

CADERNO DE ENCARGOS

Aquisição e instalação de equipamento de informática (material de rede) para as instalações do Centro de Valorização e Transferência de Tecnologia da Água - Associação AquaValor

2020

Índice

Capítulo I: Disposições gerais.....	1
Cláusula 1.ª - Objeto	1
Cláusula 2.ª - Contrato.....	1
Cláusula 3.ª – Preço base	1
Cláusula 4.ª - Prazo	2
Cláusula 5.ª - Cessão da posição contratual e subcontratação.....	2
Capítulo II: Obrigações Contratuais	2
Cláusula 6.ª - Obrigações principais do Fornecedor	2
Cláusula 7.ª – Conformidade e operacionalidade dos bens.....	3
Cláusula 8.ª - Entrega dos bens objeto de contrato.....	3
Cláusula 9.ª - Garantia Técnica.....	4
Cláusula 10.ª - Objeto do dever de sigilo.....	4
Cláusula 11.ª - Prazo do dever de sigilo	5
Cláusula 12.ª - Proteção de dados pessoais e RGPD	5
Cláusula 13.ª - Preço Contratual	7
Cláusula 14.ª - Condições de pagamento	7
Capítulo III: Penalidades Contratuais e Resolução.....	8
Cláusula 15.ª - Penalidades Contratuais	8
Cláusula 16.ª - Força maior	8
Cláusula 17.ª - Resolução por parte da entidade adjudicante.....	9
Capítulo IV: Caução	9
Cláusula 18.ª – Caução	9
Cláusula 19.ª – Patentes, licenças e marcas registadas.....	9
Capítulo V: Resolução de Litígios.....	9
Cláusula 20.ª - Foro competente.....	9
Capítulo VI: Disposições finais	9
Cláusula 21.ª - Comunicações e notificações.....	9
Cláusula 22.ª - Contagem dos prazos	10
Cláusula 23.ª - Legislação aplicável.....	10
Cláusula 24.ª – Especificações Técnicas	11

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 “Aquisição e Instalação de equipamento de informática (material de rede) para as instalações da Associação AquaValor”, dividido em 5 lotes, no âmbito do projeto NORTE-46-2018-31, com as quantidades, características e especificações constantes do **anexo A** do presente Caderno de Encargos.
2. Para efeitos de execução, o contrato deverá obedecer aos termos descritos nas cláusulas técnicas anexas a este caderno de encargos.

Cláusula 2.ª - Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
 - a. O suprimento dos erros e das omissões do Caderno de Encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contrato;
 - 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, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º e aceites pelo Adjudicatário nos termos do disposto no artigo 101.º, ambos do Código dos Contratos Públicos.

Cláusula 3.ª – Preço base

1. Com o presente procedimento de formação do contrato, a AquaValor dispõe-se a pagar o valor máximo de **52.700,00€ (cinquenta e dois mil e setecentos mil euros)**, distribuído pelos seguintes lotes:
 - a. Lote 1: Switching- 18.500,00€ (dezoito mil e quinhentos mil euros);
 - b. Lote 2: Wifi – 12.500,00€ (doze mil e quinhentos mil euros);
 - c. Lote 3: UPS - 8.500,00€ (oito mil e quinhentos mil euros);
 - d. Lote 4: Firewall - 11.000,00€ (onze mil euros);
 - e. Lote 5: Infraestrutura de voz - 2.200,00€ (dois mil e duzentos euros)
2. Os preços apresentados não incluem o Imposto sobre Valor Acrescentado (IVA).

3. O preço base foi fixado com base nos custos médios unitários resultantes de anteriores procedimentos desenvolvidos pelas entidades que constituem a “AquaValor – Centro de Valorização e Transferência de Tecnologia da Água – Associação” para aquisições da mesma tipologia, conforme estabelecido no artigo 47.º n.º 3 do CCP.

Cláusula 4.ª - Prazo

1. O contrato a celebrar vigorará até à entrega e instalação dos bens ao contraente público em conformidade com os respetivos termos e o disposto na lei.
2. Os bens objeto do presente procedimento terão de ser fornecidos, num prazo máximo de **60 (sessenta) dias** após envio da nota de encomenda ou assinatura do contrato.

Cláusula 5.ª - Cessão da posição contratual e subcontratação

São admitidas a cessão da posição contratual e a subcontratação, que se regem pelo disposto no Código dos Contratos Públicos.

Capítulo II: Obrigações Contratuais

Secção I

Obrigações do adjudicatário

Subsecção I

Disposições gerais

Cláusula 6.ª - Obrigações principais do Fornecedor

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o fornecedor as seguintes obrigações principais:
 - a. Fornecer à AquaValor os bens cujo fornecimento é objeto do presente caderno de encargos, nos prazos e moldes estabelecidos, em conformidade com as especificações, os requisitos técnicos e funcionais mínimos de fornecimento definidos no presente caderno de encargos e demais documentos contratuais;
 - b. Obrigação de garantir a boa qualidade dos equipamentos e acessórios utilizados no fornecimento, pelo período mínimo definido para cada tipo de bem no Anexo A.
 - c. Instalar e configurar os equipamentos cujo fornecimento é objeto do presente caderno de encargos;
 - d. Analisar e levar em consideração todas as situações e circunstâncias relativas e/ou relevantes à execução do fornecimento dos bens, incluindo, entre outras e a título meramente exemplificativo, a informação prévia necessária, as circunstâncias de modo, tempo e lugar e os meios, de forma a salvaguardar

- que os bens serão fornecidos nos termos contratados, sem hiatos, falhas ou interrupções que pudessem ter sido previstas;
- e. Assumir todos os riscos inerentes ao fornecimento de materiais e de equipamentos, bem como aqueles que, em concreto, apenas sejam ou possam ser do conhecimento do adjudicatário ou por este gerido em primeira linha;
 - f. O adjudicatário deverá entregar à AquaValor, sempre que solicitado, os documentos comprovativos da inexistência de dívidas à Segurança Social e à Administração Fiscal;
 - g. O adjudicatário assume integral responsabilidade pelo fornecimento contratado, sendo o único responsável perante a AquaValor pela boa execução do mesmo;
2. O adjudicatário fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados ao fornecimento, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das prestações contratuais a que está obrigado.

Cláusula 7.ª – Conformidade e operacionalidade dos bens

- 1. O fornecedor obriga-se a entregar à AquaValor os bens objeto do contrato com as características, especificações e requisitos técnicos previstos nas especificações técnicas, anexas ao presente Caderno de Encargos, que dele faz parte integrante.
- 2. Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
- 3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.
- 4. O fornecedor é responsável perante a AquaValor por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.
- 5. Os equipamentos objeto do contrato devem ter em conta os requisitos técnicos ambientais, conforme definido na ENCPE 2020.

Cláusula 8.ª - Entrega dos bens objeto de contrato

- 1. Os bens objeto do contrato devem ser entregues e instalados na Associação AquaValor- Centro de Valorização e Transferência de Tecnologia da Água, sito na Rua Dr. Júlio Martins nº 1, 5400-342 Chaves – Portugal, no prazo estipulado na cláusula 4.ª.

2. O não cumprimento dos prazos de entrega, por parte do fornecedor, confere à AquaValor o direito de adquirir no mercado artigos idênticos para satisfação de necessidades urgentes e de debitar ao fornecedor diferenças de preço para mais que se venha a verificar.
3. Os documentos que acompanham os bens objeto de contrato devem, obrigatoriamente, mencionar o número do procedimento que lhe deu origem.
4. Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local de entrega são da responsabilidade do fornecedor.

Cláusula 9.ª - Garantia Técnica

1. O fornecedor nos termos propostos e da legislação aplicável, garantirá a conformidade dos serviços e dos bens fornecidos no âmbito do contrato, sem quaisquer encargos adicionais para o contraente público, contra quaisquer defeitos ou discrepâncias, com as exigências legais e requisitos técnicos definidos no caderno de encargos, pelo(s) prazo(s) indicado(s) na sua proposta.
2. No prazo máximo de um mês, a contar da data em que o contraente público tenha detetado qualquer defeito ou discrepância nos equipamentos fornecidos, este deve notificar o fornecedor, para efeitos da respetiva reparação ou substituição.
3. São excluídas da garantia todos os defeitos que notoriamente resultem da má utilização, negligência da entidade adjudicante ou de utilização abusiva, bem como todos os defeitos resultantes de fraude, ação de terceiros e de casos fortuitos ou de força maior.

Cláusula 10.ª - Objeto do dever de sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à AquaValor 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 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 - Prazo do dever de sigilo

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

Cláusula 12.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 ou de que tenha tido conhecimento no âmbito do contrato ou por causa dele.
2. Os dados pessoais a que o adjudicatário tenha acesso ou que lhe sejam transmitidos pela Entidade Adjudicante ao abrigo do contrato, serão tratados em estrita observância das instruções desta Entidade e da legislação de Proteção de Dados Pessoais, nomeadamente do Regulamento Geral de Proteção de Dados Pessoais (RGPD - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016) e da Lei n.º 58/2019, de 8 de agosto que assegura a execução, na ordem jurídica nacional, do referido Regulamento Comunitário.
3. O adjudicatário compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer outra forma colocar à disposição de terceiros os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pela Entidade Adjudicante ao abrigo do contrato, sem que para tal tenha sido expressamente instruído, por escrito, pela referida Entidade Adjudicante.
4. O Adjudicatário obriga-se a cumprir rigorosamente o disposto na Lei n.º 58/2019, de 8 de agosto e demais legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:
 - a. Utilizar os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pela Entidade Adjudicante, 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 Entidade Adjudicante, 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 Entidade Adjudicante, contra a respetiva destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou os acessos não autorizados, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais;
 - f. Prestar à Entidade Adjudicante, toda a colaboração de que esta careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais efetuado ao abrigo do contrato e manter esta Entidade informada em relação ao tratamento de dados pessoais, obrigando-se a 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;
 - g. Assegurar que os seus colaboradores cumprem todas as obrigações previstas no contrato;
 - h. Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade.
- 5. Adotar medidas de segurança previstas no artigo 32.º 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;
 - 6. Prestar a assistência necessária à Entidade Adjudicante no sentido de permitir que estas cumpram a obrigação de dar 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 dos dados.
 - 7. Garantir mecanismos de notificação efetivos em caso de violação de dados pessoais;
 - 8. O Adjudicatário será responsável por qualquer prejuízo em que a Entidade Adjudicante, 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 na alínea g) do n.º 4 da presente cláusula, entende-se por “colaborador” toda e qualquer pessoa singular ou coletiva que preste serviços

ao adjudicatário, 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 c) do número 4 da presente cláusula mantém-se mesmo após a cessação do contrato, independentemente do motivo porque ocorra.

Secção II

Obrigações da entidade adjudicante

Cláusula 13.^a - Preço Contratual

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

Cláusula 14.^a - Condições de pagamento

1. As quantias devidas pela AquaValor, nos termos da cláusula anterior, são pagas no prazo de **30 (trinta) a 60 (sessenta) dias** após a receção pela AquaValor das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. O vencimento da obrigação ocorre, após a entrega e instalação dos bens objeto do contrato.
3. Em caso de discordância por parte da AquaValor, quanto ao valor indicado na fatura, deve este comunicar ao fornecedor, por escrito, os respetivos fundamentos, ficando o fornecedor obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas através de Transferência Bancária.

Capítulo III: Penalidades Contratuais e Resolução

Cláusula 15.ª - Penalidades Contratuais

1. Pelo não cumprimento de obrigações emergentes do contrato, a entidade adjudicante pode exigir do adjudicatário o pagamento de uma sanção pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:

- a. Pelo incumprimento das datas e prazos pelo fornecimento dos bens objeto do contrato, até 0,1 % do preço contratual por cada dia de atraso.

Cláusula 16.ª - Força maior

1. Não podem ser impostas penalidades ao adjudicatário, nem é havido 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. Circunstância que não constituam força maior para os subcontratados do Fornecedor, na parte em que intervenham;
 - b. Greves ou conflitos laborais limitados às sociedades do Fornecedor ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c. Determinações governamentais, administrativa ou judiciais de natureza sancionatória, ou de outras formas resultantes do incumprimento pelo Fornecedor de deveres que sobre ele recaiam;
 - d. Manifestações populares devidas ao incumprimento pelo Fornecedor de normas legais;
 - e. Incêndios ou inundações com origem nas instalações do Fornecedor 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 Fornecedor 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 17.ª - Resolução por parte da entidade adjudicante

Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a AquaValor pode resolver o contrato, a título sancionatório, no caso de o fornecedor violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.

Capítulo IV: Caução

Cláusula 18.ª – Caução

Nos termos do n.º 2 do artigo 88º do CCP, não é exigível a prestação de caução.

Cláusula 19.ª – Patentes, licenças e marcas registadas

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

Capítulo V: Resolução de Litígios

Cláusula 20.ª - Foro competente

Para a resolução de todas as questões judiciais emergentes do presente procedimento ou do contrato a celebrar será competente o Tribunal Administrativo e Fiscal de Mirandela.

Capítulo VI: Disposições finais

Cláusula 21.ª - Comunicações e notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 22.ª - Contagem dos prazos

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

Cláusula 23.ª - Legislação aplicável

Em tudo o omissa no presente Caderno de Encargos, aplicar-se-á o disposto no Código dos Contratos Públicos, aprovado pelo DL n.º 18/2008, de 20 de janeiro alterado pelo DL n.º 111-B/2017, de 31/08 e à restante legislação aplicável.

ANEXO A

Cláusula 24.^a – Especificações Técnicas

Descrição do Equipamento
LOTE 1
<u>Infraestrutura de Switching</u>
<u>3 Switches de 48 portas 10/100/1000 e 4 portas de uplink</u>
Equipamento fixo Ethernet L2/L3
Altura máxima 1RU e preparado para uma correta fixação em bastidor de 19” (incluindo todos os acessórios necessários para o efeito)
Equipamento Fully Managed
Incluir 48 Portas dedicadas para downlink 10/100/1000 BaseT
Módulo de uplink, permitindo fazer o swap de interfaces GE para 10GE, ou vice-versa, ou aumentar o número de portas a 10GE apenas trocando o módulo
O equipamento deverá ter capacidade para suportar as seguintes opções modulares de uplink:
a. Mínimo de 4 portas de uplink line rate 10GE SFP+ em fibra
b. Mínimo de 4 portas GE 1000Base-X, com suporte para SFPs de cobre ou fibra SX ou LX
Suporte das seguintes interfaces óticas do tipo SFP+:
a. 10G Base LR
b. 10G Base LRM
c. 10G Base SR
Suporte das seguintes interfaces óticas do tipo SFP:
a. 1000 base T
b. 1000 base ZX
c. 1000 Base SX
d. 1000 Base LX/LH
Suporte de flash com um mínimo de 2Gb para guardar configurações e logs
Equipamento com um mínimo de 4GB DRAM
Suportar stacking através de módulo dedicado (não são permitidos equipamentos que usem portas de uplink para fazer stacking), garantindo capacidade para que uns mínimos de 9 dispositivos sejam geridos como um único, através de um endereço único de gestão.
A capacidade de stacking descrita no ponto anterior tem de permitir a integração em stacks de switches existentes, baseadas no modelo Cisco Catalyst 3850.
O equipamento deve incluir todos os cabos (de comunicação e alimentação elétrica) e licenciamento necessários à ligação em stack.
Capacidade de suportar Stateful Switchover, quando comuta de Ativo para standby numa stack.
Suporte de capacidade de bandwidth da stack mínimo de 440 Gbps não bloqueante.
integração completa com a plataforma de gestão (NMS) Cisco Prime Infrastructure, em uso na instituição
Suporte mínimo de 255 VLANs ativas e com capacidade para escalar até 1000 VLAN's activas
Suporte de um mínimo de 4000 VLAN id's

Suporte de jumbo frames
Incluir fans e fontes de alimentação redundantes e hotswappable
Capacidade de suporte de powers AC ou DC
Switching bandwidth: Mínimo de 176 Gbps
Forwarding rate: Mínimo de 130 Mpps
Suporte para um mínimo de 32000 endereços MAC
Capacidade de suportar um mínimo de 24000 rotas unicast
Capacidade de suportar 802.1Q tunneling (QinQ)
Suporte para LLDP e LLDP-MED IEEE 802.1AB
Suporte para um mínimo de 128 instâncias de spanning tree
Suporte para IEEE 802.3ad LACP, garantindo um mínimo de 8 links agregados
Suporte para IEEE 802.3ad LACP através da stack
Capacidade de Suportar VRRP para IPv4
Suporte para IPv6 em hardware
Suporte para multicast em hardware
Suporte para QoS em hardware
Suporte para features de segurança em hardware
MTBF mínimo: 240.000 horas
Auto-negociação em todas as portas
Suporte para rotas estáticas IPv4 e IPv6
Capacidade para suportar: RIPv1, RIPv2, RIPv6, OSPFv2, OSPFv3, ISIS, BGPv4, BGPv6
Capacidade de suportar Multi VRF CE (VRF lite)
Capacidade de suportar rate-limiting baseado em IP Origem/destino, MAC origem/ destino, L4 TCP/UDP
Suporte de Auto-MDIX
Capacidade para suportar PIM-SM, PIM-DM, PIM-SSM
Suporte de DHCP server
Suporte de VLAN ACL's
Suporte de SSHv2 e SNMPv3
Suporte para MAB (MAC authentication Bypass)
Suporte para DAI (Dynamic ARP inspection)
Suporte para DHCP option 82
Suporte para Port security
Suporte para 802.1X
Suporte para 802.1X com ACL's
Suporte para 802.1X com guest VLAN
Suporte para web authentication para clientes não 802.1X
Suporte para plug and play da configuração de switches e software, sem intervenção do utilizador
Suporte IGMP v1, v2, v3
Suporte para 8 egress queues por porta
Suporte para ACL's IPv6
Suporte para IPv6 MLDv1 e MLDv2
Suporte para acesso de gestão em IPv6: HTTP, HTTPS, SNMP, Syslog
Capacidade para suportar DHCPv6 client/server/relay
Capacidade para suportar IPv6 QoS

Suporte de RFC4292/RFC4293 MIBs para tráfego IPv6
Suporte de inter-VLAN routing
Capacidade de suporte de IEEE 802.1AE em hardware
Capacidade de suporte de SDN (Software Defined Networks)
Suporte de Link aggregation através de diferentes membros da stack
Suporte de sessões line rate bidireccionais de port-mirroring e remote portmirroring
Capacidade de suporte de Netflow v9 ou IPFIX
Capacidade de suporte de fluxos de rede, com um mínimo de 48000 fluxos, e permitindo através de fluxos: a. Efetuar deteção de anomalias de segurança b. Identificar os Top Talkers c. Customizar fluxos por perfil de utilizador d. Utilizar múltiplos collectors e. Exportar o consumo de bandwidth, em função do número de fluxos
Suporte, através do CLI, do plug and play de dispositivos ligados ao switch, nomeadamente de pc's, switches, AP's, telefones, impressoras, sem intervenção do utilizador, configurando/desconfigurando automaticamente e adaptando ao tipo de dispositivos os parâmetros de: a. VLANs (voz e dados, ou ambas) b. QoS c. Porta de acesso/trunk d. Spanning tree e. No caso de trunking, definir o tipo de encapsulamento f. Quando o dispositivo é desligado da porta, a configuração deverá ser removida automaticamente sem intervenção do utilizador g. No caso de PC's e impressoras, deverá ser possível a deteção baseada em MAC address e OUI (Organizational Unique Identifier). Nota: Esta funcionalidade deverá ser implementada sem ter de recorrer a IEEE 802.1X
Integração LAN e WLAN: São valorizadas soluções que integrem a componente de 4 LAN e WLAN num único equipamento - acesso unificado. Desta forma a solução deverá ter a capacidade para, através do mesmo hardware (com licenciamento adicional se necessário), garantir no switch a integração do controller wireless, que deverá ter capacidade para: a. Gerir até 100 Access Points b. Suporte de 2000 clientes c. Suportar wireless Throughput de 40 Gbps d. Suportar até 64 WLAN's e. Suporte de L2/L3 roaming f. Suporte de Access Points na frequência 2.4GHz e 5Ghz g. Suporte de IEEE 802.11a/b/g/n h. Suporte de IEEE 802.11ac i. Suporte de IEEE 802.11i - EAP-TLS, EAP-SIM, EAP-TTLS, WPA, WPA2, 802.1x, WEP, WPA2 j. Deteção de interferências não WiFi k. Suporte de IEEE 802.11r l. Suporte de IEEE 802.11v m. Suporte de streams multicast n. Suporte de policieis para utilizadores e dispositivos com base em informação

contextualizada
o. Suportar visibilidade aplicacional para tráfego WLAN integrado com a componente de fluxos de rede em hardware, referida neste Caderno de Encargos
p. Aplicação de QoS, Segurança e visibilidade aplicacional, independentemente do tipo de acesso (wired ou wireless)
q. Sistema operativo único, para a componente de LAN e WLAN, configurado usando a mesma interface de linha de comandos
r. Tanto a componente de LAN como de WLAN, deverão ser geríveis através de uma plataforma de gestão única
s. Suporte de Gestão de largura de banda por:
i. Access Point
ii. Radio – 2.4Ghz ou 5Ghz
iii. SSID
iv. Cliente – PC, MAC, ipad, etc
v. Aplicação – Facebook, yahoo, etc
Equipamento de referência: Cisco Catalyst 3850-48T-L ou equivalente
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 3 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD.
Acesso, sem custos adicionais, às atualizações de software lançadas pelo fabricante para o modelo, pelo mesmo período de tempo fornecido no item anterior.
1 Switch de 48 portas 10/100/1000 PoE/PoE+ e 4 portas de uplink
Equipamento fixo Ethernet L2/L3
Altura máxima 1RU e preparado para uma correta fixação em bastidor de 19” (incluindo todos os acessórios necessários para o efeito)
Equipamento Fully Managed
Incluir 48 Portas dedicadas para downlink 10/100/1000 BaseT, com suporte de PoE 15.4W (IEEE 802.3af) simultaneamente nas 48 portas, sem recorrer a fonte de alimentação externa. Pelo menos 24 dessas portas têm de suportar simultaneamente PoE+ 30 W (IEEE 802.3at), sem recorrer a fonte de alimentação externa
Módulo de uplink, permitindo fazer o swap de interfaces GE para 10GE, ou vice-versa, ou aumentar o número de portas a 10GE apenas trocando o módulo
O equipamento deverá ter capacidade para suportar as seguintes opções modulares de uplink:
a. Mínimo de 4 portas de uplink line rate 10GE SFP+ em fibra
b. Mínimo de 4 portas GE 1000Base-X, com suporte para SFPs de cobre ou fibra SX ou LX
Suporte das seguintes interfaces óticas do tipo SFP+:
a. 10G Base LR
b. 10G Base LRM
c. 10G Base SR
Suporte das seguintes interfaces óticas do tipo SFP:
a. 1000 base T
b. 1000 base ZX
c. 1000 Base SX

d. 1000 Base LX/LH
Suporte de flash com um mínimo de 2Gb para guardar configurações e logs
Equipamento com um mínimo de 4GB DRAM
Suportar stacking através de módulo dedicado (não são permitidos equipamentos que usem portas de uplink para fazer stacking), garantindo capacidade para que uns mínimos de 9 dispositivos sejam geridos como um único, através de um endereço único de gestão.
A capacidade de stacking descrita no ponto anterior tem de permitir a integração em stacks de switches existentes, baseadas no modelo Cisco Catalyst 3850.
O equipamento deve incluir todos os cabos (de comunicação e alimentação elétrica) e licenciamento necessários à ligação em stack.
Capacidade de suportar Stateful Switchover, quando comuta de Ativo para standby numa stack.
Suporte de capacidade de bandwidth da stack mínimo de 440 Gbps não bloqueante.
integração completa com a plataforma de gestão (NMS) Cisco Prime Infrastructure, em uso na instituição
Suporte mínimo de 255 VLANs ativas e com capacidade para escalar até 1000 VLAN's activas
Suporte de um mínimo de 4000 VLAN id's
Suporte de jumbo frames
Incluir fans e fontes de alimentação redundantes e hotswappable
Capacidade de suporte de powers AC ou DC
Switching bandwidth: Mínimo de 176 Gbps
Forwarding rate: Mínimo de 130 Mpps
Suporte para um mínimo de 32000 endereços MAC
Capacidade de suportar um mínimo de 24000 rotas unicast
Capacidade de suportar 802.1Q tunneling (QinQ)
Suporte para LLDP e LLDP-MED IEEE 802.1AB
Suporte para um mínimo de 128 instâncias de spanning tree
Suporte para IEEE 802.3ad LACP, garantindo um mínimo de 8 links agregados
Suporte para IEEE 802.3ad LACP através da stack
Capacidade de Suportar VRRP para IPv4
Suporte para IPv6 em hardware
Suporte para multicast em hardware
Suporte para QoS em hardware
Suporte para features de segurança em hardware
MTBF mínimo: 240.000 horas
Auto-negociação em todas as portas
Suporte para rotas estáticas IPv4 e IPv6
Capacidade para suportar: RIPv1, RIPv2, RIPv3, OSPFv2, OSPFv3, ISIS, BGPv4, BGPv6
Capacidade de suportar Multi VRF CE (VRF lite)
Capacidade de suportar rate-limiting baseado em IP Origem/destino, MAC origem/ destino, L4 TCP/UDP
Suporte de Auto-MDIX
Capacidade para suportar PIM-SM, PIM-DM, PIM-SSM
Suporte de DHCP server

Suporte de VLAN ACL's
Suporte de SSHv2 e SNMPv3
Suporte para MAB (MAC authentication Bypass)
Suporte para DAI (Dynamic ARP inspection)
Suporte para DHCP option 82
Suporte para Port security
Suporte para 802.1X
Suporte para 802.1X com ACL's
Suporte para 802.1X com guest VLAN
Suporte para web authentication para clientes não 802.1X
Suporte para plug and play da configuração de switches e software, sem intervenção do utilizador
Suporte IGMP v1, v2, v3
Suporte para 8 egress queues por porta
Suporte para ACL's IPv6
Suporte para IPv6 MLDv1 e MLDv2
Suporte para acesso de gestão em IPv6: HTTP, HTTPS, SNMP, Syslog
Capacidade para suportar DHCPv6 client/server/relay
Capacidade para suportar IPv6 QoS
Suporte de RFC4292/RFC4293 MIBs para tráfego IPv6
Suporte de inter-VLAN routing
Capacidade de suporte de IEEE 802.1AE em hardware
Capacidade de suporte de SDN (Software Defined Networks)
Suporte de Link aggregation através de diferentes membros da stack
Suporte de sessões line rate bidireccionais de port-mirroring e remote portmirroring
Capacidade de suporte de Netflow v9 ou IPFIX
Capacidade de suporte de fluxos de rede, com um mínimo de 48000 fluxos, e permitindo através de fluxos: a. Efetuar deteção de anomalias de segurança b. Identificar os Top Talkers c. Customizar fluxos por perfil de utilizador d. Utilizar múltiplos collectors e. Exportar o consumo de bandwidth, em função do número de fluxos
Suporte, através do CLI, do plug and play de dispositivos ligados ao switch, nomeadamente de pc's, switches, AP's, telefones, impressoras, sem intervenção do utilizador, configurando/desconfigurando automaticamente e adaptando ao tipo de dispositivos os parâmetros de: a. VLANs (voz e dados, ou ambas) b. QoS c. Porta de acesso/trunk d. Spanning tree e. No caso de trunking, definir o tipo de encapsulamento f. Quando o dispositivo é desligado da porta, a configuração deverá ser removida automaticamente sem intervenção do utilizador g. No caso de PC's e impressoras, deverá ser possível a deteção baseada em MAC address e OUI (Organizational Unique Identifier). Nota: Esta funcionalidade deverá ser implementada sem ter de recorrer a IEEE 802.1X

Integração LAN e WLAN: São valorizadas soluções que integrem a componente de 4 LAN e WLAN num único equipamento - acesso unificado. Desta forma a solução deverá ter a capacidade para, através do mesmo hardware (com licenciamento adicional se necessário), garantir no switch a integração do controller wireless, que deverá ter capacidade para: a. Gerir até 100 Access Points b. Suporte de 2000 clientes c. Suportar wireless Throughput de 40 Gbps d. Suportar até 64 WLAN's e. Suporte de L2/L3 roaming f. Suporte de Access Points na frequência 2.4Ghz e 5Ghz g. Suporte de IEEE 802.11a/b/g/n h. Suporte de IEEE 802.11ac i. Suporte de IEEE 802.11i - EAP-TLS, EAP-SIM, EAP-TTLS, WPA, WPA2, 802.1x, WEP, WPA2 j. Detecção de interferências não WiFi k. Suporte de IEEE 802.11r l. Suporte de IEEE 802.11v m. Suporte de streams multicast n. Suporte de policieis para utilizadores e dispositivos com base em informação contextualizada o. Suportar visibilidade aplicacional para tráfego WLAN integrado com a componente de fluxos de rede em hardware, referida neste Caderno de Encargos p. Aplicação de QoS, Segurança e visibilidade aplicacional, independentemente do tipo de acesso (wired ou wireless) q. Sistema operativo único, para a componente de LAN e WLAN, configurado usando a mesma interface de linha de comandos r. Tanto a componente de LAN como de WLAN, deverão ser geríveis através de uma plataforma de gestão única s. Suporte de Gestão de largura de banda por: i. Access Point ii. Radio – 2.4Ghz ou 5Ghz iii. SSID iv. Cliente – PC, MAC, ipad, etc v. Aplicação – Facebook, yahoo, etc
Suportar qualquer tipo de dispositivo PoE e PoE+ de terceiros compatível com as normas 802.3af e 802.3at, incluindo telefones IP, WLAN AP, câmaras de vídeo vigilância, etc
Suporte nativo de funcionalidades de eficiência energética (802.3az), permitindo apenas a partir do software instalado no switch, medir o consumo de energia dos equipamentos ligados ao switch e aplicar políticas de otimização do consumo de energia; Esta solução deverá permitir: a) Medir o consumo de energia de cada um dos dispositivos PoE ligados na rede b) Otimizar o consumo de energia dos dispositivos PoE, permitindo a aplicação, por porta de switch, de políticas baseadas na hora do dia (ex: desligar todos os dispositivos às 22h e ligar tudo às 7h através apenas do CLI) c) Permitir, através da linha de comando (CLI), fazer o Wake up LAN (WoL) de dispositivos PoE e não PoE, através de políticas baseadas em hora do dia
Equipamento de referência: Cisco Catalyst 3850-48P-L ou equivalente

Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 3 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD.
Acesso, sem custos adicionais, às atualizações de software lançadas pelo fabricante para o modelo, pelo mesmo período de tempo fornecido no item anterior.
<u>Cordões RJ45 Cat6:</u>
200 unidades de 1,5m
50 unidades de 1m
30 unidades de 2m
20 unidades de 3m

LOTE 2 Rede WiFi
9 Access Points para áreas interiores
Deve suportar 13 canais na banda dos 2,4GHz (2,412 a 2,472 GHz; domínio ETSI), 16 canais na banda dos 5GHz (8 canais dos 5,180 a 5,320 GHz e 8 canais dos 5.500 a 5,700 GHz, excluindo as frequências entre 5,600 e 5,640 GHz; domínio ETSI)
Deve suportar os standards 802.11a, 802.11b/g, 802.11n, 802.11ac wave 2
Deve ter um design robusto para maior durabilidade, sem aberturas visíveis
Deve incluir antenas de dual band internas, para suportar 2.4GHz e 5GHz simultaneamente com uma antena única
O chipset deve fornecer uma experiência de alta densidade para a rede da organização, desenhado para aplicações de alto desempenho
O ponto de acesso deve suportar nativamente 802.11ac wave 2
Deve suportar as seguintes funcionalidades de 802.11ac wave 2: a) 4x4 Multiple-Input Multiple-Output (MIMO) com 3 (três) spatial streams, MU/SUMIMO b) Maximal ratio combining (MRC) c) Capacidade de implementar, em hardware, um mecanismo de beamforming para clientes não 802.11n, de forma a otimizar a performance não só desses clientes como de toda a rede d) Capacidade de implementar um mecanismo de beamforming para clientes 802.11n (1 spatial stream, 2 spatial streams e 3 spatial streams), de forma a otimizar a performance não só desses clientes como de toda a rede e) Capacidade de implementar um mecanismo de beamforming para clientes 802.11ac f) Canais de 20, 40, 80 e 160MHz g) PHY data rates até 5.2 Gbps h) Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) i) 802.11 Dynamic Frequency Selection (DFS) j) Suporte para Cyclic Shift Diversity (CSD) k) Suporte de 23dbm de potência de transmissão tanto nos 2.4Ghz como nos 5Ghz
Deve suportar a deteção e a otimização automática de Interferências, nomeadamente: a) Capacidade de detetar/classificar/mitigar/localizar pelo menos 20 tipos diferentes de interferências, entre 5 a 30 segundos, incluindo fontes de interferências não WiFi, ao mesmo tempo que processa o tráfego de rede b) Remediação automática sem intervenção humana c) Capacidade de providenciar em real-time informação raw do espectro RF para ser usada em troubleshooting em questões de interferências d) Capacidade de providenciar um index da "qualidade do espectro WiFi" como forma de visualização da performance da rede e dos impactos das interferências e) Capacidade de providenciar informação histórica das interferências para análise e ajuda rápida na resolução de problemas f) Incorporar "resource management" para potência, canais, deteção de falhas de

cobertura e otimização de performance g) Capacidade de poderem ser definidas políticas de segurança para que não sejam permitidos determinados tipos de equipamentos que interfiram com a rede (por exemplo para não permitir Playstations estarem a usar o espectro WiFi ou mesmo porem em causa a segurança da rede) h) Suportar balanceamento “enforced” entre a banda dos 2.4Ghz e os 5Ghz i) Suportar “Key Caching” e/ou outros métodos de forma a facilitar o roaming seguro e rápido
Deve ter 2 portas Ethernet 100/1000/2500/5000 Multigigabit Ethernet (RJ-45) que funcionem com cablagem CAT 5e e CAT 6/6a
Deve ter dois rádios (XOR e 5GHz) definidos via software
Deve ser modular e suportar módulos expansíveis, nomeadamente um terceiro rádio para WIPS, 3G Small Cell, 802.11ac 2, ou outros módulos que possam ficar disponíveis no futuro
Possibilidade de ser registado e passar a ser gerido centralmente pelo Wireless Controller em uso na instituição (Cisco 5520 Wireless Controller)
Possibilidade de ser registado no módulo wireless controller de switches Cisco Catalyst 3850 existentes na infraestrutura de rede da instituição (nomeadamente em pólos remotos, sem Wireless Controller local)
Integração completa com a plataforma de gestão (NMS) Cisco Prime Infrastructure, em uso na instituição
Portas de gestão: a) 100/1000BASE-T autosensing (RJ-45 - AUX port) b) Management console port (RJ-45)
Deve poder operar na gama de temperaturas entre 0°C e 40°C
Deve ter antenas integradas: a) 2.4 GHz, ganho 6.0 dBi, internal omnidirectional, horizontal beamwidth 360° b) 5 GHz, ganho 6.0 dBi, internal omnidirectional, horizontal beamwidth 360°
Os Pontos de Acesso devem poder ser alimentados de diversas formas, nomeadamente: a) 802.3at PoE+, Universal Power over Ethernet, 802.3at power injector e power supply
Qualidade de serviço - deve: a) Suportar Wi-Fi Multimedia (WMM) e IEEE 802.11e b) Suportar WiFi Alliance Certification para WMM e WMM power save c) Suportar multicast fiável para vídeo d) Suportar QoS e CAC (Call Admission Control)
Segurança - deve: a) Suportar Management Frame Protection (IEEE 802.11w-2009) b) Suportar certificados locais aos pontos de acesso usando uma PKI (Public Key Infrastructure)
Operar como sensor para WIPS
Suporte de: a) IEEE 802.11i, WPA, WPA2 b) IEEE 802.1x c) Suportar 16 WLAN por AP d) acesso por SSH
Deve suportar pelo menos os seguintes métodos de autenticação: a) Advanced Encryption Standards (AES)

b) Temporal Key Integrity Protocol (TKIP) c) EAP-FAST d) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) e) EAP-Tunneled TLS (TTLS) e Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) f) Protected EAP (PEAP) v0 e EAP-MSCHAPv2 g) Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) h) PEAPv1 ou EAP-Generic Token Card (GTC) i) EAP-Subscriber Identity Module (SIM) j) Suportar encriptação DTLS baseada em hardware
Equipamento de referência: Cisco Aironet 3802i ou equivalente
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 3 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD.
Acesso, sem custos adicionais, às atualizações de software lançadas pelo fabricante para o modelo, pelo mesmo período de tempo fornecido no item anterior
<u>2 Access Points de exterior</u>
Deve suportar 13 canais na banda dos 2,4GHz (2,412 a 2,472 GHz; domínio ETSI), 16 canais na banda dos 5GHz (8 canais dos 5,180 a 5,320 GHz e 8 canais dos 5.500 a 5,700 GHz, excluindo as frequências entre 5,600 e 5,640 GHz; domínio ETSI)
Deve suportar os standards 802.11a, 802.11b/g, 802.11n, 802.11ac wave 2
Deve incluir antenas de dual band para suportar 2.4GHz e 5GHz
Deve possuir conectores N-type para pelo menos 2 antenas single-band @2.4GHz e para pelo menos 2 antenas single-band @5GHz
Pelo menos 2 dos conectores devem suportar antenas dual-band @2.4GHz/5GHz simultâneos na mesma porta, configurável por software
O chipset deve fornecer uma experiência de alta densidade para redes corporativas, desenhado para aplicações de alto desempenho
O ponto de acesso deve suportar 802.11ac wave 2 nativamente
Deve suportar as seguintes funcionalidades de 802.11ac wave 2 a) Pelo menos 2x2 Multiple-Input Multiple-Output (MIMO) com 2 (dois) spatial streams, MU/SU-MIMO b) Maximal ratio combining (MRC) c) Capacidade de implementar um mecanismo de beamforming para clientes 802.ac d) Canais de pelo menos 20, 40 e 80MHz e) PHY data rates pelo menos até 867Mbps f) Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) g) 802.11 Dynamic Frequency Selection (DFS) h) Suporte para Cyclic Shift Diversity (CSD) i) Suporte de 27dbm de potência de transmissão tanto nos 2.4Ghz como nos 5Ghz
Deve suportar a deteção e a otimização automática de interferências, nomeadamente:

a) Capacidade de detetar/classificar/mitigar/localizar pelo menos 20 tipos diferentes de interferências, entre 5 a 30 segundos, incluindo fontes de interferências não WiFi, ao mesmo tempo que processa o tráfego de rede b) Remediação automática sem intervenção humana c) Capacidade de providenciar em real-time informação raw do espectro RF para ser usada em troubleshooting em questões de interferências d) Capacidade de providenciar um index da "qualidade do espectro WiFi" como forma de visualização da performance da rede e dos impactos das interferências e) Capacidade de providenciar informação histórica das interferências para análise e ajuda rápida na resolução de problemas f) Incorporar "resource management" para potência, canais, deteção de falhas de cobertura e otimização de performance g) Capacidade de poderem ser definidas políticas de segurança para que não sejam permitidos determinados tipos de equipamentos que interfiram com a rede (por exemplo para não permitir Playstations estarem a usar o espectro WiFi ou mesmo porem em causa a segurança da rede) h) Suportar balanceamento "enforced" entre a banda dos 2.4Ghz e os 5Ghz i) Suportar "Key Caching" e/ou outros métodos de forma a facilitar o roaming seguro e rápido
Deve ter as seguintes portas: a) 1 WAN Ethernet port 10/100/1000base-T (RJ-45), PoE in b) 1 SFP port (suportando módulos óticos e de cobre) c) Management console port (RJ-45) d) Entrada de alimentação DC
Condições ambientais e físicas: a) Gama de temperatura de operação: -40°/65°C b) Resistência ao vento: operação até 161 km/h constantes; sobrevivência com rajadas até 265km/h c) Proteção contra água/objetos: IP67; NEMA type 4X d) Congelamento: NEMA 250-2008 e) Corrosão: NEMA 250-2008 (600 horas) f) Radiação solar: EN 60068-2-5 (1200 W/ m2) g) Vibração: MIL-STD-810
Os Pontos de Acesso devem poder ser alimentados de diversas formas, nomeadamente: a) 802.3at PoE+, Universal Power over Ethernet, 802.3at power injector e power supply
Segurança: a) Suportar Management Frame Protection (IEEE 802.11w-2009) b) Suportar certificados locais aos pontos de acesso usando uma PKI (Public Key Infrastructure) 11 c) IEEE 802.11i, WPA, WPA2 d) IEEE 802.1x e) Suportar 16 WLAN por AP f) Suporte de telnet e SSH g) Deve suportar pelo menos os seguintes métodos de autenticação: i . Advanced Encryption Standards (AES)

ii. Temporal Key Integrity Protocol (TKIP) iii. EAP-FAST iv. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) v. EAP-Tunneled TLS (TTLS) ou Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) vi. Protected EAP (PEAP) v0 ou EAP-MSCHAPv2 vii. Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) viii. PEAPv1 ou EAP-Generic Token Card (GTC) ix. EAP-Subscriber Identity Module (SIM)
Caraterísticas das antenas a fornecer com os access points: a) Tipo: Omnidirecional de array colinear b) Gama de frequências de operação: 2400/2483MHz; 5150/5875MHz c) Gama VSWR 2:1 (voltage standing wave ratio): 2400/2483MHz; 5150/5875MHz d) Impedância de entrada nominal: 50ohm e) Ganho (2400/2483MHz): 4dBi f) Ganho (5250/5875MHz): 7dBi g) Polarização: Linear h) Abertura E-plane 3dB: 30° @2.4GHz; 14° @5GHz i) Abertura H-plane 3dB: Omnidirecional (360°) j) Tipo de conector: N-Male k) Gama de temperatura de operação: -40°/85°C l) Proteção contra água/objetos: IP66, IP67 m) Resistência ao vento: operação até 161km/h constantes; sobrevivência com rajadas até 265km/h
Deve ter dois rádios (XOR e 5GHz) definidos via software
Possibilidade de ser registado no módulo wireless controller de switches Cisco Catalyst 3850 existentes na infraestrutura de rede da instituição
Cada access point deve incluir ainda os seguintes acessórios: 1 (um) Kit de montagem fixa em poste e/ou parede/mural para ambientes exteriores, do mesmo fabricante do access point e integrando-se com este; 2 (duas) antenas para ambientes exteriores, do mesmo fabricante do access point, compatíveis e integrando-se com este; 1 (um) alimentador IEEE 802.3at para funcionamento em áreas interiores, do mesmo fabricante do access point e integrando-se com este, com 2 portas Ethernet 10/100/1000 (uma para ligação LAN e a outra para ligação+alimentação ao access point), suportando pelo menos 25W no equipamento alimentado pela saída
Equipamento de referência: Cisco Aironet 1542i ou equivalente
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 3 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD.
Acesso, sem custos adicionais, às atualizações de software lançadas pelo fabricante para o modelo, pelo mesmo período de tempo fornecido no item anterior

<u>1 Controladora wireless</u>
Equipamento em Appliance Física
Kit para instalação em Rack
Dimensão máxima de 1 RU
Capacidade mínima de 4 Gbps de throughput
Licenciamento de base para gerir 20 access points
Escalabilidade para gerir até 150 Access Points
Capacidade para suportar até 3000 clientes
Suporte para 4096 VLANs
Suporte de um mínimo de 1 porta do tipo Multigigabit e 4 portas físicas do tipo
Pelo menos 2 portas com suporte PoE
Suporte para as normas IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave1 e Wave2
Suporte de autenticação IEEE 802.1X, com pelo menos os seguintes métodos:
a) EAP-FAST
b) EAP-TLS
c) EAP-TTLS
d) PEAPv0/EAP-MSCHAPv2
e) PEAPv1/EAP-GTC
Suporte de segurança IEEE 802.11i
Suporte para implementar WEP (Wired Equivalent Privacy), chaves estáticas e dinâmicas (40 bits e 128 bits)
Suporte para implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP)
Suporte para implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES)
Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP, TKIP e WEP
Suporte de Datagram Transfer Layer Security (DTLS)
Suporte para 802.1Q
Suporte para Link Aggregation 802.1 AX
Suporte para CAPWAP
Suporte para a administração e acesso via: HTTP, HTTPS, SNMPv2C 2 SNMPv3, SSH
Capacidade de funcionar como servidor de DHCP, DHCP Proxy e DHCP Relay
Suporte para IPv4 e IPv6
Suporte para AAA mediante um servidor de RADIUS/TACACS+ para gerir as políticas dos utilizadores
Suporte para autenticação de utilizadores com base num servidor RADIUS e Web based authentication
O controlador WiFi deve possuir pelo menos uma porta de consola local para gestão
Interfaces de gestão:
a) Web-based: HTTP/HTTPS
b) Interface Web completamente funcional nas versões mais recentes dos browsers Firefox e Chrome
c) Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port

d) Integração com plataforma de gestão Cisco Prime Infrastructure
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 3 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD.
Acesso, sem custos adicionais, às atualizações de software lançadas pelo fabricante para o modelo, pelo mesmo período de tempo fornecido no item anterior

LOTE 3
<u>1 Unidade de Alimentação Ininterrupta (UPS)</u> , com as seguintes especificações mínimas:
Possibilidade de instalação nos modos torre e rack;
Capacidade mínima de energia de saída: 10000 VA
Potência mínima de saída: 10000 W;
Entrada/saída: monofásica, 230V; 50/60 Hz;
Quantidade mínima de saídas AC: 6
Autonomia mínima com 60% de carga: 20 minutos;
Carta de rede do tipo Ethernet (RJ45);
Suporte de monitorização SNMP;
Interface de gestão Web;
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 2 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD

LOTE 4
1 Firewall , com as seguintes especificações mínimas:
A solução proposta deverá endereçar todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante (single vendor): a. 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; b. Intrusion Prevention System; c. User Identity Acquisition d. Application Control and URL filtering e. Anti – Bot / Anti – Virus f. Threat Emulation (Sandboxing) g. Threat Extraction (scrubbing) h. Anti – Spam and Email Security i. IPSec VPN j. Remote Access VPN (Mobile Access) k. Data Loss Prevention l. Logging and Status m. Event Correlation and Reporting
A solução proposta deverá conter uma plataforma de gestão dedicada com: a. Centralização de políticas, logs, reports; b. Sem limite de storage com base em requisitos de licenciamento; c. O servidor de gestão deverá ter a capacidade de obter detalhes de configuração diretamente das gateways de firewall (fetch de informação de routing, interfaces, etc.) de forma “automática”, e não apenas se estas forem instanciadas previamente via template, a partir do servidor de gestão;
Requisitos mínimos de performance: a. Threat Prevention/Extraction: 1.7 Gbps b. NextGen Firewall: 3.7 Gbps c. Intrusion Prevention System: 4.6 Gbps d. VPN Throughput: 2.5 Gbps e. Firewall Throughput: 8.5 Gbps f. Conexões por segundo: 67.000
Requisitos mínimos físicos: a. Armazenamento: 240GB b. Memória RAM: 8GB, expansível a 32GB c. Deverá ser flexível quanto o número/tipos de interfaces a aplicar ao chassis: i. 8x1GE UTP (até 18 portas); ii. 4x1GE SFP (até 4 Portas); iii. 4x10GE SFP+ (até 4 Portas); d. Possibilidade de adicionar Interface LOM (Lights Out Manager);
Funcionalidades mínimas de rede: a. Suporte para 1024 interfaces vlan; b. Suporte para 4096 interfaces vlan (em cenário de contextos virtuais de firewall);

c. Suporte para protocolos de agregação de links (LACP 802.3ad); d. Suporte para funcionamento em modo L2 (bridging) e L3 (routing); e. Suporte de NAT i. Static, Hide, PAT; ii. NAT44, NAT46, NAT64, NAT66; f. Suporte para routing estático; g. Suporte para Policy Based Routing (PBR); h. Suporte para protocolos de routing dinâmico: i. BGP, OSPF (v2 v3), RIP; ii. Suporte para multicast: i. Routing Multicast: i. L2 (IGMP v1 v2); ii. L3 (PIM-SM, PIM-SSM, PIM-DM);
Suporte de funcionalidades de alta disponibilidade: a. Activo/Passivo ou Activo/Standby: i. VRRP ou IP Virtual; ii. Failover: 1. Falhas de routing; 2. Falhas de dispositivo; 3. Falhas de link; iii. Sincronização de sessões entre membros do cluster;
Requisitos técnicos/lógicos mínimos: a. O equipamento de segurança, deve utilizar a tecnologia de Stateful Inspection, para construir e manter a tabela de sessões (fluxos de comunicação). b. 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. c. A solução deve identificar/controlar o acesso de pelo menos 150 serviços/protocolos. d. Na interface da plataforma de gestão deve ser possível visualizar número de acessos por regra. e. A solução tem de suportar que se apliquem regras em intervalos de tempo, para que seja possível definir o tempo útil das mesmas. f. A comunicação entre a firewall e a solução de gestão, tem de ser encriptada e autenticada com recurso a infraestrutura própria de PKI g. A Firewall tem de suportar métodos de autenticação por sessão, utilizadores e clientes. h. Os seguintes métodos de autenticação de utilizadores têm de ser suportados pelos módulos de VPN e Firewall: i. Tokens (ie -SecureID) ii. TACACS iii. RADIUS iv. Certificados Digitais i. 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; j. A solução tem de suportar as funções de DHCP server e Relay; k. A solução tem de suportar a função de proxy em HTTP e HTTPS; l. A solução tem de ter capacidade de trabalhar em modo transparente/Bridge (L2)

m. A solução tem de suportar alta disponibilidade ou load-sharing e sincronização de estados entre os dois membros do cluster;

Sistema de prevenção de intrusões (IPS):

a. O fabricante deve fornecer evidências da sua posição de liderança, ano após ano, no Quadrante Mágico do Gartner para:

- i. Soluções de Prevenção de Intrusão;
- ii. Soluções de Firewall Enterprise;

b. O IPS deve ser baseado nos seguintes mecanismos de deteção:

- i. Assinaturas
- ii. Anomalias no protocolo
- iii. Controlo Aplicacional
- iv. Análise de comportamento

c. Os Módulos de IPS e firewall devem estar integrados na mesma plataforma.

d. O administrador deve ter a possibilidade de configurar a inspeção para proteção apenas da rede interna

e. O IPS deve ter opções para criar perfis com base em assinaturas para proteção de Clientes ou servidores. Também deve ser possível criar um perfil para proteção de ambos.

f. O IPS deve fornecer pelo menos dois perfis/políticas predefinidas que podem ser utilizados no deployment da solução.

g. O IPS deve ter um mecanismo fail-open baseado em software, ajustável com base em limites do gateway, CPU ou utilização de memória.

h. O IPS deve ter mecanismo automático para ativar ou gerir as novas assinaturas após atualizações.

i. O IPS deve suportar exceções com base em origem, destino, protocolo ou uma combinação dos três

j. O IPS deve permitir mudar para o modo de deteção, sem alterar parâmetros individuais, por forma a facilitar as ações de troubleshooting.

k. O IPS deve possuir uma solução centralizada de correlação e relatório de eventos

l. O administrador deve poder ativar de forma automática novas proteções, com base em parâmetros configuráveis:

- i. impacto no desempenho
- ii. Grau de severidade da ameaça
- iii. nível de confiança
- iv. proteções do cliente
- v. proteções do servidor

m. O IPS deve ser capaz de detetar e prevenir os seguintes tipos de ameaça:

- i. uso indevido de protocolo
- ii. comunicações de malware
- iii. tentativas de uso de protocolos de tunneling
- iv. tipos genéricos de ataque sem assinaturas predefinidas.

n. Para cada proteção, a solução deve incluir o tipo de proteção (relativamente a servidor ou cliente):

- i. gravidade da ameaça
- ii. impacto no desempenho
- iii. nível de confiança
- iv. referência - (ie CVE)

o. O IPS deve ser capaz de capturar de pacotes/evidências para proteções

específicas

p. 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:

- i. Serviços de email
- ii. DNS
- iii. FTP
- iv. Serviços do Windows (Microsoft Networking)

q. O fornecedor deve fornecer evidências de liderança na proteção de vulnerabilidades Microsoft

r. O IPS e/ou o Application Control deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (Anonymizers)

s. O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou hosts.

t. A solução deve proteger DNS Cache Poisoning e impedir o acesso dos utilizadores a endereços de domínio bloqueados

u. Solução deve fornecer proteções para protocolos VOIP

v. 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

w. IPS deve ter proteções SCADA

x. IPS deve possibilitar a conversão de assinaturas SNORT

y. 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

Aquisição de identidade de utilizadores (User ID Acquisition):

a. Deve ser capaz de adquirir a identidade dos utilizadores, com base na consulta dos eventos de segurança da Microsoft Active Directory

b. Deve ser possível a autenticação através de uma browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio.

c. Deve ter um agente que possa ser instalado nos endpoints, para reportar a firewall as identidades dos utilizadores.

d. A solução deve integrar-se perfeitamente com Microsoft Active Directory, IF23 MAP e Radius

e. O impacto do uso da solução de aquisição de identidade no CPU das AD, deve ser inferior a 3%.

f. A solução de aquisição de identidade deve suportar soluções de Terminal server e citrix

g. A solução deve permitir a identificação de utilizadores que acedem através de um proxy (exemplo: X-forwarded headers)

h. 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

i. Deve suportar autenticação Kerberos para single sign on

j. Deve suportar LDAP nested groups

k. Deve ser capaz de partilhar identidades de utilizadores entre vários gateways de segurança

l. Deve ser capaz de criar identity roles (grupos de identidades) para serem invocados em diferentes aplicações da solução.

Filtragem de URL e Controlo de Aplicações:

- a. A solução deve reconhecer e controlar mais de 8000 aplicações conhecidas
- b. 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
- c. A solução deve permitir criar uma regra de filtragem de conteúdos com várias categorias
- d. A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL
- e. A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias.
- f. A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores
- g. A solução, após 4 semanas de produção, deve ter em cache cerca de 99% das solicitações de categorização.
- h. A solução deve ter uma interface fácil de pesquisa de aplicações e URL's
- i. A solução deve categorizar aplicações e URL's por fator de risco
- j. A política de URLF e Application Control deve poder ser definida por identidade do utilizador
- k. A base de dados de URLF e Application Control devem ser atualizados por um serviço Cloud
- l. A solução deve ter o controlo de aplicações e URLF unificado na mesma política.
- m. 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
- n. A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda
- o. A solução deve permitir exceções com base em objetos de rede previamente definidos
- p. A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação.
- q. A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria
- r. A solução deve fornecer um mecanismo de substituição na categorização de URL

Anti-bot e Anti-Virus

- a. O fornecedor deve ter solução de Anti-Bot e Anti-Virus integrado na firewall
- b. A Solução de Anti-Bot deve ser capaz de detetar e parar comportamentos de rede suspeitos
- c. O aplicativo Anti-Bot deve usar um mecanismo de deteção baseado em varias pontos. Reputação de endereços IP, URLs e DNS e detetar padrões de comunicação de bots.
- d. A proteção Anti-Bot deve ter capacidade de efetuar Scan a ações de bot.
- e. 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.
- f. A solução deve ter suporte para proteção contra-ataques de spear phishing
- g. DNS based attacks - A solução deve ter recursos de detecção e prevenção para C&C DNS hideouts:
- i. Pesquisa de padrões de tráfego de C & C, não apenas no destino de DNS

ii. Reverse engineer do Malware para descobrir seu DGA (Domain Name Generation) iii. DNS Trap, como parte da política de ameaças, interceta e analisa tentativas de comunicações do endpoint com C&C. iv. A solução deve detetar e prevenir ataques de DNS tunneling. h. A política de Anti-Bot e Anti-Virus deve ser gerida a partir de uma consola central i. A solução de Anti-Bot e Anti-Virus deve ter um mecanismo centralizado de correlação e relatório de eventos j. A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos k. A solução de antivírus deve poder inspecionar o tráfego SSL. l. O Anti-Bot e o Anti-Virus devem ter atualizações em tempo real na cloud. m. O Antivírus deve ser capaz de impedir a entrada de arquivos maliciosos n. O Antivírus deve ser capaz de analisar arquivos compactados o. Políticas antivírus e Anti-Bot devem ser geridas centralmente e ser possível a parametrização das mesmas. p. O Antivírus deve suportar a análise de links dentro de emails q. O antivírus deve analisar os ficheiros que estão a passar no protocolo CIFS
Emulação e Extração de Ameaças: a. A solução deve ter a capacidade de proteger contra-ataques desconhecidos (malware Zero Day)antes que proteções de assinatura estática sejam criadas: i. Proteção em Tempo Real para malware desconhecido na navegação Web ii. Proteção em Tempo Real para malware desconhecido em email b. Cenários de implantação: i. A solução deve fazer parte da arquitetura de prevenção de ameaças (com IPS, AV, AB, URLF, APP FW) ii. A solução deve fornecer solução de implementação On Prem e Cloud Based iii. Solução de Cloud pura iv. A solução deve suportar integração com 3rd party (public API) v. A solução deve suportar implementação em modo in-line vi. A solução deve suportar a implementação modo MTA (Mail Transfer Agent) vii. A solução deve suportar implementação em modo de porta TAP / SPAN viii. A solução não deve exigir infraestrutura separada para proteção email e proteção Web ix. A solução deve suportar a implementação em modo cluster. c. Tipos de ficheiros Suportados - A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash especificamente: i. 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, xlsx, xlt, xltm, xltx, xlw, zip, pif, com, gz, bz2, tgz, apk(android), ipa (iphone), ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh; d. A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash, que sejam transmitidos pelos protocolos: i. HTTP ii. HTTPS iii. FTP iv. SMTP v. CIFS (SMB)

vi. TLS SMTP
e. OS support:
i. O mecanismo de emulação deve suportar vários sistemas operativos, como XP e Windows7, 8,10 32/64 bits, incluindo imagens personalizadas
ii. A solução deve suportar cópias LICENCIADAS de Microsoft WINDOWS e Microsoft Office através de um contrato com a Microsoft.
iii. A solução deve detectar chamadas API, alterações em ficheiros, system registry, ligações de rede e processos do sistema
iv. A solução deve suportar análise estática para windows, mac OS-X, Linux ou qualquer plataforma x86
f. O mecanismo de emulação deve ser capaz de inspecionar, emular, prevenir e compartilhar os resultados do evento de sandbox na infraestrutura de antimalware
g. A solução deve permitir a emulação de ficheiros maiores que 10 Mb, em todos os tipos suportados
h. A solução deve suportar automated machine learning based detection engines
i. 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.
j. A solução deve detectar ROP e outras técnicas de exploitation (por exemplo, elevação de privilégios), analisando o CPU
k. A solução deve suportar a análise de links no corpo do e-mail para deteção de Malware Zero Day
l. A solução deve ser capaz de verificar o histórico de URLs registrados nos últimos X e-mails e verificar se a classificação foi alterada (por exemplo: de Clean para malicious)
m. Tempo médio de emulação, para um veredito de malware suspeito como benigno não deve ser muito superior a 1 minuto
n. Tempo médio de emulação, para um veredito de malware suspeito como maligno não deve ser muito superior a 3 minutos
o. A solução de emulação de ameaças deve permitir "Geo Restriction", que permite que as emulações sejam restritas a um país
p. 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.
q. O mecanismo de emulação deve exceder 90% na taxa de captura nos testes do Total de vírus em que os PDFs e os arquivos maliciosos conhecidos são modificados com cabeçalhos "não usados" para demonstrar a capacidade das soluções de detetar malwares desconhecidos
r. A solução deve detetar o tráfego de C & C de acordo com a reputação dinâmica de ip / url
s. A solução deve ser capaz de emular e extrair arquivos incorporados em documentos
t. A solução deve ser capaz de analisar documentos com URL's
u. Na funcionalidade de Sandboxing/Scrubbing, 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;
Deteção de atividades em sistema
a. A solução deve ter a capacidade de detetar atividades fora de "padrão de

utilização/protocolo”: i. Chamadas de API ii. Alterações no sistema de arquivos iii. Alterações de Registo iv. Ligações de rede v. Em Processos do sistema Operativo vi. Criar e eliminar arquivos vii. Modificação de arquivos viii. Adição de código ao kernel ix. Detetar tentativas de elevação de privilégios x. Alterações no kernel (Alterações de memória realizadas pelo código do kernel, não o fato de que um driver ser carregado - isso é controlado pelo item acima) xi. Análise de comportamento do kernel (analisar a atividade do código, não as alterações efetuadas pelo utilizador) xii. Contornar UAC (user access control)
Mecanismos Anti-evasão: a. A solução proposta deverá ter capacidade de deteção de técnicas de evasão (emulação/sandboxing) para posterior reação e mitigação de ameaças; b. A solução deverá ser resiliente e identificar casos onde a execução de código malicioso (malware/shell-code) não ocorra mediante a deteção de um ambiente virtualizado (técnica de evasão para contornar mecanismos de deteção por sandboxing); c. A solução deverá ser resiliente e detetar delays implementados na execução de código malicioso (malware/shell-code); d. A solução deverá ser resiliente a situações em que a execução de código malicioso (malware/shell-code) apenas ocorre após um restart/shutdown da workstation/endpoint infetado;
Extração de ameaças (File Scrubbing/Flattening): a. A solução proposta deverá ter a capacidade de eliminar ameaças existentes em conteúdos dinâmicos/objetos embebidos em ficheiros; b. A solução proposta deverá ter a capacidade de reconstrução dos ficheiros, excluindo os conteúdos ativos, e mantendo apenas conteúdos seguros; c. A solução proposta deverá ter a capacidade de converter ficheiros reconstruídos (em que os conteúdos ativos foram excluídos) em formato PDF, para serem entregues em tempo real ao utilizador, de forma a melhorar a experiência de utilização; d. A solução proposta deverá ser configurável e flexível, de forma a possibilitar manter o formato do ficheiro original, especificando o tipo de conteúdo a ser removido;
Anti-Spam & Email Security: a. 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; b. A solução proposta deverá incluir mecanismos de proteção com base em serviços online de IP reputation, de forma a evitar falsos positivos; c. A solução deverá incluir mecanismos de proteção imediata (Dia Zero) para novos vírus propagados por email.

IPsec VPN:

- a. 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;
- b. A solução deverá suportar criptografia 3DES e AES-256 para IKE Phase 1 e 2.
- c. A solução deverá suportar criptografia IKEv2 plus "Suite-B-GCM-128" e "SuiteB-GCM-256" for IKE Phase 2;
- d. 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;
- e. A solução deverá suportar os seguintes tipos de mecanismos de integridade de dados: md5, sha1, SHA-256, SHA-384 and AES-XCBC;
- f. A solução proposta deverá suportar as seguintes funcionalidades VPN:
 - i. Site-to-site:
 1. Full Mesh (todos para todos);
 2. Estrela (Sites remotos para Site principal);
 3. Hub&Spoke (Site remotoA para Site RemotoB, através de site principal);
 4. Suporte para configuração através de GUI, com opção de drag&drop de objetos nas comunidades VPN;
 - ii. Suporte para VPN's de acesso remoto "clientless" e "client based";
 - iii. Suporte para aplicação de políticas de segurança específicas, para controlo de tráfego associado à comunidade VPN;

Security Management:

- a. A solução deverá possibilitar a segmentação da política de segurança numa estrutura de subpolíticas;
- b. A solução deverá possibilitar a segmentação da política de segurança numa estrutura de layers;
- c. A solução deverá possibilitar a integração de logs e audit logs numa única consola, para contextualizar o administrador ao efetuar alterações sobre a política de segurança;
- d. A solução de gestão deverá suportar role based access control, para segregar acessos de administração para gestão de política e visualização de logs;
- e. A solução deverá implementar um mecanismo de comunicação segura, assente em certificados, entre todas as componentes de segurança integradas no sistema de gestão centralizada;
- f. A solução deverá incluir um Certificate Authority x.509 com capacidade para gerir/gerar certificados internos, para autenticação de utilizadores em acessos VPN remotos;
- g. A solução deverá disponibilizar um mecanismo de pesquisa para facilitar a utilização e identificação de objetos, com base no seu endereço IP;
- h. A solução deverá disponibilizar métricas de "hit count" nas regras presentes na política de segurança;
- i. A solução deverá possibilitar a utilização de etiquetas (labels) ou secções (tabs) para melhor organização da política de segurança;
- j. A solução deverá permitir gravar a política de forma integral ou parcial;
- k. A solução deverá disponibilizar um mecanismo de validação da política de segurança, antes da sua instalação nas gateways de firewall;
- l. A solução deverá disponibilizar um mecanismo de backup e revisão da política

de segurança, possibilitando comparar versões da política e reverter para versões anteriores, se necessário;
Logging e Monitorização: a. A solução de logging, deverá estar integrada na componente de gestão centralizada, e possibilitar a visualização de logs afetos a políticas específicas, sem ser necessário recorrer a uma nova janela, ou aplicação; b. A solução deverá poder ser integrada na componente de gestão centralizada, ou numa appliance/máquina virtual dedicada; c. A solução deverá ter a capacidade de produzir logs de todas as políticas (30k logs/seg); d. 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; e. A solução deverá suportar um mecanismo de captura de pacotes para eventos de IPS, para facilitar despiste e análise forense; f. A solução deverá implementar um mecanismo seguro de forwarding de logs, com autenticação e encriptação, para evitar potenciais ataques (ex. 33 Eavesdropping); i. Os logs deverão ser transferidos de forma segura entre a FW gateway, o log server, e o utilizador final; g. A solução deverá disponibilizar detalhes sobre o estado de todos os túneis IPSEC, site-to-site e remote access (client-to-site); h. A solução deverá possibilitar a customização de valores de threshold, para execução de ações, uma vez atingido/ultrapassado esse threshold: log, alert, snmp-trap, email notification;
Correlação de eventos e reporting: a. A solução deverá integrar a componente de reporting e correlação de eventos com a sua componente de gestão centralizada; b. A solução deverá ter a capacidade de correlacionar eventos de todas as funcionalidades ativas nas demais gateways (FW, IPS, URL-F, etc.); c. A solução deverá possibilitar a criação de filtros de logging, com base em qualquer característica, tal como: aplicação, ip de origem e destino, serviço, tipo de evento, severidade do ataque, país de origem e destino, etc.; d. A solução deverá disponibilizar um mecanismo para assignar os filtros criados a diferentes tipos de gráficos, a serem atualizados periodicamente, apresentando todos os eventos que igualem o filtro aplicado, permitindo ao operador focar-se nos eventos mais importantes; e. A solução deverá assegurar a possibilidade de pesquisar na lista de eventos, e garantir o “drill down” de detalhes em pesquisas e análise forense; f. A solução deverá ter capacidade de detectar e alertar para eventos de login de administradores, em horários não frequentes; g. A solução deverá detetar ataques de “credential guessing / brute force”; h. A solução deverá reportar todos os eventos de alteração/instalação de políticas de segurança; i. A solução deverá incluir relatórios horários, diários, semanais e mensais predefinidos, incluindo pelo menos: Top Events, Top Sources, Top Destinations, Top Services, etc.;

j. A solução de reporting deverá disponibilizar informação consolidada sobre: i. Volume de ligações bloqueadas por uma regra de segurança em particular; ii. Top de origens bloqueadas, e os destinos e serviços respetivos; iii. Top de regras mais utilizadas na política de segurança; iv. Top de ataques detetados no perímetro, com informação das origens e destinos associados; v. Atividade web por user, com top de web users e websites mais utilizados;
Compliance e Boas Práticas: a. A solução deverá contemplar Risk Governance e Compliance totalmente integrado na componente de gestão centralizada; b. A solução deverá ter uma opção para controlar o cumprimento em tempo real de todos os serviços de segurança do produto; c. A solução deverá ter uma opção para entregar a avaliação em tempo real de acordo com as regulamentações principais (tais como: PCI-DSS, HIPAA, SOX, GDPR...); d. A solução deverá ter uma opção para notificação imediata sobre as mudanças nas políticas que afetem o cumprimento das certificações; e. A solução deverá ter uma opção para disponibilizar recomendações práticas para melhorar a conformidade de segurança; f. A solução deverá ter uma opção para recomendar Práticas recomendadas de segurança; g. A solução deverá ter uma opção para traduzir os requisitos regulamentares em melhores práticas de segurança acionáveis; h. A solução deverá ter uma opção para monitorizar constantemente a configuração das gateways com as melhores práticas de segurança; i. A solução deverá ter uma opção para gerar relatórios de avaliação automatizados para avaliar a conformidade com os principais regulamentos; j. A solução deverá ter uma opção para integrar plenamente na infra-estrutura de arquitetura de Software e Gestão; k. A solução deverá ter uma opção para verificar a conformidade com cada mudança de política para todas as funcionalidades dos equipamentos de firewall.
SSL Inspection (inbound / outbound): a. A solução deverá suportar inspeção SSL (inspection/decryption) com performance comprovada em todas as tecnologias de mitigação; b. A solução deverá suportar Perfect Forward Secrecy (PFS , ECDHE cipher suites); c. A solução deverá suportar AES-NI, AES-GCM for improved throughput; d. A solução deverá suportar a integração das tecnologias de emulação/sandboxing com inspeção SSL; e. A solução deverá permitir a reutilização da base de dados de URL Filtering, para criação de políticas de inspeção de SSL granulares;
Equipamento de referência: CheckPoint 6200 NGTP ou equivalente
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 3 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD

Acesso, sem custos adicionais, às atualizações de software lançadas pelo fabricante para o modelo, bem como a todas as atualizações de assinaturas das funcionalidades de segurança contratadas, pelo mesmo período de tempo proposto pelo concorrente para o item anterior.

LOTE 5	
<u>Infraestrutura de Voz</u>	
<u>8 Telefones IP</u>, com as seguintes especificações mínimas:	
Suporte de Voz em HD	
Suporte dos codecs de voz G.722, G.711(A/μ), G.729A/B, G.726, G.723.1, iLBC, Opus	
DTMF: In-band, Out-of-band (RFC 2833) e SIP INFO	
RTCP-XR (RFC3611), VQ-RTCPXR (RFC6035)	
Duas portas Gigabit Ethernet	
Alimentação elétrica por PoE (Power over Ethernet)	
Display de 7" e 800x400 píxeis ou superior, com teclado iluminado	
Suporte de auricular Bluetooth com USB dongle	
Suporte de até 16 contas SIP	
Suporte de até 6 módulos de expansão	
Entrada RJ9 para conexão auricular	
Suporte de chamada em espera	
Função de toque com:	
a. Tecla de espera	
b. tecla de navegação	
c. tecla de remarcação	
d. tecla função mãos livres	
e. Tecla, mute	
f. tecla para lista de chamadas efetuadas	
g. tecla R	
Chamada de conferência a 3	
Pelo menos 5 toques programáveis	
Livro de endereços com até 1000 contactos	
Suporte de livro de contactos remoto por XML/LDAP	
Histórico de chamadas: dialed/received/missed/forwarded	
Teclas de controlo de volume	
Controlo de volume no alta-voz, controlo de volume no terminal e controlo de volume no timbre	
Indicador luminoso de chamada	
Configuração: browser/telefone/auto-provisionamento	
Auto provisionamento em massa via FTP/TFTP/HTTP/HTTPS	
SIP v1 (RFC2543) e v2 (RFC3261)	
Redundância de Call server	
NAT traversal: STUN mode	
Proxy mode e peer-to-peer SIP link mode	
Atribuição de endereçamento IP: estático/DHCP/PPPoE	
Servidor web HTTP/HTTPS	
Sincronização de data e hora por SNTP	
UDP/TCP/DNS-SRV(RFC 3263)	
QoS: 802.1p/Q tagging (VLAN), Layer 3 ToS DSCP	
SRTP for voice	

Transport Layer Security (TLS)
Gestão de certificados HTTPS
Cifragem do ficheiro de configuração por AES
Digest authentication com MD5/MD5-sess
OpenVPN, IEEE802.1X
IPv6
LLDP/CDP/DHCP VLAN
Opção para montagem em parede
Modelo de referência: Yealink T48S ou equivalente
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 2 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD
Acesso, sem custos adicionais, às <u>atualizações</u> de software lançadas pelo fabricante para o modelo, pelo mesmo período de tempo proposto pelo concorrente para o item anterior.
<u>3 Módulos de expansão para telefone IP</u> , com as seguintes especificações mínimas:
Módulo de expansão compatível com o telefone IP proposto no ponto anterior
Visor gráfico LCD 160x320 ou superior
Pelo menos 20 teclas físicas, cada uma com indicador luminoso dual
Pelo menos 20 teclas adicionais através de mudança de página
Suporte de pelo menos 2 páginas de teclas programáveis
Teclas de controlo independentes que se utilizam para a comutação rápida das páginas
Luz de fundo no LCD
Diferentes ícones para cada função que se mostra no LCD
Alimentação do módulo via telefone
Suporte de até 6 módulos em cadeia
Modelo de referência: Yealink EXP40 ou equivalente
Assistência técnica, com reposição de peças avariadas ou defeituosas (por peças originais do mesmo fabricante do bem), sem custos adicionais, para um período mínimo de 2 anos após a instalação do bem e com um tempo de resposta do tipo 8x5xNBD

Notas:

- Os equipamentos do presente procedimento pré-contratual requerem instalação, por parte do adjudicatário, nas instalações da Associação AquaValor.
- Qualquer menção a marca específica deve ser entendida como “do tipo”, “ou equivalente”.