncias com as características definidas, deve a AD-ABC informar o Adjudicatário da aceitação do equipamento.
2. No caso de o equipamento não estar em conformidade a AD-ABC deve declarar, por escrito, e solicitar ao Adjudicatário a substituição do mesmo.
3. O equipamento objeto do contrato devem ser entregues na AD-ABC e colocado em funcionamento no prazo máximo de 40 (quarenta) dias a contar do início da produção de efeitos do contrato.

4. O Adjudicatário obriga-se a disponibilizar, simultaneamente com a entrega dos equipamentos objeto de contrato, todos os documentos em língua portuguesa ou inglesa, que sejam necessários para a boa e integral utilização ou funcionamento do equipamento.

Cláusula 9.ª

Dever de sigilo

1. O Adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao Contraente de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo 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.
4. O Adjudicatário deverá guardar sigilo quanto a informações que possa obter no âmbito da execução do presente contrato, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Cláusula 10.ª

Proteção de dados pessoais

1. A AD-ABC e o Adjudicatário assumem a obrigação de estrita confidencialidade relativamente a todos os dados pessoais de que venham a ter conhecimento no âmbito do contrato, extensiva à informação a que os seus trabalhadores, agentes, subcontratados e consultores tenham acesso, garantindo que os mesmos assumiram um compromisso de confidencialidade.
2. A AD-ABC e o Adjudicatário apenas podem transmitir dados pessoais a que tenham acesso por conta do contrato a terceiros, como seja Tribunal de Contas, plataformas eletrónicas de contratação, portal dos contratos públicos e outras entidades públicas ou privadas, com limitação dos dados transmitidos ao estritamente necessário e mediante as adequadas medidas de segurança.
3. O Adjudicatário encontra-se expressamente proibido de transmitir a terceiros dados pessoais de utentes e funcionários da AD-ABC.

4. A AD-ABC e o Adjudicatário obrigam-se a adotar todas as medidas organizativas, técnicas e de segurança necessárias e adequadas para assegurar a confidencialidade, o segredo e a preservação dos dados pessoais a que tenham acesso por conta do contrato, na medida e na extensão necessárias ao efeito, seja qual for o suporte utilizado.
5. Cada uma das partes no contrato presta assistência à outra, através de medidas técnicas e organizativas necessárias, para permitir que esta cumpra a sua obrigação de dar resposta aos pedidos realizados pelos titulares dos dados pessoais, para efeitos do exercício dos seus direitos, nomeadamente do direito de retificação, apagamento ou limitação do tratamento.
6. Com a cessação do contrato, o Adjudicatário, consoante a decisão da AD-ABC, devolve-lhe ou elimina todos os dados pessoais, apagando as cópias existentes, a menos que a conservação dos dados seja exigida abrigo do direito da União Europeia ou da legislação nacional.
7. Os dados pessoais relativos ao Adjudicatário, incluindo dos seus representantes, trabalhadores, agentes, subcontratados e consultores são eliminados no prazo de 4 anos, salvo exista obrigação legal ou contratual que justifique a conservação por prazo superior.

Secção II

Obrigações da AD-ABC

Cláusula 11.ª

Preço contratual

1. Pelo fornecimento do equipamento objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a AD-ABC deve pagar ao Adjudicatário, o preço da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço inclui todas as despesas que o Adjudicatário prevê realizar no fornecimento, como despesas com deslocações, alimentação, alojamento, despesas de aquisição, desalfandegamento, transporte, acondicionamento, armazenamento e manutenção de meios materiais, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.
3. O preço não será sujeito a qualquer atualização, variação ou alteração até ao termo da vigência do contrato.

Cláusula 12.ª

Preço Base do Procedimento

Pela aquisição do equipamento objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a AD-ABC, deve pagar ao Adjudicatário o preço de acordo com a proposta adjudicada, o qual não pode exceder para a totalidade das prestações que constituem o objeto do contrato, o montante global de 160.000,00 € (cento e sessenta mil euros).

Cláusula 13.ª

Condições de pagamento

1. A entidade adjudicante é exclusivamente responsável pelo pagamento do preço dos fornecimentos que lhes sejam efetuados.
2. O preço dos fornecimentos a prestar à entidade adjudicante é o que resultar do disposto no Caderno de Encargos e da proposta apresentada pela entidade fornecedora.
3. As quantias devidas pela AD-ABC, nos termos dos números anteriores, devem ser pagas no prazo de 60 (sessenta) dias após a receção pela AD-ABC das respetivas faturas, de acordo com o n.º 4 do artigo 299.º do CCP, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
4. Para os efeitos do número anterior, a obrigação considera-se vencida com a emissão da comunicação de aceitação pela AD-ABC.
5. A AD-ABC reserva-se no direito de não aprovar as faturas quando estas não respeitem o contrato ou o presente Caderno de Encargos.
6. Em caso de discordância por parte da AD-ABC, quanto aos valores indicados nas faturas, deve esta comunicar ao Adjudicatário, por escrito, no prazo máximo de 10 dias, os respetivos fundamentos, ficando o Adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
7. As faturas deverão ser emitidas em nome da AD-ABC, com referência aos documentos que lhe deram origem, devendo especificar:
 - a. Número do contrato;
 - b. Descrição dos bens fornecidos;
 - c. Valor respetivo dos bens, com discriminação das respetivas taxas praticadas.
 - d. A faturação está sujeita ao disposto no artigo 299.º B do Código dos Contratos Públicos.
 - e. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas serão pagas através de transferência bancária.

CAPÍTULO III

PENALIDADES CONTRATUAIS E RESOLUÇÃO

Cláusula 14.ª

Penalidades contratuais

1. Pelo incumprimento, cumprimento defeituoso ou mora no cumprimento de obrigações emergentes do contrato, o contraente pode exigir do Adjudicatário o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
 - a. Pelo incumprimento, cumprimento defeituoso ou mora no cumprimento das datas e prazos de resposta, até 10% do preço contratual;
 - b. Pelo incumprimento, cumprimento defeituoso ou mora no cumprimento da obrigação das demais obrigações emergentes do presente caderno de encargos até 5% do preço contratual;
2. Em caso de resolução do contrato por incumprimento do Adjudicatário, o contraente público pode exigir-lhe uma pena pecuniária de até 20% do preço contratual.
3. Em caso de resolução do contrato por incumprimento do Adjudicatário, a Contraente pode exigir-lhe uma pena pecuniária de até 10% do preço executado.
4. Na determinação da gravidade do incumprimento, o Contraente tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do Adjudicatário e as consequências do incumprimento.
5. O Contraente pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.
6. As penas pecuniárias previstas na presente cláusula não obstam a que o Contraente exija uma indemnização pelos danos correspondentes.

Cláusula 15.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: sismos, 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 do Adjudicatário ou a grupos de sociedades em que 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 correspondente ao impedimento resultante da força maior.

Cláusula 16.ª

Resolução por parte da AD-ABC

Sem prejuízo de outros fundamentos de resolução do Contrato previstos na Lei, a AD-ABC pode resolver o Contrato, a título sancionatório, sem formalidades, exceto a notificação pelo correio, sob registo, no caso do Adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, nos casos previstos no artigo 333.º do CCP.

Cláusula 17.ª

Resolução por parte do Adjudicatário

Sem prejuízo de outros fundamentos de resolução previstos na lei, o Adjudicatário pode resolver o Contrato nos casos previstos no artigo 332º do CCP.

CAPÍTULO IV

SEGUROS

Cláusula 18.^a

Seguros

1. É da responsabilidade do Adjudicatário a cobertura, através de contratos de seguro, dos seguintes riscos:
 - a. Danos do equipamento no transporte;
 - b. Prejuízos decorrentes das falhas de produção por avaria durante o prazo de garantia para além da disponibilidade operacional contratada.
2. A AD-ABC pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos no número anterior, devendo o Adjudicatário fornecê-la no prazo 5 (cinco) dias.

CAPÍTULO V

CAUÇÃO

Cláusula 19.^a

Caução

O valor da caução não é exigível, no termo do n.º 2 do artigo 88.º do CCP.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Cláusula 20.^a

Resolução de litígios - Foro competente

Para resolução de todos os litígios decorrentes quer da interpretação, quer da execução do Contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Loulé, com expressa renúncia a qualquer outro.

Cláusula 21.ª

Cessão da posição contratual

O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem a prévia autorização da entidade adjudicante; existindo autorização deve ser apresentada pelo cessionário toda a documentação exigida ao adjudicatário no presente procedimento.

Cláusula 22.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 CCP, 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, por escrito e por meio de carta com aviso de receção.

Cláusula 23.ª

Contagem dos prazos

Os prazos previstos no Contrato são contínuos, correndo em sábados, domingos e dias feriados, nos termos do n.º 3 do artigo 470.º do CCP.

Cláusula 24ª

Direito aplicável

Em tudo o que não se encontre expressamente previsto nas cláusulas deste Caderno de Encargos e respetivos Anexos os quais são parte integrante do Caderno de Encargos, aplicam-se as disposições constantes do CCP e restante legislação aplicável.

Assinado por : **NUNO SILVA MARQUES**
Num. de Identificação: BI113289421
Data: 2021.12.07 09:55:39+00'00'



Cofinanciado por:



ANEXO I

ESPECIFICAÇÕES TÉCNICAS

As presentes Especificações Técnicas são parte integrante do Caderno de Encargos do procedimento para aquisição de Solução Data Center com hardware e licenciamento, firewall de perímetro e hardware diverso e solução de storage no âmbito dos seguintes projetos: projeto nº 072586 - ALFA Score - Algarve Fit Ageing Score: uma nova ferramenta integrada para melhorar a qualidade de vida e o envelhecimento saudável; projeto nº 072682 - PtCAC Rede Nacional de Centros Académicos Clínicos Portuguese: Centro de Investigação de Excelência do Centro Académico de Investigação e Formação Biomédica do Algarve e projeto nº 072680 - PtCRIN - Portuguese Clinical Research infrastructure network - Desenvolvimento do Centro de Investigação Clínica Avançada e gestão de ensaios clínicos do Algarve, com as seguintes especificações técnicas mínimas dos bens/serviços a adquirir:

1. Todos os equipamentos propostos devem ser obrigatoriamente do mesmo Fornecedor por conjunto de equipamentos.
2. O equipamento proposto deve incluir garantia do fabricante pelo período mínimo de 2 anos.
3. O equipamento proposto deve ser obrigatoriamente “novo”, não sendo aceites equipamento “refeito” ou “usado”.
4. O adjudicatário tem obrigatoriamente que responder a todo o conjunto de equipamentos constantes neste Anexo.
5. No âmbito do presente procedimento, a proposta comercial, declarações, documentos técnicos ou outros documentos que se considerem importantes juntar tais como brochuras ou certificações, entregues pelo adjudicatário devem ser redigidos em língua portuguesa ou inglesa ou não o sendo, devem ser acompanhados de tradução devidamente legalizada e em relação à qual o Adjudicatário declara aceitar a prevalência, para todos os efeitos, sobre os respetivos originais.
6. Custos de transporte, alfandegários, entrega e instalação do equipamento estão incluídos no preço base do procedimento.

Equipamento a Adquirir: Solução Data Center com hardware e licenciamento, firewall de perímetro e hardware diverso e solução de storage

Especificações técnicas:

1. Solução centro de dados

1.1. Servidores “Rackmount”, montagem em bastidor:

Mínimo de 3 servidores cada um com as seguintes características mínimas:

- a) 2 CPU de 16 Cores, Intel com pelo menos 2.30 Ghz e 22 MB de Cache;
- b) Altura máxima em bastidor: 2U;
- c) Capacidade RAM de 256GB, com velocidade de 2933 Mhz e com capacidade de expansão a 1.54TB de RAM distribuídos por 24 slots DIMM;
- d) 2 Discos Hot-Plug de 240 GB SATA SSD SFF e deverá apresentar escalabilidade interna para um mínimo de 8 discos, os quais deverão ter um indicador de utilização (para evitar perda de dados ou downtime, devido a remoção indevida de discos);
- e) Controladora RAID, com 2 GB de Cache protegida por bateria, e com capacidade para RAID 1 & 10 (Drive Mirroring), RAID 5, RAID 50, RAID 6 e RAID 60, RAID 1 & 10 com terceiro disco para paridade;
- f) Os servidores propostos deverão ser suportados para utilização em Rack. Deverão suportar a instalação de calhas adequadas para o efeito e incluir braço condutor de cablagem
- g) Deverá incluir duas fontes de alimentação redundantes e Hot-Plug de 800W;
- h) Conectividade USB 3.0 com disponibilização de 5 portas, sendo pelo menos uma interna, um frontal e uma porta USB frontal para efeitos de gestão;
- i) Disponibilização de um sistema de suporte preditivo cloud-based, sem custos, com capacidade de suporte e de recomendações proactivas para impedir a ocorrência de problemas;
- j) Suporte para uma porta dedicada a Gestão remota, com capacidade de federação – Capacidade de efetuar a gestão de vários servidores como se tratasse de apenas um, implementando pelo menos as seguintes definições: controlo energético, atualizações de firmware, configurações na Bios, virtual media de modo unificado;
- k) Incluir capacidade e licenciamento (caso exista) para consola remota com Virtual KVM Web-Based e capacidade para 6 users concorrentes, Virtual Power, Virtual Media (DVD, PEN USB ou pasta de ficheiros), acesso seguro SSL/AES/RC4, Consola SSH, Acesso a consola remota em modo pre-boot (antes do arranque do OS);
- l) Capacidade de assegurar que o servidor não executa código de firmware que possa estar comprometido, bem como capacidade para fazer rollback para o firmware de fábrica, através do Silicon Root of Trust;
- m) Suporte para UEFI e RESTful API;
- n) Suporte para pelo menos os seguintes Sistemas Operativos: Windows Server 2012 R2, Windows Server 2016, VMware ESXi 6.0 U3, VMware ESXi 6.5, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES);
- o) Certificação Energy Star, Microsoft LOGO Certifications;

Cofinanciado por:

1.2. Sistema de armazenamento principal

Array de discos com as seguintes especificações mínimas:

Plataforma

1. O armazenamento proposto deve ser uma plataforma de armazenamento de próxima geração que deve oferecer as funcionalidades de ambos convergentes e hiperconvergentes com escalonamento independente do armazenamento e da computação sem qualquer tempo de downtime.
2. A solução proposta deve ter total independência para o crescimento da plataforma de computação e armazenamento. O crescimento de ambos os componentes devem ser completamente independentes, sem qualquer operação imediata de rebalancear a informação nos discos.

Suporte de Hypervisor

A solução proposta deve fornecer a simplicidade da hiperconvergência de um Hypervisor bem conhecido, como VMware/Microsoft/Linux Platform, juntamente com as licenças necessárias de acordo com as especificações e requisitos abaixo.

1. A solução proposta deve ser fornecida com pelo menos 3 número de nó de computação em um único cluster, escalável para pelo menos 32, junto **com a capacidade de 46 TB de armazenamento**.
2. Cada nó de computação deve ter flexibilidade para ver e consumir toda a capacidade da camada de armazenamento.
3. Cada nó de computação deve ser fornecido com pelo menos 4 portas IP de 10 Gbps, 4 portas IP de 1 Gbps, 256 GB de memória escalável para pelo menos 1.54TB, junto com 2 processadores com 2,13Ghz e 16 cores. Cada nó de computação deve ter pelo menos duas unidades de 240 GB para sistema operativo. O nó de computação proposto também deve suportar portas IP de 25 Gbps e 100 Gbps.
4. A solução proposta também deve ser fornecida com cache/memória adicional de 128 GB para operações de leitura e gravação na camada de armazenamento.

Gestão

1. A plataforma completa deve ser gerida diretamente a partir da consola de gestão do hypervisor proposto e não deve exigir várias ferramentas de gestão para as operações do dia a dia.
2. Cada nó de computação deve ter uma porta de rede adicional para acesso e gestão remota. A gestão remota deve ter memória flash própria dedicada.
3. Cada nó de computação deve ter um silício de segurança imutável, **Silicon Root of Trust**, para garantir que, em qualquer situação - o firmware seja totalmente à prova de falsificação e em qualquer estágio não possa ser comprometido.

Data Protection

1. A solução proposta deve usar todos os discos flash apenas para o sistema de armazenamento. Todos os discos Flash propostos no sistema de armazenamento devem ser configurados com RAID por hardware com resiliência que permita pelo menos três falhas de disco, em simultâneo, ou então um fator de replicação 3 (RF-3) para a capacidade útil, em caso de o RAID por hardware não for suportado pelo licitante.
2. A falha de qualquer nó de computação não deve reduzir o número total de unidades propostas. Caso o fornecedor não ofereça suporte a esse recurso, um nó adicional com a mesma configuração em termos de computação e armazenamento deve ser fornecido.

Cofinanciado por:

Performance

1. A solução proposta deve ter flexibilidade para utilizar todas as unidades propostas no sistema de armazenamento para uma determinada máquina virtual para operações de leitura e gravação e não deve ser limitada à alocação de nó local.
2. Não deve haver degradação de desempenho durante atividades críticas de suporte, como atualização de firmware, atualização de patch, etc.
3. Para um desempenho máximo e impacto mínimo no uso da capacidade flash, a solução proposta deve ter a capacidade de gravar sempre um strip size de pelo menos 10 MB no sistema de armazenamento.
4. O fornecedor deve fornecer 20% da capacidade adicional dentro da plataforma se o tamanho do stripe size de back-end for inferior a 10 MB.

Sem Single Point of Failure

1. A solução proposta não deve ser configurada com nenhum ponto de falha. O fornecedor deve desenhar uma solução de forma que o sistema de armazenamento forneça pelo menos 6 noves de disponibilidade de dados e a disponibilidade de VM seja assegurada por meio do cluster de hypervisor proposto.
2. Não deve haver degradação de desempenho no sistema de armazenamento devido a um único componente ou falha do nó de armazenamento. O fornecedor deve fornecer uma prova documentada para o mesmo.

CPU e discos suportados

A solução proposta deve ter a capacidade de suportar processadores *Intel Skylake*, bem como processadores *Cascade Lake* e várias capacidades de flash dentro do mesmo cluster.

Sistema de monitorização em cloud, suporte IA e analítica

1. A solução proposta deve ter monitorização através da cloud, com suporte de IA (inteligência artificial) e mecanismos de análise para gestão proativa e mitigação de riscos. Todas as licenças necessárias para a mesma devem ser incluídas na solução.
2. A monitorização, através da cloud, com suporte de IA e mecanismos de análise devem ter capacidade para fornecer o seguinte:
 - a. Fornecer recomendações de atualização de firmware e atualização de patch de forma proativa e com conhecimento da infraestrutura periférica ligada à plataforma.
 - b. Impedir automaticamente a instalação de firmware que possa entrar em conflito com outros componentes da infraestrutura ligados ao sistema de armazenamento.
 - c. Fornecer informação histórica de capacidade ao minuto extremamente granular e análise de tendência de desempenho por defeito, sem a necessidade de habilitar logging adicional, instalar qualquer dispositivo (físico ou virtual) ou instalar qualquer software adicional.
 - d. A análise de desempenho deve ser capaz de dividir o I/O em histogramas por tamanho de I/O, identificar I/O sequencial versus aleatório e fornecer recomendações baseadas em IA para corrigir problemas de desempenho.
 - e. Elimine a necessidade de o cliente fornecer logs para suporte, uma vez que o suporte terá as informações necessárias enviadas automaticamente pela plataforma.

Cofinanciado por:

- f. Deve fornecer um histórico de casos de suporte registados com a equipa de suporte com informação de eficiência operacional. Deve ser clara a demonstração da percentagem de casos de suporte que foram encerrados automaticamente vs manualmente.
- g. Deve ser capaz de fornecer um resumo executivo único cobrindo os vários aspectos críticos e obrigatórios da economia de espaço de tecnologias de redução de dados.
- h. Forneça recomendações de atualização automática para software e hardware, com instruções específicas sobre o que precisa ser atualizado e quando.

Cloud Enabled – Analítica

O mecanismo de análise habilitado para cloud deve ter a capacidade de fornecer o seguinte:

- a. Deve ter capacidade de aprendizagem global - mecanismo analítico deve recolher informações de controle da base instalada de fornecedores de diferentes clientes para resultados significativos. O vendedor deve fornecer a prova documental para isso.
- b. O mecanismo de análise deve ter capacidade de fazer recomendações proativas para evitar as questões/problemas observados numa outra base instalada do fornecedor após a identificação da assinatura problemática.

Quality of Service

- 1. A solução proposta deve suportar e ser fornecida com Quality of Services (QoS) para controlar os IOPS e MB/s para um determinado datastore.
- 2. A solução proposta deve fazer QoS automaticamente para evitar que uma única carga de trabalho assuma todo o desempenho do sistema de armazenamento.

Thin Provisioning e otimização de espaço

- 1. A solução proposta deve suportar recursos críticos de eficiência de dados globais - deduplicação e compressão inline e thin provisioning sem qualquer degradação de desempenho
- 2. Todos os recursos de eficiência de dados acima referidos devem ser verdadeiramente globais e devem ter capacidade para comparar chunks em todas as VMs e datastores habilitados/criados na plataforma.
- 3. A solução proposta deve suportar tanto datastores não duplicados quanto datastores duplicados ao mesmo tempo dentro da plataforma.
- 4. A solução proposta deve suportar datastores não comprimidos e comprimidos ao mesmo tempo dentro da plataforma.

Snapshot/Point in time copy/Zero Copy Clone/Thin Clone e Backups integrados

- 1. A solução proposta deve suportar mais de 1000 snapshots para um determinado datastore. O fornecedor deve usar tecnologia de desempenho eficiente como re-direct on write ou melhor.
- 2. A solução proposta deve suportar backup online para máquinas virtuais críticas usando snapshots de aplicação consistentes. Qualquer licença necessária para a mesma deve ser fornecida para toda a capacidade

suportada da plataforma. Todos os snapshots criados também devem suportar a de-duplicação e compactação globais.

3. A solução proposta deve ter uma política de backup de snapshots separada entre a produção e o site de DR.
4. A solução proposta deve suportar múltiplas sessões de snapshots, clones ou replicações sem qualquer impacto no desempenho.

Integridade dos dados e encriptação

1. A solução proposta deve oferecer checksums que vão além do padrão T10-PI. As checksums irão detectar e prevenir automaticamente erros resultantes de leituras ou gravações perdidas/mal colocadas que T10-PI e sistemas de checksum equivalentes não podem corrigir
2. A solução proposta deve ser fornecida com encriptação certificada AES-256 XTS FIPS em nível de armazenamento de dados granular sem o uso de unidades flash encriptadas.

Licenciamento

O fornecedor deve fornecer a licença para todas as funcionalidades críticas, como expansão de capacidade, snapshots, snapshots geridos por aplicações, clone fino, replicação e QOS, etc. para a capacidade máxima suportada pela plataforma. Não haverá nenhum requisito de licença de software adicional para futura atualização de capacidade. Qualquer licença adicional necessária para atender às especificações do RFP também deve ser proposta antecipadamente.

1.3. Sistema de armazenamento backups e arquivo

Servidor com as seguintes características mínimas:

O dispositivo de backup de disco para disco, D2D, proposto deve ter espaço eficiente e a unidade controladora não deve consumir mais de 2U de espaço em rack. O dispositivo proposto deve ser certificado para funcionar com pelo menos 3 fornecedores de aplicações de backup ISV, como HPE, Veritas, Dell-EMC, Veeam, Commvault etc.

O dispositivo proposto deve ser proposto com um mínimo de 48 TB de espaço bruto, escalável a 108TB.

O dispositivo proposto deve ter discos dedicados e separados para o sistema operativo do dispositivo e não deve participar no backup de dados.

O dispositivo proposto também deve ser escalável para pelo menos 100 TB úteis no modo nativo (sem eliminação de duplicação e compressão) e 200 TB adicionais de capacidade utilizável nativa usando armazenamento na nuvem como AWS, Azure ou em armazenamento de objeto.

O fornecedor não deve usar nenhum dispositivo de teste adicional no meio ao mover os dados do dispositivo de backup baseado em disco para nuvem pública ou armazenamento de objeto.

O dispositivo proposto deve ser protegido com hardware RAID 6 de fábrica para que nenhuma configuração RAID seja necessária on site.

O dispositivo proposto deve suportar a emulação de targets VTL e NAS como CIFS.

O dispositivo proposto deve ter a capacidade de fazer uma cópia completa de data sets do armazenamento de backup em disco local para o armazenamento em nuvem, em vez de data tiering.

O dispositivo proposto deve ter a capacidade de configurar pelo menos uma combinação de 20 tape librarys e target NAS junto com 20.000 ou mais slots de cartridge num único dispositivo.

O dispositivo proposto deve ter capacidade para fornecer restore seletivo da própria library de disco.

O dispositivo proposto deve integrar e utilizar a infraestrutura de backup em tape atual do cliente nos seguintes aspetos:

a. Compatibilidade com o servidor de backup/servidores de mídia existentes no cliente.

b. Compatibilidade com biblioteca de fitas e unidades de fita existentes

c. Compatibilidade com software de backup existente"

O dispositivo proposto deve ter licença integrada de de-duplicação, licença de replicação de baixa largura de banda, de forma que apenas blocos não duplicados exclusivos sejam transferidos para uma localização remota/DR.

O dispositivo proposto deve ter inteligência para entender a de-duplicação com base na origem e no destino e deve ser integrado a todos os ISVs de backup conhecidos, como Veritas, Commvault e Veeam, etc. Pelo menos 3 ISVs devem ser suportados.

O dispositivo proposto deve suportar o receber dados não duplicados de locais remotos ou filiais diretamente dos servidores de aplicações/servidores do cliente em modo de baixa largura de banda, sem usar nenhum dispositivo baseado em backup ou replicação em locais remotos/filiais.

Capacidade de emular com flexibilidade os formatos de unidade/fita LTO-Gen5, LTO-Gen6 e LTO-Gen7 etc.

O dispositivo proposto deve ter um mínimo de 2 x 10 Gbps IP. Licença e SFP para todas as portas devem ser propostos e configurados.

O dispositivo de backup baseado em disco proposto também deve suportar a funcionalidade de encriptação.

O dispositivo de backup baseado em disco proposto deve suportar VLAN tagging. As portas IP propostas do mesmo tipo também devem suportar Port bonding em Adaptive Load Balancing assim como mode Ativo de backup.

O dispositivo proposto deve suportar desempenho de gravação de pelo menos 7 TB por hora no modo nativo.

O dispositivo proposto deve suportar desempenho de gravação, quando habilitado com de-duplicação na origem, de pelo menos 16 TB/h.

1.4. Rede:

Switchs com as seguintes características mínimas:

- a) Mínimo de 2 switchs de dados, cada um com pelo menos 18 portas de downlink a 25 Gb/s e pelo menos 4 portas de uplink a 100Gb/s com fontes de alimentação redundantes:
 - a. Altura máxima em bastidor: 1U
 - b. Capacidade de switching mínima de 1.7 Tb/s
 - c. Capacidade de processamento mínima de 1.26 Bpps
 - d. Latência máxima de 300ns
- b) Switch de gestão com mínimo de 24 portas 10 Gbit Base-T e 2 portas 10 Gbit SFP+;

A solução global deverá apresentar:

- a) Capacidade de gestão da solução através de uma única interface – interface de gestão do hypervisor utilizado;
- b) Essa interface única deverá permitir a gestão dos recursos de computação (cores e RAM) e os recursos de Storage num único dashboard, um single pane of glass
- c) Deverá ser incluído licenciamento de Software de Virtualização que permita VMs ilimitadas e que disponibilize o mesmo nível de suporte que o Hardware.

1.5. Serviços de suporte e manutenção para o centro de dados do ABC

Os serviços de Manutenção de hardware e software deverão ser prestados para uma duração de 3 anos, com abertura de chamada automática via ligação segura https;

- a) A manutenção deverá ser assegurada pelo fabricante dos equipamentos;
- b) A reparação de Hardware deverá apenas ser realizada com peças genuínas do fabricante dos equipamentos;
- c) Deve ser implementada uma solução de suporte para permitir a abertura automática de chamadas, no caso de incidentes de falha ou pré-falha de algum componente.
- d) Disponibilização de um portal/ferramenta que permite uma visão global e em tempo real do estado de suporte de todos os equipamentos registados. Deverá também permitir a abertura de chamadas de suporte e o acompanhamento de todos os casos abertos.

2. Licenciamento de software centro de dados;

2.1. Sistema operativo servidor

Deverá privilegiar a utilização de interfaces gráficas nas suas consolas de administração e gestão e não requerer serviços de configuração e administração especializados. A implementação total do sistema operativo deverá requerer apenas configuração de componentes e não qualquer tipo de desenvolvimento à medida ou compilação de software:

- **Funcionalidade de servidor de ficheiros:** O sistema operativo servidor pretendido deve ter nativamente funções de servidor de ficheiros para postos de trabalho sem necessidade de software adicional. Deverá ter a capacidade nativa de cifra dos dados transportados na rede, definição de quotas de espaço em disco por utilizador e controlo dinâmico de políticas de classificação e segurança da informação armazenada no servidor. Suporte nativo para cluster por software de sistemas de ficheiros e deduplication;
- **Funcionalidade de servidor de directório de utilizadores:** O sistema operativo servidor deverá ter nativamente a capacidade de implementação de um directório de utilizadores que suporte as interfaces e standards LDAP e utilize como protocolo de autenticação o Kerberos. A autenticação também deverá ser possível através do uso de smartcards. Este directório deverá ter características de alta disponibilidade com replicação automática de dados entre várias instâncias que podem estar fisicamente distantes entre si (entre instalações físicas distintas separadas por ligações WAN). Este directório deverá ter integração nativa com redes de postos de trabalho e deverá ser gerido por meio de configurações administradas por interfaces gráficas não necessitando de desenvolvimentos à medida ou compilação de software específico para a solução pretendida;
- **Funcionalidade de servidor web:** O sistema operativo servidor deverá oferecer capacidades nativas de servidor Web HTTP/S suportando linguagens e rotinas de desenvolvimento múltiplas. Deverá ter capacidade para albergar múltiplos sites em simultâneo com autenticação integrada com os postos de trabalho com autenticação kerberos;
- **Funcionalidade de servidor de virtualização:** O sistema operativo servidor deverá ter capacidades nativas de motor de virtualização de servidores e postos de trabalho sem necessidade de adição de software ou desenvolvimentos/compilação de software à medida. Deverá ter suporte para virtualizar servidores com sistemas operativos Windows e Linux com integração nativa sem necessidade de software adicional. A virtualização integrada no sistema operativo servidor deverá ter capacidades nativas de alta disponibilidade e possibilitar a movimentação de máquinas virtuais entre servidores sem quebra de serviço bem como satisfazer cenários de recuperação de desastres sem necessidade de software ou hardware específico e adicional. Deverá suportar discos virtuais até 92 TB;
- **Funcionalidades de acesso remoto:** O sistema operativo servidor deverá fornecer de uma forma integrada como funcionalidades base, capacidades de acesso remoto disponíveis para postos de trabalho móveis ou localizações distantes do servidor via Internet ou linha comunicações temporária. Este servidor deverá ser capaz de fornecer serviços de Virtual Private Network (para computador individual ou entre sites – site-to-site VPN), IP Router, Network Address Translation e acesso remoto automático sem VPN (autenticação IPsec). A autenticação dos utilizadores e computadores deverá ser possível por intermédio de username/password, certificados e OTP – One Time Passwords. Deverá suportar os seguintes protocolos de túnel a usar nos acessos remotos: PPTP, L2TP/IPSEC;

- Funcionalidade de sessão remota: O sistema operativo servidor deverá ser capaz de fornecer a capacidade de criar sessões de utilizador (administrador ou utilizador normal) iniciadas a partir de postos de trabalho. Nestas sessões de utilizador no servidor, é fornecida uma interface gráfica remota semelhante ao Microsoft Windows onde o utilizador poderá realizar acções de produtividade pessoal como seja a escrita de um documento ou executar uma aplicação existente na organização. Pretende-se que todo o esforço de computação das aplicações seja realizado no hardware servidor. O acesso por parte do utilizador deverá ter a capacidade de ser utilizado a partir da Internet e com comunicações cifradas com certificado digital;
- Capacidades de acesso remoto: funcionalidades nativas de VPN através dos protocolos PPTP, L2TP/IPSEC, SSL HTTPS;
- Funcionalidade de servidor de serviços básicos de rede: O sistema operativo deverá ter como funcionalidades básicas e integradas, os serviços de gestão de endereçamento IP (DHCP) e resolução de nomes (DNS). Os serviços deverão ter a capacidade de implementação em modelo de alta disponibilidade com base em múltiplos servidores. A autorização de activação de servidores de DHCP e de registo nos servidores de DNS deverá ser integrada com a Microsoft Active Directory.

2.2. Software de backups de infraestrutura e software de virtualização

Licenciamento pelo período de três anos, do software Veeam Backup Essentials Enterprise Plus e do software VMware vSphere Essencial Plus Kit 6P E-LTU, ou equivalente, nomeadamente no que diz respeito a:

- Plataforma única para ambientes virtuais, físicos e na nuvem;
- Portabilidade de licenças;
- Restauração de uma máquina inteira, de discos e de arquivos de sistema operativo instalado;
- Recuperação instantânea entre plataforma para qualquer carga de trabalho;
- Recuperação de itns de aplicação sem agente;
- Restauração para nuvem pública e storage de objetos;
- Backup sem agente, com detecção de aplicações e baseados em imagem;
- Cópias de backup;
- Backup e recuperação a partir de storage snapshots;
- Possibilidade de cópia de backups para a nuvem e para o storage de objetos;
- Testes de backup e verificação de recuperação automatizados;
- Backup e recuperação de NAS escaláveis e agnósticos em relação ao storage;
- Imutabilidade para proteção contra ransomware;
- Monitorização e relatórios avançados;
- Replicação de VM's baseada em imagem;
- Suporte nativo a fitas;

- Hipervisor de gestão e de arquitectura que permita a partilha de recursos de hardware por parte das máquinas virtuais;
- Possibilidade de criação de máquinas virtuais até quatro CPU's virtuais;
- As máquinas virtuais devem aceder a dispositivos de armazenamento compartilhado (Fiber Channel, iSCSI, etc.) e é uma chave permitindo tecnologia para outros componentes, como VMware/vSphere Storage vMotion®;

3. Firewall de perímetro de segurança;

3.1. Âmbito da solução pretendida

Pretende-se adquirir uma solução de firewall com as seguintes funcionalidades:

- Prevenção de ataques de dia zero
- Bloqueio de ligações a bot net
- Mitigação de vulnerabilidades conhecidas
- Bloqueio de acesso a sites em termos globais ou por grupo de utilizadores
- Permita acesso remoto a infraestrutura
- Aplicação movel que permita a receção de alertas e visualização do estado da infraestrutura em tempo real
- Retenção de Log's em plataforma externa que permita:
 - Consulta dos log's
 - Retenção de pelo menos 60 dias
- Envio de relatórios periódicos com:
 - Informação focada nos ataques que a plataforma foi alvo
 - Tipificação do tráfego benigno e malicioso

A solução a propor deve ter em conta a possibilidade de evolução para gestão centralizada.

3.1.1. Requisitos genéricos

- a. O fabricante deverá endereçar todos os requisitos de um equipamento de segurança (Firewall), tais como processamento de largura de banda, número de ligações, capacidade de securização de aplicações de nova geração em todas as vertentes da rede (escritório, centro de dados) num único equipamento;
- b. O fabricante deverá disponibilizar as mesmas funcionalidades de inspeção avançada (Firewall, intrusion prevention, application control, URL filtering, Anti-Bot, Anti-Virus, Sandboxing) em modelo físico e virtual, quaisquer destas com a possibilidade de gestão por uma única consola central e dedicada;
- c. A solução proposta, deverá endereçar todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante (single vendor):
 - i. Statefull Inspection Firewall - A gateway deverá inspecionar end-to-end (não apenas "half-way" ou "header") todos os fluxos de comunicação desde o estabelecimento da sessão (3-way handshake TCP), durante a transferência de informação (payload), até que esta seja terminada;
 - ii. Intrusion Prevention System;
 - iii. User Identity Acquisition
 - iv. Application Control and URL filtering
 - v. Anti – Bot / Anti – Virus
 - vi. Threat Emulation (Sandboxing)

Cofinanciado por:

- vii. Anti – Spam and Email Security
 - viii. IPSec VPN
 - ix. Remote Access VPN (Mobile Access)
 - x. Logging and Status
- d. A solução proposta, não poderá em momento algum “sacrificar” a segurança em detrimento da performance (desabilitar inspeção end-to-end em cenários de “carga” na plataforma);
- e. A solução proposta deverá conter uma plataforma externa que permita:
- i. Armazenamento de Log’s, retenção mínima de 60 dias;
 - ii. Consulta de Logs
 - iii. De futuro permitir gestão e acesso á solução

3.1.2 Requisitos de Performance e Hardware

A appliance a propor terá de cumprir os requisitos mínimos abaixo descritos:

a. Requisitos de Performance

Parâmetro	Métrica
Threat Prevention	>=1.4 Gbps
NextGen Firewall	>=3.1 Gbps
Intrusion Prevention System	>= 3.4 Gbps
VPN Throughput	>= 3.1 Gbps
Firewall Throughput	>= 8.5 Gbps
Connections per second	55k
Concurrent Connections	2.4 M
Vlans	100 interfaces vlan

b. Requisitos de Hardware

- Energia:

Parâmetro	Métrica
Fontes de alimentação redundantes	não
Consumo Máximo	72W
Valor máximo de emissão de calor	244.31BTU/hr

- Dimensões máximas:

Parâmetro	Métrica
Peso	6,17kg
Ocupação no Bastidor	1RU
Dimensões (WxDxH)	430 x 300 x 44.2 mm

- Interfaces:

Parâmetro	Métrica
Porta de Consola - USB Type-C	Sim
Porta de Consola - RJ45	sim
Interfaces Gigabit Dual Cobre/Fibra	2
Interfaces Gigabit Base T	16
USB 3.0	2

3.1.3 Requisitos para a plataforma de Monitorização e visualização de Logs

- A solução deverá ter a capacidade de consolidar os logs de todas as componentes de segurança que se encontrem ativas na plataforma: IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, User Identity, Mobile Access;
- Os logs deverão ser transferidos de forma segura entre a gateway e o log server
- A solução deverá permitir no mínimo o arquivo de 60 dias de Log's

3.1.4 Requisitos para a aplicação de gestão móvel

- A aplicação deverá permitir em tempo real verificar se existem atualização para os varos serviços e permitir que o utilizador os efetue.
- Verificar os eventos de segurança
- Notificar sobre a existência de novos dispositivos na infraestrutura, e permitir o seu bloqueio
- Notificar comportamento maliciosos e bloquear as respetivas origens
- Consultar o histórico de alertas
- Visualizar o estado do acesso ou acessos internet

3.1.5 Requisitos de firewall

a. Requisitos - Funcionalidades de rede

- Suporte para protocolos de agregação de links (LACP 802.3ad);
- Suporte para funcionamento em modo L2 (bridging) e L3 (routing);
- Suporte de NAT
 - Static, Hide, PAT;
 - NAT44, NAT46, NAT64, NAT66;
- Suporte para routing estático;
- Suporte para Policy Based Routing (PBR);
- Suporte para protocolos de routing dinâmico:
 - BGP, OSPF, RIP;

b. Requisitos de alta disponibilidade

- A solução deve permitir a evolução para alta disponibilidade, com os seguintes requisitos:
 - Activo/Passivo ou Activo/Standby
 - VRRP ou IP Virtual;
 - Failover:
 - Falhas de routing;
 - Falhas de dispositivo;
 - Falhas de link;
 - Sincronização de sessões entre membros do cluster;

c. Requisitos técnicos/lógicos

- O equipamento de segurança, deve utilizar a tecnologia de **Stateful Inspection**, para construir e manter a tabela de sessões (fluxos de comunicação).
- O Equipamento de segurança deve ser capaz de suportar o debito, número de novas ligações e manutenção das mesmas de acordo com as necessidades do cliente.
- A solução deve identificar/controlar o acesso de pelo menos 150 serviços/protocolos.
- A solução tem de suportar que se apliquem regras em intervalos de tempo, para que seja possível definir o tempo útil das mesmas.
- A Firewall tem de suportar métodos de autenticação por sessão, utilizadores e clientes.
- A solução tem de ter base de dados de utilizadores local, para permitir a autenticação e autorização dos mesmos sem recurso a um dispositivo externo;
- A solução tem de suportar as funções de DHCP server e Relay;
- A solução tem de ter capacidade de trabalhar em modo transparente/Bridge (L2)
- A solução tem de suportar alta disponibilidade ou load-sharing e sincronização de estados entre os dois membros do cluster;

3.1.6 Sistema de prevenção de intrusões (IPS)

- O fabricante deve fornecer evidências da sua posição de liderança, ano após ano, no Quadrante Mágico do Gartner para:
 - Soluções de Prevenção de Intrusão
 - Soluções de Firewall Enterprise
- O IPS deve ser baseado nos seguintes mecanismos de deteção:
 - Assinaturas
 - Anomalias no protocolo
 - Controlo Aplicacional
 - Análise de comportamento
- Os Módulos de IPS e firewall devem estar integrados na mesma plataforma.

- O administrador deve ter a possibilidade de configurar a inspeção para proteção apenas da rede interna
- O IPS deve ter um mecanismo fail-open baseado em software, ajustável com base em limites do gateway, CPU ou utilização de memória.
- O IPS deve ter mecanismo automático para ativar ou gerir as novas assinaturas após atualizações.
- O IPS deve suportar exceções com base em origem, destino, protocolo, ou uma combinação dos três
- O IPS deve permitir mudar para o modo de deteção, sem alterar parâmetros individuais, por forma a facilitar as ações de troubleshooting.
- O administrador deve poder ativar de forma automática novas proteções, com base em parâmetros configuráveis
 - impacto no desempenho
 - Grau de severidade da ameaça
 - nível de confiança
 - proteções do cliente
 - proteções do servidor
- O IPS deve ser capaz de detetar e prevenir os seguintes tipos de ameaça:
 - uso indevido de protocolo
 - comunicações de malware
 - tentativas de uso de protocolos de tunneling
 - tipos genéricos de ataque sem assinaturas predefinidas.
- Para cada proteção, a solução deve incluir o tipo de proteção (relativamente a servidor ou cliente)
 - gravidade da ameaça
 - impacto no desempenho
 - nível de confiança
 - referência - (ie CVE)
- O IPS deve ser capaz de detetar e bloquear ataques nas layers de network e application layer, protegendo pelo menos os seguintes tipos de serviços:
 - Serviços de email
 - DNS
 - FTP
- O fornecedor deve fornecer evidências de liderança na proteção de vulnerabilidades Microsoft
- O IPS e/ou o Application Control deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (Anonymizers)
- O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou hosts.
- A solução deve proteger DNS Cache Poisoning e impedir o acesso dos utilizadores a endereços de domínio bloqueados
- Solução deve fornecer proteções para protocolos VOIP
- O IPS e/ou o Application Control devem detetar e bloquear aplicações que permitam controlo remotos, incluindo as que são capazes de realizar tunneling sobre o tráfego HTTP
- IPS deve ter proteções SCADA
- A solução deve permitir ao administrador bloquear de forma fácil o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os intervalos de IP correspondentes ao país

3.1.7 Aquisição de identidade de utilizadores (User ID Acquisition)

- Deve ser capaz de adquirir a identidade dos utilizadores, com base na consulta dos eventos de segurança da Microsoft Active Directory
- Deve ser possível a autenticação através de uma browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio.
- A solução deve integrar-se perfeitamente com Microsoft Active Directory
- O impacto do uso da solução de aquisição de identidade no CPU das AD, deve ser inferior a 3%.
- Deve ser capaz de adquirir a identidade de um utilizador presente numa Microsoft Active Directory sem qualquer tipo de agente instalado no controlador de domínio
- Deve ser capaz de criar identity roles (grupos de identidades) para serem invocados em diferentes aplicações da solução.

3.1.8 Controlo de aplicações e acesso a sites

- A solução deve reconhecer e controlar mais de 6000 aplicações conhecidas
- A base de dados da solução deve conter mais de 200 milhões de URL's categorizados, abrangendo mais de 85% da Alexa's top 1M sites
- A solução deve permitir criar uma regra de filtragem de conteúdos com várias categorias
- A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL
- A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias.
- A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores
- A solução, após 4 semanas de produção, deve ter em cache cerca de 99% das solicitações de categorização.
- A solução deve ter uma interface fácil de pesquisa de aplicações e URL's
- A solução deve categorizar aplicações e URL's por fator de risco
- A política de URLF e Application Control deve poder ser definida por identidade do utilizador
- A base de dados de URLF e Application Control devem ser atualizados por um serviço Cloud
- A solução deve ter o controlo de aplicações e URLF unificado na mesma política.
- A solução deve ter mecanismos para informar ou perguntar ao utilizador em tempo real, para os educar ou para confirmarem as suas ações com base na política de segurança
- A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda
- A solução deve permitir exceções com base em objetos de rede previamente definidos
- A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação.
- A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria
- A solução deve fornecer um mecanismo de substituição na categorização de URL

3.1.9 Anti-bot e Anti-Virus

- O fornecedor deve ter solução de Anti-Bot e Anti-Virus integrado na firewall
- A Solução de Anti-Bot deve ser capaz de detetar e parar comportamentos de rede suspeitos
- O aplicativo Anti-Bot deve usar um mecanismo de detecção baseado em varias pontos. Reputação de endereços IP, URLs e DNS e detectar padrões de comunicação de bots.
- A proteção Anti-Bot deve ter capacidade de efetuar Scan a ações de bot.
- A solução deve apoiar a detecção e prevenção de vírus e variantes de Cryptors & ransomware (por exemplo, Wannacry, Cryptlocker, CryptoWall ...) através do uso de análise estática e/ou dinâmica.
- A solução deve ter suporte para proteção contra-ataques de spear phishing
- DNS based attacks - A solução deve ter recursos de detecção e prevenção para C&C DNS hideouts:
 - Pesquisa de padrões de tráfego de C & C, não apenas no destino de DNS
 - Reverse engineer do Malware para descobrir seu DGA (Domain Name Generation)
 - DNS Trap, como parte da política de ameaças, interceta e analisa tentativas de comunicações do endpoint com C&C.
 - A solução deve detetar e prevenir ataques de DNS tunneling.
- A solução de Anti-Bot e Anti-Virus deve ter um mecanismo centralizado de correlação e relatório de eventos
- A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos
- A solução de antivírus deve poder inspecionar o tráfego SSL.
- O Anti-Bot e o Anti-Virus devem ter atualizações em tempo real na cloud.
- O Antivírus deve ser capaz de impedir a entrada de arquivos maliciosos
- O Antivírus deve ser capaz de analisar arquivos compactados
- Políticas antivírus e Anti-Bot devem ser geridas centralmente e ser possível a parametrização das mesmas.
- O antivírus deve analisar os ficheiros que passam no protocolo CIFS

3.1.10. Emulação de ameaças

- A solução deve ter a capacidade de proteger contra ataques desconhecidos (malware Zero Day) antes que proteções de assinatura estática sejam criadas:
 - Proteção em Tempo Real para malware desconhecido na navegação Web
 - Proteção em Tempo Real para malware desconhecido em email
- Cenários de implantação:
 - A solução deve fazer parte da arquitetura de prevenção de ameaças (com IPS, AV, AB, URLF, APP FW)
 - A solução deve fornecer solução de implementação On Prem e Cloud Based
 - Solução de Cloud pura
 - A solução não deve exigir infraestrutura separada para proteção email e proteção Web
 - A solução deve suportar a implementação em modo cluster.
- Tipos de ficheiros Suportados - A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash especificamente:
 - 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xls, xlsx, xlt, xltm, xltx, xlw, zip, pif, bz2, tgz;

- A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash, que sejam transmitidos pelos protocolos:
 - HTTP
 - HTTPS
 - FTP
 - SMTP
 - TLS SMTP
- OS support:
 - O mecanismo de emulação deve suportar vários sistemas operativos, como XP e Windows7, 8,10 32/64 bits, incluindo imagens personalizadas
 - A solução deve suportar cópias LICENCIADAS de Microsoft WINDOWS e Microsoft Office através de um contrato com a Microsoft.
 - A solução deve detetar chamadas API, alterações em ficheiros, system registry, ligações de rede e processos do sistema
 - A solução deve suportar análise estática para windows, mac OS-X, Linux ou qualquer plataforma x86
- O mecanismo de emulação deve ser capaz de inspecionar, emular, prevenir e compartilhar os resultados do evento de sandbox na infraestrutura de anti-malware
- A solução deve permitir a emulação de ficheiros maiores que 14 Mb, em todos os tipos suportados
- A solução deve suportar automated machine learning based detection engines
- A solução deve detectar o ataque na fase de exploitation - ou seja, antes que o código seja executado e antes que se tenha concluído o download do malware.
- A solução deve detectar ROP e outras técnicas de exploitation (por exemplo, elevação de privilégios), analisando o CPU
- A solução deve suportar a análise de links no corpo do e-mail para detecção de Malware Zero Day
- Tempo médio de emulação, para um veredito de malware suspeito como benigno não deve ser muito superior a 1 minuto
- Tempo médio de emulação, para um veredito de malware suspeito como maligno não deve ser muito superior a 3 minutos
- A solução deve possuir um mecanismo automático de partilha de informação com outros gateways em meio a atualizações de assinaturas etc, por forma a partilhar informações sobre novos ataques.
- A solução deve detectar o tráfego de C & C de acordo com a reputação dinâmica de ip / url
- A solução deve ser capaz de analisar documentos com URL's
- Na funcionalidade de Sandboxing, a solução proposta deverá ter a capacidade de suportar detecção de ameaças e técnicas de evasão (com tentativas de explorar vulnerabilidades de S.O.) ao nível do CPU – CPU-Level detection;

3.1.11. Anti-spam & email Security

- A solução deverá ser agnóstica em relação ao conteúdo, e ter a capacidade de classificar ameaças em tempo real, protegendo a infraestrutura com base padrões comportamentais, e não com base em conteúdo;
 - A solução proposta deverá incluir mecanismos de proteção com base em serviços online de IP reputation, de forma a evitar falsos positivos;
 - A solução deverá incluir mecanismos de proteção imediata (Dia Zero) para novos vírus propagados por email.

3.1.12 IPsec VPN

- A solução deverá suportar implementações de VPN (domain based, e route based com protocolos de routing dinâmico e virtual tunnel interfaces), com utilização de Internal Certificate Authority ou External 3rd party Certificate Authority;
- A solução deverá suportar criptografia 3DES e AES-256 para IKE Phase 1 e 2.
- A solução deverá suportar criptografia IKEv2 plus "Suite-B-GCM-128" e "Suite-B-GCM-256" for IKE Phase 2;
- A solução deverá suportar os seguintes grupos Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20;
- A solução deverá suportar os seguintes tipos de mecanismos de integridade de dados: md5, sha1, SHA-256, SHA-384 and AES-XCBC;
- A solução proposta deverá suportar as seguintes funcionalidades VPN:
 - Site-to-site:
 - Full Mesh (todos para todos);
 - Estrela (Sites remotos para Site principal);
 - Hub&Spoke (Site remotoA para Site RemotoB, através de site principal);
 - Suporte para configuração através de GUI, com opção de drag&drop de objetos nas comunidades VPN;
 - Suporte para VPN's de acesso remoto "clientless" e "client based";
 - Suporte para aplicação de políticas de segurança específicas, para controlo de tráfego associado à comunidade VPN;

3.1.13 SSL Inspection outbound

- A solução deverá suportar inspeção SSL (inspection/decryption) com performance comprovada em todas as tecnologias de mitigação;
- A solução deverá suportar Perfect Forward Secrecy (PFS , ECDHE cipher suites);
- A solução deverá suportar AES-NI, AES-GCM for improved throughput;
- A solução deverá suportar a integração das tecnologias de emulação/sandboxing com inspeção SSL;
- A solução deverá permitir a reutilização da base de dados de URL Filtering, para criação de políticas de inspeção de SSL granulares;

4. Computador Desktop

Um computador desktop com as seguintes características mínimas:

Processador	1 x Intel Xeon Silver 4208 / 2.1 GHz (3.2 GHz) (8 núcleos)
Socket do Processador	FCLGA3647 Socket
Principais Recursos do Processador	Tecnologia Hyper-Threading (hiperprocessamento), Intel Turbo Boost Technology 2
Memória cache	11 MB L3 Cache

RAM	128 GB (instalado) / 768 GB (máx.) - DDR4 SDRAM - ECC
Controlador de capacidade	SATA (SATA 6Gb/s)
Disco rígido	SSD 1 TB - PCI Express 3.0 x4 - M.2 2280 - HP Z Turbo Drive, TCG Opal Encryption 2, NVMe Express (NVMe), célula de nível triplo (TLC), 3D NAND Technology
Armazenamento óptico	Gravador DVD
Velocidade de Memória Efectiva	2400 MHz
Slots	6 (Total) / 1 (vazio)
Tipo Disco	SSD - M.2 2280
Capacidade	1 x 1 TB
Tipo de interface	PCI Express 3.0 x4
Resistência SSD	400 TB
Gravador DVD	Inclui
Placa gráfica	5GB GDDR5X Pcie 3.0x16 4 x Displayport, CUDA Cores 1280
	Largura de banda 200 GBps
	Consumo de potência em modo operacional 75 Watt

Saída de áudio

Padrões de Conformidade	Áudio de Alta Definição
-------------------------	-------------------------

Dispositivo de entrada

Tipo	Rato Optico USB ,teclado Slim uSB PT
Portas de Ethernet	2 x Gigabit Ethernet
Controlador de Ethernet	Intel i219-LM, X722
Protocolo de Ligação de Dados	Ethernet, Fast Ethernet, Gigabit Ethernet
Características	Wake on LAN (WoL), PXE 2.1 support
Padrões de Conformidade	IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.1as, IEEE 802.3az

Expansão / conectividade

Unidades	2 (total) / 2 (livres) x interno 3.5"
	2 (total) / 2 (livres) x externo 5.25"
	1 (total) / 0 (livres) x externo 5,25" Slim Line

Cofinanciado por:

Slots	3 (total) / 3 (livres) x PCIe 3.0 x4 (aberto)
	2 (total) / 2 (livres) x PCIe 3.0 x16
	1 (total) / 1 (livres) x PCIe 3.0 x8 (aberto,slot converte para x4 elétrica quando o SSD está instalado na segunda slot M.2)
	2 (total) / 1 (livres) x M.2 Card (modo X4)
Interfaces	1 x auscultadores/microfone (1 no dianteiro)
	2 x USB 3.1 Gen 1 (2 no dianteiro) (um deles está a carregar)
	2 x LAN (Gigabit Ethernet)
	1 x saída de linha de áudio
	1 x entrada de linha de áudio/microfone
	1 x rato PS/2
	1 x teclado PS/2
	6 x USB 3.1 Gen 1
Cabos incluídos	2 x USB-C 3.1 Gen 2 (2 no dianteiro)
	Adaptador Mini DisplayPort-DisplayPort
Tipo de Encaixe de Segurança	Ranhura de segurança Kensington
Padrões de Conformidade	RoHS,WEEE,Critérios Comuns EAL4+,ACPI 5.0,baixo halogéneo
Potência	
Tipo de dispositivo	Suprimento de potência
Voltagem necessária	AC 90 - 269 V (50/60 Hz)
Potência fornecida	1000 Watt
Certificação 80 PLUS	80 PLUS
Eficiência	90%
Correcção de Factor de Potência	Sim (activo)
SO fornecido	Windows 10 Pro para Workstations Plus Edição 64-bit Português
Serviço e suporte	Garantia limitada - peças e mão de obra - 3 anos - no local
Parâmetros ambientais	
Temperatura de Funcionamento Mínima	5 °C
Temperatura de Funcionamento Máxima	35 °C
Limite de Humidade em Funcionamento	10 - 85% (sem condensação)
Dimensões e peso	
Largura	16.9 cm
Profundidade	46.5 cm
Altura	44.5 cm
Peso	13.1 kg

5. Computador Portátil

Um computador portátil com as seguintes características mínimas:

Sistema operativo

Windows 10 Pro 64

Família de processadores

Processador Intel® Core™ i7 de 10.ª geração

Processador

Intel® Core™ i7-10510U (1.8 GHz de frequência base, até 4.9 GHz com Tecnologia Intel® Turbo Boost, cache de 8 MB L3, 4 núcleos)

Chipset

SoC integrado Intel®

Especificações de impacto sustentável

Baixo halogéneo

Gestão de segurança

Ranhura para cabo antirroubo; Chip de segurança Trusted Platform Module (TPM) 2.0 incorporado; Microsoft Security Defender;; Microsoft BitLocker Encryption; Capacidade Secured-core PC

Memória, padrão

RAM DDR4 (2666 MHz) de 64 GB

Descrição do disco rígido

SSD M.2 PCIe® NVMe™ TLC de 1 TB

Unidade óptica

Não incluída

Ecrã

Ecrã 4K UHD (3840 x 2160) de 39,6 cm (15,6 pol. 39,6cm) na diagonal, IPS, antirreflexo, 550 nits, HDR 400, NTSC a 72%

Placa gráfica (integrada)

Placa gráfica Intel® UHD

Localização das portas de E/S

Lado esquerdo **Portas**; 1 Tomada combinada para auscultadores/microfone; 1 Porta USB 3.1 Gen 1; 1 Porta USB 3.1 Gen 1 (carregamento)

Lado direito: **Portas** 1 conector de alimentação; 1 HDMI 1.4b; 2 portas USB Type-C™ (Thunderbolt™ 3)

Slots de expansão; 1 leitor de Smart Card

Interface de rede; Adaptador combinado Intel® AX201 com Wi-Fi 6 (2x2) e Bluetooth® 5, sem vPro™

Tipo de interface de rede; WLAN

Interface de rede; Tomada combinada Intel® Wi-Fi 6 AX201 (2x2) e Bluetooth® 5 (suporta velocidades de transferência de ficheiros da ordem dos Gigabits) **Tipo de interface de rede**: NFC

Banda larga móvel; Módulo Near Field Communication (NFC)

Energia/Alimentação; Adaptador com USB Type-C™ (65 W)

Tipo de bateria; Bateria de grande autonomia de 3 células, de polímeros de iões de lítio, 56 Wh

Teclado; teclado integral com resistência a derramamentos, retroiluminação

Certificação ENERGY STAR

Certificação ENERGY STAR®

Dimensões mínimas (L x P x A); 35,95 x 23,36 x 1,92 cm

Peso; A partir de 1,75 kg

Garantia: A garantia limitada de 3 anos

6. Monitor A

Um monitor com as seguintes características mínimas:

Dimensão do ecrã (diagonal): 23.8" 60,45cm

Tipo de ecrã; IPS

Proporção; 16:9

Resolução (nativa):FHD (1920 x 1080)

Resoluções suportadas; 1024 x 768; 1280 x 1024; 1280 x 720; 1280 x 800; 1366 x 768; 1440 x 900; 1600 x 900; 1680 x 1050; 1920 x 1080; 640 x 480; 720 x 400; 800 x 600

Distância entre pixels; 0,274 mm

Cores do ecrã; Até 16,7 milhões de cores suportadas (através da tecnologia FRC)

Luminosidade; 250 nits

Relação de contraste; 1000:1

Tempo de resposta; 5 ms (cinzento para cinzento) (com overdrive)

Conector de entrada; 1 porta VGA; 1 porta DisplayPort™ 1.2 (com suporte HDCP); 1 porta HDMI 1.4 (com suporte HDCP)

Características do ecrã; Controlo de recursos; Controlos no ecrã; Plug and Play; Controlos do utilizador; Modo Low Blue Light; Antirreflexo

Mostrar frequência do ecrã (horizontal); 30 a 86 KHz

Mostrar frequência do ecrã (vertical); 48 a 75 Hz

Controlos apresentados no ecrã; Luminosidade; Controlo de cores; Sair; Controlo de imagem; Informação; Gestão; Controlo de energia; Controlo de entrada; Controlo de menu

Energia/Alimentação; Tensão de entrada (de 100 a 240 V CA)

Tipo de fonte de alimentação; Interno

Consumo de energia; 26 W (máximo), 22 W (típico), 0,3 W (modo de espera)

Gama de temperaturas de funcionamento; 5 a 35 °C

Especificações de impacto sustentável; Vidro de ecrã sem arsénico; Baixo halogéneo; Retroiluminação de ecrã sem mercúrio; Certificação TCO

Dimensões com suporte (largura x profundidade x altura)

53,82 x 21,16 x 46,43 cm

Peso; 4,51 kg

Conteúdo da embalagem; Monitor; Cabo DisplayPort™; Cabo HDMI; Cabo de alimentação de CA

Garantia; Garantia limitada de 3 anos, incluindo 3 anos para peças e mão de obra.

7. Monitor B

Um monitor com as seguintes características mínimas:

Dimensão do ecrã (diagonal) :23.8", 60.45cm

Tipo de ecrã; IPS

Proporção; 16:9

Resolução (nativa); FHD (1920 x 1080)

Resoluções suportadas; 1024 x 768; 1280 x 1024; 1280 x 720; 1280 x 800; 1440 x 900; 1600 x 900; 1680 x 1050; 1920 x 1080; 640 x 480; 720 x 400; 800 x 600

Distância entre pixels; 0,274 mm

Cores do ecrã; Até 16,7 milhões de cores suportadas (através da tecnologia FRC)

Luminosidade; 250 nits

Relação de contraste; 1000:1

Tempo de resposta; 5 ms (cinzento para cinzento) (com overdrive)

Cofinanciado por:

Características do ecrã; Modo Low Blue Light; Antirreflexo, 60.45cm 1 porta **Conector de Entrada:** 1 x VGA; 1 porta USB Type-B; 1 DisplayPort™ 1.4 (com suporte HDCP); 1 porta HDMI 1.4 (com suporte HDCP); 4 portas USB-A 3.2 de 1.ª geração

Mostrar frequência do ecrã (horizontal); 30 a 80 KHz

Mostrar frequência do ecrã (vertical); 50 a 60 Hz

Controlos apresentados no ecrã; Luminosidade; Sair; Informações; Gestão; Controlo de energia; Controlo de entrada; Controlo do menu; Imagem; Cores

Segurança física; Preparado para fecho

Webcam; Sem câmara integrada

Energia/Alimentação; Tensão de entrada (de 100 a 240 V CA)

Tipo de fonte de alimentação; Interno

Consumo de energia; 6 W (máximo), 3,5 W (típico), 0,3 W (modo espera)

Gama de temperaturas de funcionamento; 5 a 35 °C

Dimensões mínimas (L x P x A); 53,94 x 4,7 x 32,33 cm (Sem suporte.)

Peso; 5,7 kg

Conteúdo da embalagem; Monitor; Cabo DisplayPort™ 1.2; Cabo HDMI; Cabo USB Type-B para A; Guia de início rápido; Kit de documentos; Cabo de alimentação CA

Garantia; Garantia limitada de 3 anos, incluindo 3 anos para peças e mão de obra.