Aprovo.

Luís Miguel Pereira dos Santos

Assinado de forma digital por Luís Miguel Pereira dos Santos
DN: c=PT, title=Presidente do Conselho Diretivo do IAVE, ou=Conselho Diretivo, o=Instituto de Avaliação Educativa IP, sn=Pereira dos Santos, givenName=Luís Miguel, cn=Luís Miguel Pereira dos Santos
Dados: 2023.09.20 14:16:14 +01'00'

CONCURSO PÚBLICO COM PUBLICIDADE INTERNACIONAL Nº CPI/02/2023

CADERNO DE ENCARGOS Nº 12/IAVE/2023

Abertura do procedimento de concurso público com publicidade internacional para aquisição e instalação de solução de *networking* e segurança para apoio à elaboração, aplicação, classificação e produção de resultados de provas de avaliação externa em ambiente desmaterializado.

Classificação CPV: 32420000-3 – Equipamento de rede
48820000-2 – Servidores
48730000-4 – Pacote de software de segurança

PARTE I

Cláusulas Jurídicas

Artigo 1º
Objeto do procedimento

1. O objeto do Caderno de encargos do presente procedimento é a aquisição e instalação de:

1.1. **Solução *Wireless***

Pretende-se a evolução da rede wireless atualmente existente no IAVE, I.P. segundo um modelo padronizado e estratificado em camadas lógicas estanques, com responsabilidades e capacidades claramente definidas, e que permitam por um lado otimizar o investimento na rede e por outro garantir uma implementação e manutenção flexível com capacidade de adaptação granular dos conceitos de alto nível aplicados à realidade intrínseca de cada site/camada funcional.

Para tanto, pretende-se a aquisição dos seguintes equipamentos:

Tipo	Descrição	Quantidade
Controladora Wireless	Controlador wireless	1
Access Point	Access Point	30

1.2. Solução *Switching*

Pretende-se a evolução da rede *switching* atualmente existente no IAVE, I.P. segundo um modelo padronizado e estratificado em camadas lógicas estanques, com responsabilidades e capacidades claramente definidas, e que permitam por um lado otimizar o investimento na rede e por outro garantir uma implementação e manutenção flexível com capacidade de

adaptação granular dos conceitos de alto nível aplicados à realidade intrínseca de cada site/camada funcional.

Para tanto, pretende-se a aquisição dos seguintes equipamentos:

Tipo	Descrição	Quantidade
Gestão	Plataforma de Gestão	1
Switch tipo 1	Switch Core	2
Switch tipo 2	Switch de 48 Portas	9
Switch tipo 3	Switch de 48 Portas mGig	5
Transceivers	Multimodo Enterprise Class	26
Transceivers	Singlemodo Enterprise Class	16

1.3. Solução Segurança

Pretende-se a evolução da infraestrutura de segurança atualmente existente no IAVE, I.P. segundo um modelo padronizado e estratificado em camadas lógicas estanques, com responsabilidades e capacidades claramente definidas, e que permitam por um lado otimizar o investimento na rede e por outro permitir uma implementação e manutenção flexível com capacidade de adaptação granular dos conceitos de alto nível aplicados à realidade intrínseca de cada site/camada funcional.

Para tanto, pretende-se a aquisição dos seguintes equipamentos:

Tipo	Descrição	Quantidade
Servidor	Servidor de Suporte à Virtualização	1
Switch	Switch de Perímetro	2
Firewall	Firewall de Perímetro	2
Controlo de acessos	Controlo de acessos	1
MFA	Multi fator de autenticação	500
Analítica	Sonda IOT	1

2. Consideram-se, nomeadamente, abrangidos pelo objeto do presente procedimento a execução de todas as prestações inerentes aos serviços pós-venda, de acordo com as especificações descritas no artigo 23º do presente caderno de encargos.

Artigo 2º

Forma e documentos contratuais

1. O contrato a celebrar integra os seguintes elementos:
   a) O presente caderno de encargos;
   b) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelas entidades convidadas, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;

c) Os esclarecimentos e as retificações relativos ao caderno de encargos;
d) A proposta adjudicada;
e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

2. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem que nele se dispõe, sem prejuízo da aplicação do princípio da prevalência revisto no artigo 51º do Código dos Contratos Públicos, doravante apenas CCP.
3. Em caso de divergência entre os documentos referidos no nº 1 e o clausulado do contrato e seus anexos prevalecem os primeiros, salvo quanto aos ajustamentos propostos, de acordo com o disposto no artigo 99º do CCP e aceites pelo adjudicatário, nos termos do disposto no artigo 101º desse mesmo diploma;
4. Além dos documentos referidos no nº 1, o adjudicatário obriga-se igualmente a respeitar, no que lhe seja aplicável, as normas europeias e portuguesas, as especificações e homologações de organismos oficiais e fabricantes ou entidades detentoras de patentes.

Artigo 3º
Boa-fé

1. As partes obrigam-se a atuar de boa-fé na execução do contrato e a não exercer os direitos nele previstos, ou na lei, de forma abusiva.

Artigo 4º
Local, forma e período de execução do contrato

1. O contrato que vier a ser celebrado vigorará nos termos previstos no seu clausulado, devendo ser executado no período máximo de 60 (sessenta) dias, sem prejuízo do período previsto para assistência técnica.
2. Os bens e serviços objeto do contrato deverão ser disponibilizados nas instalações do Instituto de Avaliação Educativa, sitas na Travessa Terras de Sant'Ana, nº 15, 1250-269 Lisboa.

Artigo 5º
Preço base

1. O preço base, estabelecido de acordo com o artigo 47º do CCP, é de 743.502,82 €, (setecentos e quarenta e três mil, quinhentos e dois euros e oitenta e dois cêntimos), valor ao qual acresce o IVA à taxa legal em vigor.
2. A fixação do presente preço base tem como fundamento a pesquisa preliminar ao mercado, na qual foram consultadas três empresas. O preço base resulta da média do valor dos orçamentos rececionados pelo IAVE, I.P.

Artigo 6º
Condições de pagamento

1. Os pagamentos serão realizados no prazo máximo de 60 (sessenta) dias após a aceitação e verificação, pelo IAVE, I.P. da conformidade dos bens e serviços fornecidos e da receção das respetivas faturas.
2. Não são, em caso algum, concedidos adiantamentos.

3. Em caso de discordância, por parte do IAVE, I.P., quanto aos valores indicados nas faturas, devem ser comunicados ao adjudicatário, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. As faturas devem conter obrigatoriamente o nº de compromisso gerado pela entidade adjudicante, nos termos da lei, bem como descrever o bem e serviço.
5. Desde que regularmente emitidas, e observado o disposto nos números precedentes, as faturas são pagas através de transferência bancária para o IBAN indicado pelo adjudicatário, mediante preenchimento da ficha de fornecedor.

Artigo 7º
Obrigações do adjudicatário

1. São obrigações do adjudicatário, além de outras decorrentes do estabelecido nas peças do presente procedimento e na legislação aplicável, os que seguidamente se enunciam e que devem ser objeto de cláusulas específicas a incluir no contrato a celebrar:
    a. Assegurar a entrega dos bens e a prestação dos serviços conforme definido no presente caderno de encargos e seus anexos, bem como nos demais documentos contratuais;
    b. Comunicar, antecipadamente, ao IAVE, I.P., qualquer facto que torne total ou parcialmente impossível a prestação de qualquer dos serviços objeto do presente procedimento, ou que implique o incumprimento de qualquer outra das suas obrigações;
    c. Alterar as condições subjacentes à prestação de serviço acordada entre as partes, através da celebração de contrato escrito entre as mesmas, apenas com prévia autorização escrita da entidade adjudicante;
    d. Assegurar todos os meios humanos e materiais que se demonstrem necessários e indispensáveis à execução do contrato;
    e. Assegurar, de forma correta e fidedigna, as informações referentes às condições em que a prestação dos bens será executada, disponibilizando todos os esclarecimentos que se justifiquem, no tempo adequado para o efeito, a indicar pelo IAVE, I.P.;
    f. Comunicar qualquer facto ocorrido durante a execução do contrato que se mostre relevante para a normal prestação dos bens e para a execução contratual, nomeadamente, a alteração da denominação social ou dos seus representantes legais.

Artigo 8º
Patentes, licenças e marcas registadas

1. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização de marcas registadas, patentes registadas, licenças ou outros direitos similares.

Artigo 9º
Uso de sinais distintivos

1. Nenhuma das partes pode utilizar a denominação, marcas, nomes comerciais, logótipos e outros sinais distintivos do comércio que pertençam à outra sem o seu prévio consentimento escrito.

Artigo 10º
Sigilo

1. O adjudicatário garantirá o sigilo quanto a quaisquer informações de que venham a ter conhecimento relacionadas com a atividade do IAVE, I.P., em virtude da aquisição dos bens e serviços objeto do presente contrato.
2. Excluem-se do dever de sigilo previsto no número anterior, a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo prestador de bens ou que este seja obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Artigo 11º
Regulamento de Proteção de Dados

1. O adjudicatário obriga-se a cumprir o disposto em todas as disposições legais aplicáveis em matéria de tratamento de dados pessoais, no sentido conferido pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ("Regulamento Geral sobre a Proteção de Dados") e demais legislação comunitária e nacional aplicável, em relação a todos os dados pessoais a que aceda no âmbito ou para efeitos da prestação dos bens, nomeadamente, dados pessoais de clientes, trabalhadores, colaboradores e prestadores de bens do IAVE, I.P.
2. As partes reconhecem e aceitam que, relativamente a todos os dados pessoais a que o adjudicatário tiver acesso ou lhe forem transmitidos pelo IAVE, I.P. para efeitos da prestação dos bens:
    a) O IAVE, I.P. atuará na qualidade de responsável pelo tratamento dos dados (tal como definido no Regulamento Geral sobre a Proteção de Dados), determinando as finalidades e os termos do tratamento desses dados pelo adjudicatário;
    b) O adjudicatário atuará na qualidade de entidade subcontratante (tal como definido no Regulamento Geral sobre a Proteção de Dados), tratando os dados pessoais em estrita observância das instruções do responsável pelo tratamento desses dados;
    c) Entende-se, para este efeito, que tratamento de dados pessoais são as operações, com ou sem recurso a meios automatizados, efetuadas sobre os dados pessoais dos trabalhadores do IAVE, I.P., incluindo a recolha, o registo, a organização, o armazenamento, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a divulgação, a transferência e/ou a disponibilização a terceiros, o alinhamento, a combinação, o bloqueamento, o apagamento e a destruição dos dados suprarreferidos.
3. O adjudicatário compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou, por qualquer outra pessoa, colocar à disposição de terceiros os dados pessoais a que tiver acesso ou lhe forem transmitidos pelo responsável dos tratamentos de dados ao abrigo do presente Contrato, sem que para tal tenha sido expressamente instruído, por escrito, por aquele responsável ou pelos titulares dos dados no exercício dos seus respetivos direitos.
4. Sem prejuízo das demais obrigações previstas no presente Contrato, o adjudicatário obriga-se a cumprir rigorosamente o disposto na legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:
    a) Tratá-los apenas de acordo com as instruções do IAVE, I.P., única e exclusivamente, para efeitos da presente prestação dos bens, cumprindo-se as obrigações estatuídas sobre proteção de dados;

b) Prestar toda a colaboração de que este careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais efetuado ao abrigo do presente Contrato e manter o IAVE, I.P. informado em relação ao tratamento de dados pessoais;
c) Prestar assistência ao IAVE, I.P. , tendo em conta a natureza do tratamento e a informação ao seu dispor, no sentido de assegurar as obrigações referentes à notificação de violações de dados pessoais, designadamente através da comunicação sempre que possível até 72 horas subsequentes ao conhecimento (da ocorrência) de qualquer violação de dados pessoais que ocorra, prestando ainda colaboração ao IAVE, I.P. na adoção de medidas de resposta ao incidente, na investigação do mesmo e na elaboração das notificações que se mostrem necessárias nos termos da lei;
d) Colaborar com o IAVE, I.P. tendo em conta a natureza do tratamento e, na medida do possível adotar as medidas técnicas e organizativas referidas nesta Cláusula, onde se incluem a cifragem ou a pseudonimização aos dados pessoais para reduzir os riscos para os titulares de dados em questão, não excluindo outras eventuais medidas de proteção de dados, e permitindo-se que estas cumpram a sua obrigação de dar resposta aos pedidos dos titulares dos dados, tendo em vista o exercício, por estes, dos seus direitos nos termos da lei;
e) Não comunicar dados pessoais a terceiros e a prestadores de bens não autorizados ou não indicados pelo IAVE, I.P.;
f) Consoante a escolha do IAVE, I.P. ou do titular, eliminar ou devolver os dados pessoais no momento da cessão do Contrato, apagando e destruindo quaisquer cópias existentes, exceto se a conservação ou a transmissão dos dados for exigida por lei;
g) Manter registos das atividades de tratamento de dados realizadas em nome do IAVE, I.P. ao abrigo do presente Contrato, segundo os requisitos previstos na lei;
h) Cumprir todas as demais disposições legais no que respeita ao registo, transmissão ou qualquer outra operação de tratamento de dados pessoais previstas na lei;
i) Não os transferir para fora do Espaço Económico Europeu, sem o consentimento prévio por escrito da responsável pelo tratamento dos dados;
j) Disponibilizar ao responsável pelo tratamento dos dados todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na lei no respetivo âmbito e facilitar e contribuir para as auditorias, inclusive as inspeções conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado;
k) Assegurar que o pessoal autorizado a tratar de dados pessoais assume um compromisso de confidencialidade e que conhece e se compromete a cumprir todas as obrigações aqui previstas.

5. O adjudicatário obriga-se a pôr em prática as medidas técnicas e de organização necessárias à proteção dos dados pessoais tratados por conta do IAVE, I.P. contra a respetiva destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.
6. As medidas a que se refere o número anterior devem garantir um nível de segurança adequado em relação aos riscos que o tratamento de dados apresenta, à natureza dos dados a proteger e aos riscos, de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares.

7. O adjudicatário concorda com o acesso aos dados pessoais tratados ao abrigo do presente Contrato será estritamente limitado ao pessoal que necessitar de ter acesso aos mesmos para efeitos de cumprimento das obrigações aqui assumidas pelo adjudicatário.
8. O adjudicatário obriga-se a comunicar ao responsável pelo tratamento dos dados qualquer situação que possa afetar o tratamento dos dados pessoais ou de algum modo dar origem ao incumprimento das disposições legais em matéria de proteção de dados, devendo ainda tomar todas as medidas necessárias e ao seu alcance para a fazer cessar de imediato.

9. O adjudicatário será responsável por qualquer prejuízo em que o IAVE, I.P. vier a incorrer em consequência do tratamento, por si ou pelo seu pessoal, de dados pessoais ou em violação das normas legais aplicáveis e ao disposto no presente Contrato, quando tal violação seja imputável ao adjudicatário e solidária com o pessoal no âmbito do serviço prestado, quando a violação seja imputável à atuação destes últimos.
10. O adjudicatário, sempre que o IAVE, I.P. receber um pedido de acesso ou retificação de dados pessoais ou uma oposição ao seu tratamento por parte dos seus titulares dos dados, deverá prestar assistência ao responsável pelo tratamento dos dados através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares, tendo em vista o exercício dos seus direitos legais.

Artigo 12º
Alterações ao contrato

1. O contrato pode ser alterado, de acordo com os artigos 311º e 312º, ambos do CCP, nomeadamente, por:
   a) Acordo das partes, que não pode revestir forma menos solene do que a do contrato;
   b) Alteração anormal e imprevisível das circunstâncias em que as partes tenham fundado a decisão de contratar, desde que a exigência das obrigações por si assumidas afete gravemente os princípios da boa-fé e não esteja coberta pelos riscos próprios do contrato;
   c) Razões de interesse público decorrentes de necessidades novas ou de uma nova ponderação das circunstâncias existentes, sem prejuízo das indeminizações a que houver lugar, nos termos da lei.

Artigo 13º
Cessão da posição contratual

1. O adjudicatário não poderá ceder a sua posição contratual sem autorização prévia do IAVE, I.P.
2. O adjudicatário será autorizado a recorrer à subcontratação de um terceiro para colaboração na prestação dos bens, desde que se assegure que o mesmo cumprirá o disposto na legislação aplicável, devendo tal obrigação constar de contrato escrito que, para o efeito, se obriga a celebrar com esse terceiro em que este se vincula ao cumprimento das obrigações decorrentes do Regulamento (UE) 2016/679 e demais legislação aplicável relativa a Dados Pessoais, vinculando suas ações à essência, natureza e finalidades da presente disposição contratual, no estrito cumprimento do dever de sigilo e de confidencialidade.
3. Para efeitos da autorização prevista no número anterior, deve ser apresentada pelo cessionário toda a documentação exigida ao adjudicatário no presente procedimento, para verificação pelo IAVE, I.P. de que o cessionário não se encontra em nenhuma das situações previstas no artigo

55.º do CCP e que a cessão não altera as circunstâncias do cumprimento das obrigações contratuais e legais.

Artigo 14º
Resolução do Contrato

1. O incumprimento por uma das partes dos deveres resultantes do contrato confere, nos termos previstos no regime jurídico aplicável, à outra parte, o direito a resolver o contrato, sem prejuízo das correspondentes indemnizações legais e dos demais fundamentos gerais de resolução do contrato legalmente previstos.
2. Para efeitos do disposto no número anterior, considera-se existir incumprimento definitivo quando houver atraso na prestação por período superior a 10 dias úteis, decorrido após interpelação admonitória, que fixe um prazo para cumprimento, nunca inferior a dez dias.
3. A resolução será efetuada mediante aviso prévio, através de carta registada com aviso de receção, enviada com a antecedência mínima de 10 dias úteis, contados a partir da data do que se considera ser o incumprimento de definitivo, previsto no número anterior, deste mesmo artigo.
4. A resolução do contrato não prejudica a aplicação de quaisquer sanções pecuniárias, nos termos do artigo seguinte.

Artigo 15º
Penalidades

1. No caso de não cumprimento das obrigações contratuais, a entidade adjudicante pode aplicar ao adjudicatário as seguintes sanções contratuais pecuniárias, em função da gravidade ou reiteração da infração:
    a) Pelo incumprimento das obrigações relativas ao dever de confidencialidade, até 1000,00€ (mil euros), por infração;
    b) Pelo incumprimento das obrigações relativas à propriedade intelectual e dados pessoais, até 1000,00€ (mil euros), por infração;
    c) Pelo incumprimento dos deveres de informação até 250,00€ (duzentos e cinquenta euros), por infração;
    d) Pelo incumprimento da determinação que seja dirigida ao adjudicatário nos termos do presente caderno de encargos, nas quais se incluem as obrigações previstas na Cláusula 1ª, até 250,00€ (duzentos e cinquenta euros), por infração;
    e) Pelo incumprimento das obrigações acima elencadas, poderão ser aplicadas as referidas penalidades, não excedendo os 20% ou 30% do montante total adjudicado, consoante os casos e, de acordo com o previsto no artigo 329.º do Código dos Contratos Públicos.
2. O pagamento das eventuais penalidades em que o adjudicatário incorra será deduzido do valor líquido da faturação do segundo outorgante.
3. A aplicação das penalidades previstas na presente cláusula será objeto de audiência prévia, nos termos previstos no nº 2 do artigo 308.º do Código dos Contratos Públicos.
4. O adjudicatário será notificado, por escrito, para que no prazo de 10 (dez) dias úteis se pronuncie. Caso o adjudicatário não se pronuncie no prazo concedido, a entidade adjudicante aplica a penalidade de acordo com o nº 2 da presente Cláusula.

Artigo 16º

Mora da entidade adjudicante

1. O atraso em qualquer pagamento não determina o vencimento das restantes obrigações de pagamento.
2. Em caso de mora, os pagamentos devidos pela entidade adjudicante vencem juros, à taxa legal, desde a data em que se tornaram exigíveis e até integral pagamento, nos termos do artigo 326.º do Código dos Contratos Públicos.
3. Em caso de desacordo sobre o montante devido, deve o contraente público efetuar o pagamento sobre a importância em que existe concordância do cocontratante.
4. Os valores contestados pela entidade adjudicante e que vierem a ser objeto de correção não vencem juros de mora em caso de não pagamento.

Artigo 17º

Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, for impedida de cumprir as obrigações assumidas no contrato, 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) Greves ou conflitos laborais limitados às sociedades da segunda outorgante ou a grupos de sociedades em que esta se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
   b) Circunstâncias que não constituam força maior para os subcontratados do segundo outorgante, na parte em que intervenham;
   c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo segundo outorgante de deveres ou ónus que sobre ela recaiam;
   d) Manifestações populares resultantes do incumprimento, pelo segundo outorgante, de normas legais;
   e) Incêndios ou inundações com origem nas instalações do segundo outorgante 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 segundo outorgante não devidas a sabotagem;
   g) Eventos que estejam ou devam estar cobertos por seguros.

4. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar de imediato tais situações à outra parte, por qualquer meio escrito, bem como informar o prazo previsível para restabelecer a situação.
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.

Artigo 18º

Contagem dos prazos na fase de execução do contrato

1. À contagem de prazos na fase de execução do contrato a celebrar na sequência do presente procedimento, são aplicáveis as seguintes regras:
   a) Os prazos são contínuos, não se suspendendo nos sábados, domingos e feriados;
   b) O prazo que termine em sábado, domingo, feriado ou em dia em que o serviço, perante o qual deva ser praticado o ato, não esteja aberto ao público, ou não funcione durante o período normal, transfere-se para o 1.º dia útil seguinte.

Artigo 19º

Celebração do contrato escrito

1. De acordo com o disposto nº 1 do artigo 94º do Código dos Contratos Públicos o contrato será reduzido a escrito.

Artigo 20º

Comunicações e notificações

1. Todas as notificações e comunicações entre a entidade adjudicante e a entidade adjudicatária deverão ser efetuadas por escrito, através de correio, correio eletrónico ou de telecópia, para o domicílio ou sede contratual de cada uma, identificado no contrato, com suficiente clareza, para que o destinatário fique ciente da respetiva natureza e conteúdo.
2. Qualquer alteração das informações de contacto constantes do contrato, mesmo que pontuais ou temporárias, devem ser comunicadas de imediato e por escrito à outra parte.

Artigo 21º

Fundamentação da decisão do procedimento

1. O presente procedimento concurso público é adotado nos termos do disposto na alínea a) do artigo 20º e artigo 130º e seguintes do CCP e a decisão de contratar foi tomada pelo Presidente do Conselho Diretivo Luís Pereira dos Santos.

Artigo 22º

Foro competente

1. Em tudo o que o presente caderno de encargos for omisso observar-se-á o disposto no CCP, e demais legislação e regulamentação aplicável.
2. Para o conhecimento de quaisquer litígios emergentes do contrato, designadamente relativas à respetiva interpretação, execução, incumprimento, invalidade, resolução ou redução, é competente o foro da comarca de Lisboa.

Parte II

Cláusulas técnicas

Artigo 23º
Especificações técnicas dos equipamentos

1. As especificações técnicas dos equipamentos objeto do presente caderno de encargos, estão descriminadas de acordo com o infra previsto:

1.1. Solução Wireless

Deverá ser assegurada compatibilidade total entre os equipamentos e software a fornecer no presente procedimento.
A solução a propor deverá incluir fichas e cablagem necessárias para a ligação de todos os equipamentos de acordo com as melhores práticas.

A solução a adquirir assenta nos seguintes pressupostos:

- Distinção e controlo entre cliente interno (Corp) e cliente externo (GUEST).
- Visibilidade sobre acessos a recursos de rede.

1.1.1. Equipamentos e software a adquirir

É pretendida a aquisição dos seguintes equipamentos

Tipo	Descrição	Quantidade
Controladora Wireless	Controlador wireless	1
Access Point	Access Point	30

1.1.1.1. Controlador Wireless

A controladora wireless a adquirir tem como objetivo fornecer redundância à controladora existente por forma a permitir alta-disponibilidade na solução através de um cluster e eliminando qualquer *single point of failure*

De acordo com os seguintes requisitos:

REQ	Requisito
1	A controladora deverá ser suportada em ambientes de IaaS na plataforma de *cloud* pública da Google e da AWS, sendo disponibilizadas via o Marketplace respetivo. A controladora deverá estar certificada para ambientes de *GovCloud* da AWS
2	Em ambientes de *cloud* privada deverá ser possível implementar a controladora nos seguintes hipervisores:
3	*VMware ESXI*
4	*Microsoft Hyper-V*
5	*KVM*

6	Deverá suportar topologias centralizadas para tráfego de controlo e tráfego de utilizadores
7	Deverá suportar topologias centralizadas para tráfego de controlo e topologia local para tráfego de utilizadores.
Capacidade	
8	Número máximo de pontos de acesso - 6.000 por controladora
9	Número máximo de clientes - 64000 por controladora
10	Taxa de transferência máxima 5 Gbps em modo de central *swithing*
11	Máximo de WLANs - 4096
12	VLANs máximas - 4096
13	Topologias de Alta Disponibilidade
14	IPv6
Normas Wireless	
15	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 Wave 1 and Wave 2, 802.11ax
Normas Wired, Switching e Routing	
16	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation
Normas de Dados	
17	RFC 768 User Datagram Protocol (UDP)
18	RFC 791 IP
19	RFC 2460 IPv6
20	RFC 792 Internet Control Message Protocol (ICMP)
21	RFC 793 TCP
22	RFC 826 Address Resolution Protocol (ARP)
23	RFC 1122 Requirements for Internet Hosts
24	RFC 1519 Classless Interdomain Routing (CIDR)
25	RFC 1542 Bootstrap Protocol (BOOTP)
26	RFC 2131 Dynamic Host Configuration Protocol (DHCP)
27	RFC 5415 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol
28	RFC 5416 CAPWAP Binding for 802.11
Normas de Segurança	
29	Wi-Fi Protected Access (WPA)
30	IEEE 802.11i (WPA2, RSN)
31	Wi-Fi Protected Access 3 (WPA3)
32	RFC 1321 MD5 Message-Digest Algorithm
33	RFC 1851 Encapsulating Security Payload (ESP) Triple DES (3DES) Transform
34	RFC 2104 HMAC: Keyed-Hashing for Message Authentication
35	RFC 2246 TLS Protocol Version 1.0
36	RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile
37	RFC 4347 Datagram Transport Layer Security (DTLS)
38	RFC 5246 TLS Protocol Version 1.2
Normas de Encriptação	
39	Static Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits
40	Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with CBC Message Authentication Code Protocol (CCMP)
41	Data Encryption Standard (DES): DES-CBC, 3DES

42	Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit
43	DTLS: AES-CBC
44	IPsec: DES-CBC, 3DES, AES-CBC
45	802.1AE MACsec encryption
Normas de Authentication, Authorization e Accounting (AAA)	
46	IEEE 802.1X
47	RFC 2548 Microsoft Vendor-Specific RADIUS Attributes
48	RFC 2716 Point-to-Point Protocol (PPP) Extensible Authentication Protocol (EAP)-TLS
49	RFC 2865 RADIUS Authentication
50	RFC 2866 RADIUS Accounting
51	RFC 2867 RADIUS Tunnel Accounting
52	RFC 2869 RADIUS Extensions
53	RFC 3576 Dynamic Authorization Extensions to RADIUS
54	RFC 5176 Dynamic Authorization Extensions to RADIUS
55	RFC 3579 RADIUS Support for EAP
56	RFC 3580 IEEE 802.1X RADIUS Guidelines
57	RFC 3748 Extensible Authentication Protocol (EAP)
58	TACACS support for management users
Normas de Gestão	
59	Simple Network Management Protocol (SNMP) v1, v2c, v3
60	RFC 854 Telnet
61	RFC 1155 Management Information for TCP/IP-based Internets
62	RFC 1156 MIB
63	RFC 1157 SNMP
64	RFC 1213 SNMP MIB II
65	RFC 1350 Trivial File Transfer Protocol (TFTP)
66	RFC 1643 Ethernet MIB
67	RFC 2030 Simple Network Time Protocol (SNTP)
68	RFC 2616 HTTP
69	RFC 2665 Ethernet-Like Interface Types MIB
70	RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions
71	RFC 2819 Remote Monitoring (RMON) MIB
72	RFC 2863 Interfaces Group MIB
73	RFC 3164 Syslog
74	RFC 3414 User-Based Security Model (USM) for SNMPv3
75	RFC 3418 MIB for SNMP
76	RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs
77	RFC 4741 Base NETCONF protocol
78	RFC 4742 NETCONF over SSH
79	RFC 6241 NETCONF
80	RFC 6242 NETCONF over SSH
81	RFC 5277 NETCONF event notifications
82	RFC 5717 Partial Lock Remote Procedure Call
83	RFC 6243 With-Defaults capability for NETCONF
84	RFC 6020 YANG
Interfaces de Gestão	

85	Web-based: HTTP/HTTPS
86	Command-line interface: Telnet, Secure Shell (SSH) Protocol,
87	SNMP
88	NETCONF
Radio Frequência	
89	O controlador deverá suportar vários perfis de gestão de RF por grupo de APs, incluindo controle de potência de transmissão e atribuição de canal dinâmico em 2,4 GHz e 5 GHz
90	O controlador deverá identificar e evitar interferências com relatório de análise de impacto de desempenho da rede
91	O controlador deverá suportar seleção de largura de canal automática otimizada (20 ~ 160Mhz) em 5 GHz, 802.11ac
92	Capacidade de ativar / desativar recursos 11ax por WLAN
93	Deverá suportar SSID's por rádio em Dual 5G
Controlo de Reconhecimento de Aplicações	
94	O controlador deverá suportar o reconhecimento de aplicações por utilizador e por WLAN e controle de largura de banda
95	A tecnologia de reconhecimento de aplicações do controlador deverá suportar a exportação para formatos compatíveis com terceiros, como NetFlow v9
96	O controlador deverá suportar novas assinaturas de aplicações sem atualizar o software do controlador
Software	
97	O Ponto de Acesso deve distribuir proactivamente a ligação do cliente antes e depois da associação e analisar a condição do utilizador em tempo real usando pacote de dados RSSI
98	O controlador deve suportar a securização de dados de controlo e de data com CAPWAP
99	O controlador deve suportar roaming sem fios entre controladores
100	O controlador deve manter estatísticas de utilização por aplicação por utilizador e deve ser capaz de exportar para análise de rede.
101	O controlador deve suportar opções de vários idiomas de gestão de GUI embutido
102	O controlador deve fornecer o estado da qualidade de ligação por cliente
103	Visibilidade de clientes com endereços MAC aleatórios
Alta Disponibilidade	
104	O modo de alta disponibilidade deve permitir a instalação geograficamente dispersa entre os controladores
105	O failover do controlador não deve desencadear a desautenticação e reassociação do cliente
106	O intervalo de keepalives não deve ser superior a 100 mseg
107	O controlador deverá suportar patching de software na WLC, sem necessidade de reload, para corrigir bugs
108	O controlador deverá suportar patching de software de AP, sem necessidade de reload, para corrigir bugs
109	O controlador deverá suportar novo hardware de AP sem a necessidade de atualizar todo o software do controlador.
110	O controlador redundante deve sincronizar o ponto de acesso e o status do cliente, incluindo o status de concessão de IP DHCP dos clientes.
BYOD & Segurança	

111	O controlador deverá ser capaz de incorporar uma página de portal da web personalizada (HTML) para personalizar totalmente a experiência do utilizador
112	O controlador deverá fornecer uma classificação de ap's rogue baseada em regras e executar ações de mitigação.
113	O controlador deverá ser capaz de detetar a ligações do dispositivo do utilizador ao Ponto de Acesso Rogue e contê-la
114	O controlador deverá suportar a segurança de conteúdo usando a integração DNS, a classificação da Web deve ser totalmente personalizável
115	O sistema deverá suportar criptografia de plano de controle em IPv4 e IPv6
116	A atualização da imagem do Controlador deve ser feita por meio de transporte criptografado seguro
117	O controlador deve ser capaz de fornecer chaves pré-compartilhadas exclusivas para os dispositivos que não suportam o protocolo de segurança 802.1x
118	O controlador deve fornecer certificação FIPS-140 / CC, incluindo certificação pendente
119	O controlador deverá suportar Identidade PSK
120	O controlador deverá poder desativar clientes com endereço MAC aleatório
Configuração da Rede	
121	O controlador deverá suportar o mapeamento de VLANs específicas para SSID único, dependendo da localização do ponto de acesso e do usuário
122	O controlador deverá suportar a atribuição automática de VLAN por SSID para a ligação do utilizador com equilíbrio de carga.
123	O controlador deverá suportar a fragmentação dos pacotes entre o ponto de acesso e a comunicação com o controlador
QOS/Voice/Video	
124	O ponto de acesso deverá ser capaz de suportar roaming rápido baseado em 802.11r e dispositivos WPA2 genéricos sob o mesmo SSID
125	O controlador deverá ser capaz de priorizar a chamada Skype4Business com uma política de priorização de aplicativos por utilizador.
126	O ponto de acesso deverá adiar o scan de canais mediante atividade de tráfego de alta prioridade
127	O ponto de acesso deverá ser compatível com o controle de admissão de chamadas baseado na largura de banda
128	O controlador deverá fornecer opções para escolher uma classificação de QoS confiável de várias fontes (DSCP, UP) e manter a classificação de prioridade sobre a rede.

1.1.1.2. Pontos de acesso

Requisitos pretendidos:

REQ	Requisito
Interfaces	
1	1x 100, 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz
2	Management console port (RJ-45)
Arquitetura	
3	Gestão em controladora centralizada
4	Gestão local e independente

5	Controladora embebida para gestão de outros pontos de acesso
6	50 access points, 1000 clients
Capacidade	
7	Número máximo de pontos de acesso - 6.000 por controladora
8	Número máximo de clientes - 64000 por controladora
9	Taxa de transferência máxima - 5 Gbps em modo de central swithing
10	Máximo de WLANs 4096
11	VLANs máximas 4096
12	Topologias de Alta Disponibilidade
13	IPv6
Normas 802.1n versão 2.0	
14	4x4 MIMO with four spatial streams
15	Maximal Ratio Combining (MRC)
16	802.11n and 802.11a/g beamforming
17	20- and 40-MHz channels
18	PHY data rates up to 890 Mbps (40 MHz with 5 GHz and 20 MHz with 2.4 GHz)
19	Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive)
20	802.11 Dynamic Frequency Selection (DFS)
21	Cyclic Shift Diversity (CSD) support
Normas 802.1ax	
22	4x4 MIMO with four spatial streams:
23	4x4:4 on 5 GHz with MU-MIMO and downlink/uplink OFDMA
24	4x4:4 on 2.4 GHz with MU-MIMO and downlink/uplink OFDMA
25	Combined data rate of 5.2 Gbps
26	Built-in BLE radio (Bluetooth 5.0)
27	Supports up to 500 Wi-Fi devices
28	Uplink/downlink OFDMA
29	TWT
30	BSS coloring
31	MRC
32	802.11ax beamforming
33	20-, 40-, 80-, and 160-MHz channels
34	PHY data rates up to 5.38 Gbps (160 MHz with 5 GHz and 20 MHz with 2.4 GHz)
35	Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive)
36	802.11 DFS
37	CSD support
38	WPA3 support
Funcionalidades	
39	O ponto de acesso deve ter capacidade de suporte para protocolo VXLAN
40	O ponto de acesso deve estar pronto para IoT (BLE)

1.2. Solução Switching

Deverá ser assegurada compatibilidade total entre os equipamentos e software a fornecer no presente procedimento, incluindo os *transceivers*.

A solução a adquirir assenta nos seguintes pressupostos:

- Funcionalidades Layer2/3
- Uplinks a 10G/25G
- Downlinks mGig
- Suportar stack
- 48 portas PoE+

1.2.1. Equipamentos e software a adquirir

É pretendida a aquisição dos seguintes equipamentos

Tipo	Descrição	Quantidade
Gestão	Plataforma de Gestão	1
Switch tipo 1	Switch Core	2
Switch tipo 2	Switch de 48 Portas	9
Switch tipo 3	Switch de 48 Portas mGig	5
Transceivers	Multimodo Enterprise Class	26
Transceivers	Singlemodo Enterprise Class	16

1.2.1.1. Plataforma de Gestão

Deverá ser fornecido um sistema de gestão único que permita a gestão centralizada de elementos de rede, tendo capacidade para gestão de switches, routers, pontos de acesso sem fios, controladores wireless.

O sistema de gestão deverá permitir instalação em ambiente virtualizado Vmware ESXi e Hyper-V.
Juntamente com a plataforma deverá ser fornecido o licenciamento necessário para os equipamentos a fornecer (switches, routers, pontos de acesso sem fios, controladores wireless).

O sistema deverá ter capacidade de suportar as seguintes funcionalidades:

REQ	Requisito
Funcionalidades	
1	Documentar a rede e as suas alterações;
2	Aplicar modificações globais a equipamentos;
3	Fazer backup de configurações de maneira automática e regular, possibilitando:
4	Visualização do histórico das configurações;
5	Comparação entre configurações em diferentes pontos no tempo;
6	Comparação de configurações entre equipamentos;
7	Rollback de configurações para configurações previamente guardadas.
8	Fazer backup de imagens de software de elementos de rede possibilitando:
9	Transferência de imagens de software de/para elementos de rede;
10	Ativação das imagens de software nos elementos de rede.
11	Visualização de inventário de rede;
12	Auditoria à rede;
13	Monitorizar falhas e alarmes;
14	Aviso por email para categorias de falhas e alarmes;
15	Suporte de domínios virtuais de gestão com gestão de acessos a diferentes utilizadores
16	Monitorizar a performance de rede;
17	Interface gráfica intuitiva web-based;
18	Visualização da topologia de rede possibilitando:
19	Deteção automática de links através de LLDP;
20	Apresentação de alarmes ativos nos elementos de rede;
21	Suporte de vistas diferenciadas por localização e com identificação do tipo de devices e número de devices por localização;
22	Aceder diretamente ao elemento por telnet/SSH;
23	Fazer pings e traceroutes;
24	Visualização de mapas baseados no número de saltos de distância de um elemento.
25	Suporte de dashboards contextuais, permitindo obter rapidamente informação sobre:
26	Número de elementos geridos;
27	Tipo de elementos geridos (router, switch, access point, servidor, etc);
28	Alarmística de falhas e correlação de eventos;
29	Estado dos interfaces (Up/Down) e sua taxa de utilização;
30	Utilização de interfaces, CPU, memória, uptime, versões de software;
31	Número de clientes wireless ligados por access point;
32	Número de clientes wired e wireless ligados à rede e detalhes sobre os mesmos (IP, Mac Address, VLAN, elemento/porta/AP a que o cliente se encontra ligado);
33	Top clientes em termos de utilização de largura de banda;
34	Aplicações mais usadas na rede ao nível L7 (gmail, office365, skype, etc);
35	Aplicações mais usadas por site, equipamento, interface e utilizador;
36	Top clientes em termos de utilização de largura de banda por aplicação ao nível do L7;
37	Suporte a templates de configuração de elementos de rede. Os templates deverão poder ser aplicados a vários elementos de rede simultaneamente;

38	Inclusão de base de templates de configuração para:
39	802.1X
40	Access-Lists
41	Configuração de Interfaces
42	Configuração de LACP
43	Configuração de VLANs
44	Configuração de Logging, SNMP, NTP, DNS
45	Configuração de Radius, TACACS+
46	Configuração de Spanning-Tree
47	Configuração de protocolos de routing
48	Configuração de VPNs
49	Configuração de exportação de fluxos (Netflow ou similares)
50	Configuração de QoS
51	Configuração de Visibilidade Aplicacional L7 (gmail, office365, skype, etc)
52	Suporte à criação de "jobs" com tarefas de implementação de alterações na configuração de elementos de rede. Este "jobs" poderão estar definidos para serem executados num determinado momento futuro (dia/hora);
53	Suporte para efetuar diretamente na plataforma de gestão um packet capture, que permite ter a funcionalidade de "snifer" à rede em tempo real;
54	Suporte de configuração de controladores wireless;
55	Suporte de configuração de alta disponibilidade em controladores wireless;
56	Suporte à configuração de equipamentos que tenham integração LAN e WLAN de forma unificada, permitindo gerir a configuração da componente de switching e Wireless numa entidade única
57	Suporte de configuração de access-point em modo standalone e baseados em controlador;
58	Suportar a identificação dos seguintes parâmetros para endpoints em ambientes wireless:
59	MAC address;
60	IP address (IPv4 e IPv6);
61	VLAN
62	Tipo de autenticação;
63	Vendor;
64	Localização do endpoint;
65	Nome do access point;
66	Nome do controlador wireless associado;
67	Suportar a identificação/estatísticas dos seguintes parâmetros em ambiente wireless:
68	RSSI (histórico);
69	Pacotes e bytes Tx/Rx;
70	Estatísticas de qualidade do ar em 802.11 a/b/g/n/ac;
71	Identificação do número de clientes em cada rádio: 2.4GHz e 5GHz;
72	Histórico das associações por access points;
73	Duração das associações;
74	SSID;
75	Troubleshooting dos passos de associação:
76	Associação 802.11;
77	Autenticação 802.1X;
78	Atribuição de endereçamento;

79	Resultado final associação.
80	Identificação de “Rogue APs” e interferências, nomeadamente Bluetooth;
81	Em ambiente wireless, suporte para a integração com sistemas que permitam fazer o “tracking” da localização dos endpoints;
82	Suporte à inclusão de plantas de edifícios possibilitando:
83	Visualização da localização dos access points e endpoints;
84	Visualização da cobertura wireless prevista (heat maps);
85	Otimização da cobertura wireless através da simulação de adição/remoção de access points e obstáculos.
86	Suporte da definição de vários perfis de administração da plataforma de gestão, permitindo ter privilégios diferentes de acesso aos ativos de rede;
87	Suporte à integração com sistemas LDAP e sistemas de controlo de acessos;
88	Suporte à integração de equipamentos de diferentes “Vendors”.

1.2.1.2. Switch tipo 1

Abaixo encontram-se os requisitos pretendidos.

REQ	Requisito
Características Físicas	
1	Equipamento fixo ethernet L2/L3
2	Dimensões: 1RU
3	12 x portas 1/10/25G SFP28
4	Suporte dos seguintes óticos do tipo SFP+:
5	Suporte dos seguintes óticos do tipo SFP:
6	O equipamento deve ter a capacidade de suportar os seguintes módulos:
7	8 x Portas Multigigabit (1/2,5/5,10G)
8	8 x Portas SFP28 (1/10/25G)
9	2 x Portas 40/100G
10	Suporte de flash com um mínimo de 16GB para guardar configurações e logs
11	Capacidade de suporte de Fontes de Alimentação DC e AC
12	Capacidade de suporte de storage externo de até 240G SSD
13	Suporte de stacking através de módulo dedicado, garantindo capacidade para que uns mínimos de 8 equipamentos sejam geridos como um único, através de um endereço único de gestão;
14	A arquitetura do equipamento e da stack tem de ser igual entre os elementos do stack
15	Suportar stacking entre equipamentos com diferentes densidades de portas de acesso, com e sem PoE
16	Suporte para partilha do power entre elementos do stack
17	Suporte de Stateful switchover, quando comuta de activo para standby numa stack
18	Suporte para fontes de alimentação redundantes e hot-swappable (incluídas)
19	Suporte para fans redundantes e hot-swappable
20	Suporte de RFID embebido no equipamento para gestão de activos
21	Suporte de 128 Port-Channles com suporte de até 16 membros por port-channel
22	Suporte de Blue Beacon para identificação do switch
Escalabilidade e Performance	

23	Capacidade de switching mínima: 1T Gbps
24	Capacidade de forwarding mínima:744.0 Mpps
25	Capacidade de stack bandwidth throughput mínimo de 1Tbps
26	Número mínimo de VLAN ID's: 4094
27	Número mínimo de SVIs: 1000
28	Número mínimo de router ports por stack : 448
29	Número mínimo de MAC Addresses: 32000
30	Número mínimo de rotas IPv4: 39000
31	Número mínimo de rotas IPv6: 19500
32	Número mínimo de entradas ACL: 5000
33	Instancias de MST : 64
34	Instancias de (RSTP/PVSTP) : 256
35	Suporte de Jumbo Frames
36	Suporte de um mínimo de 16MB de buffers
37	Suporte de até 64.000 fluxos de rede em hardware. E com capacidade de através de fluxos:
38	Identificar os Top Talkers
39	Customizar fluxos por perfil de user
40	Utilizar multiplos collectors
41	Exportar o consumo de bandwith, em função do número de fluxos
42	Exportar informação de fluxos em netflow v9 ou IPFIX
Funcionalidades	
43	Suporte para LLDP
44	Suporte de LACP - 802.3ad
45	Suporte de gestão WEB
46	Suporte de LACP através de diferentes membros da stack
47	Suporte para IPv6 em Hardware
48	Suporte para 8 egress queues por porta
49	Suporte de 802.1ad (QINQ)
50	Suporte de selective QINQ ou Vlan Mapping
51	Suporte de ACLs
52	Suporte de STP, RSTP
53	Suporte de VRRP
54	Suporte de HQoS, WRED, CBWFQ
55	Suporte de MACSec (802.1AE) com encriptação 128 bits em todas as interfaces
56	Suporte de MACSec (802.1AE) com encriptação 256 bits em todas as interfaces
57	Capacidade de suporte de Suporte de IP SLA
58	Suporte de NAT e PAT
59	Suporte de IPSEC, com suporte de até 100G de performance em hardware
60	Suporte de IP SLA Responder
61	Suporte de rotas estáticas IPv4 e IPv6
62	Suporte de RIPv1, RIPv2, RIPnG
63	Suporte de OSPFv2 e OSPFv3
64	Suporte de inter-vlan routing
65	Suporte de Suporte de BGP e IS-IS
66	Suporte de PBR
67	Suporte de tuneis GRE
68	Suporte de EoMPLS sobre tuneis GRE
69	Suporte de PBR com visibilidade de VRF's

70	Suporte de Suporte de MPLS Layer 3 VPNs
71	Suporte de Suporte de MPLS Layer 2 VPNs
72	Suporte de Suporte de MPLS Multicast VPN
73	Suporte de Suporte de VRF-Lite
74	Suporte de BGP EVPN sobre VXLAN
75	Suporte de Suporte de VXLAN
76	Suporte de NETCONF/YANG e RESTCONF
77	Suporte para hosting de aplicações third party em containers diretamente no switch
78	Suporte de Python
79	Suporte de Suporte de patching para correção de bugs sem necessidade de instalar novas imagens de software
80	Suporte de Port Mirroring e envio de tráfego monitorizado para equipamento remoto através de uma rede L3
81	Suporte para captura de fluxos de tráfego em formato IPFIX ou similares em hardware e sem recurso a sampling de pacotes
82	Suporte de deteção de fluxos ao nível aplicacional - Layer L7. Exemplos de aplicações: facebook, skype, yahoo, http, https/ssl, youtube
83	Suporte de aplicação de políticas de QoS ao nível aplicacional - Layer 7. Exemplos de aplicações: facebook, skype, yahoo, http, https/ssl, youtube
84	Suporte de VLAN ACLSs
85	Suporte de Port Based ACLs
86	Suporte para DAI(Dynamic ARP inspection)
87	Suporte para Port security
88	Suporte para 802.1X
89	Suporte para 802.1X com Change of Authorization
90	Suporte para 802.1X com downloadable ACLs
91	Suporte para 802.1X com guest VLAN
92	Suporte para web authentication para clientes não 802.1X
93	Suporte para RADIUS Authentication, Authorization e Accounting
94	Suporte para TACACS Authentication, Authorization e Accounting
95	Suporte IGMP
96	Suporte de PIM Stub,
97	Suporte de PIM-BIDIR, DM, SM e PIM SSM
98	Suporte de SSHv2
99	Suporte de SNMPv3 e Syslogs
100	Suporte de identificação de malware em tráfego encriptado
101	Suporte de funcionalidades de segurança para defesa da integridade do hardware e software do switch, nomeadamente:
102	Assinatura de imagens para garantir a autenticidade da imagem de software
103	Boot seguro do switch assente em chip de hardware imutável (IEEE 802.1AR)

1.2.1.3. Switch Tipo 2

Abaixo encontram-se os requisitos pretendidos.

REQ	Requisito

Características Físicas	
1	Equipamento fixo ethernet L2/L3
2	Dimensões: 1RU
3	48 portas 1G com interface do tipo RJ-45;
4	Suportar 48 portas PoE 15.4 W (IEEE 802.3af) ou 24 portas PoE+ 30 W (IEEE 802.3at) sem recorrer a power externo (ex: RPS), e apenas com uma power supply no equipamento;
5	Suportar 48 portas PoE+30W(IEEE 802.3at) com a adição de power redundante
6	O equipamento deverá ter de base um uplink com um mínimo de 4 portas line rate 10G SFP+;
7	Suporte dos seguintes óticos do tipo SFP+ (em módulo uplink):
8	10G Base SR, 10G Base LR, 10G Base ER, 10G Base ZR
9	Suporte dos seguintes óticos do tipo SFP (em módulo uplink):
10	1000Base T, 1000Base SX, 1000Base LX/LH, 1000Base EX, 1000Base ZX
11	Suporte de flash com um mínimo de 4GB para guardar configurações e logs;
12	Capacidade de suporte de stacking através de módulo dedicado, garantindo capacidade para que um mínimo de 8 equipamentos sejam geridos como um único, através de um endereço único de gestão;
13	Capacidade de suporte de stacking através de módulo dedicado (não são permitidos equipamentos que utilizem o uplink para fazer stacking)
14	A arquitetura do equipamento e da stack tem de ser igual entre os elementos do stack
15	Capacidade de suportar stacking entre equipamentos com diferentes densidades de portas de acesso, com e sem PoE
16	Capacidade de suporte de Stateful switchover, quando comuta de ativo para standby numa stack
17	Capacidade de suporte para fontes de alimentação redundantes e hot-swappable
18	Capacidade de suporte para fans redundantes
19	Suporte de RFID embebido no equipamento para gestão de ativos
20	Suporte de Blue Beacon para identificação do switch
21	MTBF Mínimo: 346.200 horas
Escalabilidade e Performance	
22	Capacidade de switching mínima: 176 Gbps
23	Capacidade de forwarding mínima: 130Mpps
24	Capacidade de stack bandwidth throughput mínimo de 80 Gbps
25	Número mínimo de VLAN ID's: 4096
26	Número mínimo de SVIs: 512
27	Número mínimo de MAC Addresses: 16000
28	Número mínimo de rotas IPv4: 3000
29	Número mínimo de rotas IPv6: 1500
30	Número mínimo de entradas ACL: 1500
31	Suporte de 6M Buffers
32	Instâncias de MST: 64
33	Instancias de (RSTP/PVSTP) : 128
34	Suporte de Jumbo Frames: 9198 Bytes
35	Número mínimo de entradas multicast routing : 1000
Funcionalidades	
36	Suporte para LLDP
37	Suporte de Gestão WEB(HTTPS) Embutida no Equipamento

38	Suporte de LACP - 802.3ad
39	Suporte de LACP através de diferentes membros da stack
40	Suporte para IPv6 em Hardware
41	Suporte de POE Perpétuo nas Interfaces
42	Suporte para 8 egress queues por porta
43	Suporte de 802.1ad (QINQ)
44	Capacidade de suporte Selective QINQ ou Vlan Mapping
45	Suporte de ACLs
46	Suporte de STP, RSTP
47	Capacidade de Visibilidade Aplicacional
48	Suporte de VRRP
49	Suporte de HQoS, WRED
50	Suporte de MACSec (802.1AE) com encriptação 128 bits
51	Capacidade de Suporte de IP SLA
52	Suporte de IP SLA Responder
53	Suporte de rotas estáticas IPv4 e IPv6
54	Suporte de RIPv1, RIPv2, RIPnG
55	Suporte de OSPFv2 e OSPFv3
56	Capacidade de suporte de ISIS
57	Suporte de Inter-vlan routing
58	Suporte de PBR
59	Capacidade Suporte de VRF
60	Capacidade Suporte de VXLAN
61	Suporte de NETCONF/YANG
62	Capacidade de suporte de patching para correção de bugs sem necessidade de instalar novas imagens de software
63	Suporte para captura de fluxos de tráfego em formato IPFIX ou similares em hardware e sem recurso a sampling de pacotes
64	Suporte de até 16.000 fluxos Full Flexible Netflow ou equivalente
65	Suporte de Ingress e Egress FNF ou equivalente
66	Suporte de VLAN ACLSs IPv4 e IPv6
67	Capacidade de Suporte de Port Based ACLs IPv4 e IPv6
68	Suporte para DAI (Dynamic ARP inspection)
69	Suporte para Port security
70	Suporte para 802.1X
71	Suporte para 802.1X com Change of Authorization
72	Suporte para 802.1X com downloadable ACLs
73	Suporte para 802.1X com guest VLAN
74	Suporte para web authentication para clientes não 802.1X
75	Suporte para RADIUS Authentication, Authorization e Accounting
76	Suporte para TACACS Authentication, Authorization e Accounting
77	Suporte IGMPv1, v2 e v3
78	Suporte de PIM Stub
79	Capacidade de Suporte de PIM, PIM-SM, PIM-SSM
80	Suporte de SSHv2
81	Suporte de SNMPv1,SNMPv2, SNMPv3 e Syslogs
82	Suporte de Funcionalidades de Proteção de Integridade de Hardware e Software:
83	Assinatura de Software e Firmware
84	Secure Boot

1.2.1.4. Switch Tipo 3

De acordo com os seguintes requisitos.

REQ	Requisito
Características Físicas	
1	Equipamento fixo ethernet L2/L3
2	Dimensões: 1RU
3	48 portas 1G com interface do tipo RJ-45;
4	Suportar 48 portas PoE 15.4 W (IEEE 802.3af) ou 24 portas PoE+ 30 W (IEEE 802.3at) sem recorrer a power externo (ex: RPS), e apenas com uma power supply no equipamento;
5	Capacidade de suportar 48 portas PoE+30W(IEEE 802.3at) com a adição de power redundante
6	Suportar velocidades até de (1,2.5,5 e 10Gbps) em 12 das portas RJ-45;
7	O equipamento deverá ter de base um uplink com um mínimo de 4 portas line rate 10G SFP+;
8	Suporte dos seguintes óticos do tipo SFP+ (em módulo uplink):
9	10G Base SR, 10G Base LR, 10G Base ER, 10G Base ZR
10	Suporte dos seguintes óticos do tipo SFP (em módulo uplink):
11	1000Base T, 1000Base SX, 1000Base LX/LH, 1000Base EX, 1000Base ZX
12	Suporte de flash com um mínimo de 4GB para guardar configurações e logs;
13	Capacidade de suporte de stacking através de módulo dedicado, garantindo capacidade para que uns mínimos de 8 equipamentos sejam geridos como um único, através de um endereço único de gestão;
14	Capacidade de suporte de stacking através de módulo dedicado (não são permitidos equipamentos que utilizem o uplink para fazer stacking)
15	A arquitetura do equipamento e da stack tem de ser igual entre os elementos do stack
16	Capacidade de suportar stacking entre equipamentos com diferentes densidades de portas de acesso, com e sem PoE
17	Capacidade de suporte de Stateful switchover, quando comuta de ativo para standby numa stack
18	Capacidade de suporte para fontes de alimentação redundantes e hot-swappable
19	Capacidade de suporte para fans redundantes e hot-swappable
20	Suporte de RFID embebido no equipamento para gestão de ativos
21	Suporte de Blue Beacon para identificação do switch
22	MTBF Mínimo: 337.300 horas
Escalabilidade e Performance	
23	Capacidade de switching mínima: 391 Gbps
24	Capacidade de forwarding mínima: 290Mpps
25	Capacidade de stack bandwidth throughput mínimo de 80 Gbps
26	Número mínimo de VLAN id's: 4096
27	Número mínimo de SVIs: 512
28	Número mínimo de MAC Addresses: 16000
29	Número mínimo de rotas IPv4: 3000
30	Número mínimo de rotas IPv6: 1500
31	Número mínimo de entradas ACL: 1500
32	Suporte de 12M Packet Buffers

33	Instâncias de MST: 64
34	Instâncias de (RSTP/PVSTP) : 128
35	Suporte de Jumbo Frames: 9198 Bytes
36	Suporte de 48 Port-Channles com suporte de até 16 membros por port-channel
Funcionalidades	
37	Suporte para LLDP
38	Suporte de LACP - 802.3ad
39	Suporte de LACP através de diferentes membros da stack
40	Suporte de POE Perpétuo nas Interfaces (não é removido com o reboot)
41	Suporte para 8 egress queues por porta
42	Suporte de 802.1ad (QINQ)
43	Capacidade de suporte Selective QINQ ou Vlan Mapping
44	Suporte para IPv6 em Hardware
45	Suporte para 8 egress queues por porta
46	Suporte de ACLs
47	Suporte de STP, RSTP
48	Capacidade de Visibilidade Aplicacional
49	Suporte de VRRP
50	Suporte de HQoS, WRED
51	Suporte de MACSec (802.1AE) com encriptação 128 bits em todas as interfaces
52	Capacidade de suporte IP SLA
53	Suporte de IP SLA Responder
54	Suporte de rotas estáticas IPv4 e IPv6
55	Suporte de RIPv1, RIPv2, RIPnG
56	Suporte de OSPFv2 e OSPFv3
57	Capacidade de suporte de IS-IS
58	Suporte de inter-vlan routing
59	Suporte de PBR
60	Suporte de NETCONF/YANG
61	Capacidade de suporte VRF
62	Capacidade de suporte VXLAN
63	Suporte para SPAN e Remote SPAN
64	Capacidade de suporte de patching para correção de bugs sem necessidade de instalar novas imagens de software
65	Suporte para captura de fluxos de tráfego em formato IPFIX ou similares em hardware e sem recurso a sampling de pacotes
66	Suporte de até 32.000 fluxos.
67	Suporte de Ingress e Egree FNF
68	Suporte de VLAN ACLSs IPv4 e IPv6
69	Capacidade de Suporte de Port Based ACLs IPv4 e IPv6
70	Suporte para DAI(Dynamic ARP inspection)
71	Suporte para Port security
72	Suporte para 802.1X
73	Suporte para 802.1X com Change of Authorization
74	Suporte para 802.1X com downloadable ACLs
75	Suporte para 802.1X com guest VLAN
76	Suporte para web authentication para clientes não 802.1X
77	Suporte para RADIUS Authentication, Authorization e Accounting
78	Suporte para TACACS Authentication, Authorization e Accounting

79	Suporte IGMP
80	Capacidade de suporte PIM, PIM-SM, PIM-SSM
81	Suporte de PIM-Stub
82	Suporte de SSHv2
83	Suporte de SNMPv1,SNMPv2, SNMPv3 e Syslogs
84	Suporte de gestão Web(HTTPS) embutida nos equipamentos
85	Suporte de funcionalidades de segurança para defesa da integridade do hardware e software do switch, nomeadamente:
86	Assinatura de imagens para garantir a autenticidade da imagem de software

1.3. Solução Segurança

Deverá ser assegurada compatibilidade total entre os equipamentos e software a fornecer no presente procedimento, incluindo os *transceivers*.

A solução a adquirir assenta nos seguintes pressupostos:

- Firewall
- Controlo de acessos
- MFA
- Sonda IoT

1.3.1. Equipamentos e software a adquirir

É pretendido a aquisição dos seguintes equipamentos

Tipo	Descrição	Quantidade
Servidor	Servidor de Suporte à Virtualização	1
Switch	Switch de Perímetro	2
Firewall	Firewall de Perímetro	2
Controlo de acessos	Controlo de acessos	1
MFA	Multi fator de autenticação	500
Analítica	Sonda IOT	1

1.3.1.1. Servidor de Suporte à Virtualização

Para além das plataformas, é ainda objeto deste concurso o fornecimento de HW (servidor) e SW (virtualização) necessários para o funcionamento da solução nas versões propostas e de acordo com os requisitos e recomendações do fabricante.

O IAVE, I.P. pretende que a solução proposta seja suportada sobre virtualização e que sejam propostos os servidores necessários para o correto funcionamento da solução.

A solução a propor deverá incluir fichas e cablagem necessárias para a ligação de todos os equipamentos de acordo com as melhores práticas.

O servidor proposto deverá ter as seguintes especificações ou equivalentes:

- 2 x 2.4 GHz 6336Y/185W 24C/36MB Cache/DDR4 3200MHz
- 2 x 64GB DDR4-3200-MHz RDIMM/DRx4
- 3 x 1.2TB 12G SAS 10K RPM SFF HDD
- 1 x 4x 10/25G SFP28 Interfaces
- 2 x 1050W AC Power Supply for Rack Server
- Sistema de hypervisor de suporte às máquinas virtuais da gestão centralizada da firewall e do controlo de acessos.

1.3.1.2. Switch

Abaixo encontram-se descritas as características do equipamento a adquirir.

REQ	Requisito
Características Físicas	
1	Equipamento Fixo Ethernet L2/L3
2	8 Portas dedicadas para downlink 10/100/1000 BaseT com suporte para um mínimo de 8 portas PoE 15.4 W (IEEE 802.3af) ou 8 portas PoE+ 30 W (IEEE 802.3at), sem recorrer a power externo (ex: RPS), e apenas com uma power supply no equipamento
3	O equipamento deverá ter 2 portas de uplink em cobre e 2 portas de uplink 1GE com interfaces do tipo SFP, com suporte dos seguintes tipos de SFP:
4	1000 Base T
5	1000 Base SX
6	1000 Base LX/LH
7	1000 Base EX
8	1000 base ZX
9	1000BASE-BX10-D
10	1000BASE-BX10-U
11	Suporte para ter as 4 interfaces de uplink do equipamento a funcionar em simultâneo independente de serem GE ou SFP
12	O switch deverá ter um flash com um mínimo de 128MB para storage
13	O switch deverá ter um mínimo de DRAM de 512MB
14	Suporte de interface USB para storage e porta de consola
15	Consumo máximo de power com 0% throughput e sem portas de PoE de 23W;
16	Consumo máximo de power com 100% throughput e sem portas de PoE de 25W;
17	MTBF mínimo: 528,480 horas;
18	Suporte para montagem em Rack e DIN Rail
Escalabilidade e Performance	
19	Capacidade de switching mínima: 92 Gbps
20	Capacidade de forwarding mínima: 68.4 mpps
21	Suporte para um mínimo de 4000 VLAN IDs
22	Suporte para um mínimo 1023 VLAN’s ativas em simultâneo
23	Suporte para um mínimo de 16000 MAC Addresses
24	Suporte de um mínimo de 1000 entradas na tabela de routing IPv4

25	Suporte de um mínimo de 1000 entradas na tabela de routing IPv6
26	Suporte de um mínimo de 1000 IGMP groups
27	Suporte de 6 Port-channels com 8 membros por port-channle
28	Suporte de jumbo frames 9198Bytes
Funcionalidades	
29	Suporte de VLANs (IEEE 802.1Q)
30	Suporte de rotas estáticas IPv4 e IPv6
31	Suporte para inter-vlan routing
32	Suporte de RIP
33	Suporte de BGP, OSPF
34	Suporte de VRRP
35	Suporte de VRF
36	Suporte para LLDP
37	Suporte de PBR
38	Suporte de LACP
39	Suporte de Spanning-Tree, RSTP (802.1w) e MSTP (802.1s)
40	Suporte de DHCP v6 Client/Server/Relay
41	Suporte de Auto-MDIX
42	Suporte de POE Perpetuo
43	Suporte de IEEE 802.1AE MACsec
44	Suporte de port security
45	Suporte de ACLs IPv4 e IPv6 por VLAN e porta
46	Suporte de RADIUS
47	Suporte de RADIUS change of authorization
48	Suporte de Voice VLAN
49	Suporte para configuração simplificada de QoS para voz numa porta através de um único comando por porta
50	Suporte de 802.1X
51	Suporte de 802.1X com downloadable ACLs
52	Suporte de 802.1X guest VLAN
53	Suporte de 802.1X com dynamic VLAN assignment
54	Suporte de 802.1x autenticação multidomínio (permitir que se possa ligar um PC atrás de um telefone IP onde o telefone fica no domínio de voz e o PC no domínio de dados)
55	Suporte de 802.1X MAC authentication bypass
56	Suporte de Web authentication para clientes não 802.1X
57	Suporte de Multicast VLAN Registration (MVR)
58	Suporte de IGMP Snooping v1,v2,v3
59	Suporte de IPv6 MLDv1 e MLDv2 snooping
60	Capacidade de Suporte PIM-SM, PIM-DM, PIM-SSM
61	Suporte de até 8 egress queues por porta
62	Suporte de strict priority queueing
63	Suporte de policer por porta
64	Suporte de port mirroring
65	Suporte de SSHv2 e SNMPv3
66	Suporte de agente de plug-and-play para provisionamento automático de imagem de software e configurações sem intervenção do utilizador
67	Suporte para IPv6 host (addressing, ICMPv6, SNMP para objectos IPv6, traceroute, SSH)

68	Suporte de captura de fluxos de tráfego e export (em formato Netflow v9) para ferramentas de análise de fluxos de tráfego, permitindo detetar anomalias de segurança e top talkers
69	Permitir através do CLI o plug and play de equipamentos ligados ao switch, nomeadamente de pc's, switches, AP's, telefones, impressoras, sem intervenção utilizador, configurando/desconfigurando automaticamente e adaptando ao tipo de device os parâmetros de VLANs, QoS, tipo de porta (acesso/trunk), spanning-tree, protocolo de trunking. Quando o device é desligado da porta, a configuração deverá ser removida automaticamente sem intervenção do utilizador. No caso PC's e impressoras, deverá ser possível a deteção baseada em MAC address e OUI (Organizational Unique Identifier (OUI)). Esta funcionalidade deverá ser implementada sem ter de recorrer a IEEE 802.1X
70	Suporte de protocolo de eficiência energética IEEE 802.3az
71	Suporte nativo de funcionalidades de eficiência energética, 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.

1.3.1.3. Firewall

Abaixo encontram-se descritas as características dos equipamentos a adquirir onde devem estar incluídas todas as licenças necessárias para as funcionalidades pretendidas.

REQ	Requisito
Arquitetura	
1	O mesmo sistema deve suportar os seguintes modos de operação:
2	routed stateful firewall ou transparent stateful firewall e IPS inline set (”bump in the wire” – sem switching ou aprendizagem de MACs)
3	IPS inline set com modo Tap (1 única cópia do packet é inspecionado, mas o IPS está inline)
4	IPS SPAN e interfaces ERSPAN.
Performance e Escalabilidade	
5	FW + AVC Mínimo: 3.3 Gbps
6	FW + AVC + NGIPS Mínimo: 3.3 Gbps
7	Mínimo de sessões concorrentes: 400 mil
8	Mínimo de novas sessões por segundo: 22000
9	IPSEC VPN throughput Mínimo: 1.4 Gbps
10	Número mínimo de peers VPN: 400
Hardware	
12	Deve suportar pelo menos:
13	8 interfaces a 10M/100M/1GBASE-T Ethernet (RJ-45)
14	4 interfaces a 1G SFP
15	Porta serie
16	Porta USB
17	HDD a 200GB
Identity Firewall	
18	A firewall deve ser capaz de autenticar utilizadores através de LDAP ou grupos de Active Directory como condição nas políticas de controlo de acessos.
19	A Firewall deve ser capaz de identificar um utilizador passivo com ’traffic-based detection’ através de inspeção de protocolos LDAP, AIM, Oracle, SIP, HTTP, FTP, MDNS, POP3, IMAP.
Intrusion Prevention System	
20	O sistema deve ter um mecanismo IPS, que deve poder ser ativo através de licenciamento adicional.
21	O mecanismo IPS deve ser compatível com assinaturas snort e suportar regras customizadas.
22	Ao ativar o motor de IPS não deve existir degradação na performance da firewall
23	O mecanismo IPS deve suportar diferentes políticas de IPS e pré-processamento (normalização e fragmentação) para cada política de controlo de acessos.
24	As políticas de configuração IPS devem suportar uma abordagem por camadas. Modificações no set de regras devem ser colecionados em cima das camadas base providenciadas pelo fabricante. Estas camadas podem ser eliminadas ou copiadas entre políticas.
25	O sistema deve ter as seguintes políticas de IPS por defeito: Conectividade sob segurança, balancing, Segurança sob Conectividade e Máxima deteção.

26	O sistema deve sugerir automaticamente regras de IPS a aplicar de acordo com os dispositivos existentes na rede e as vulnerabilidades conhecidas para esses dispositivos
27	O sistema de ser capaz de prioritizar os eventos do IPS de acordo com a relevância dos eventos para a infraestrutura do cliente e do perigo que representam.
28	O sistema deve ser capaz de detetar novas aplicações e sistemas operativos na rede e automaticamente sugerir novas regras de IPS a implementar para proteger a organização contra vulnerabilidades existentes nessas aplicações e sistemas.
29	Deve ser suportado 'Dynamic Rule State' ou funcionalidade similar que permita modificar as ações das regras baseadas em rate counters por Origem, Destino ou ambos.
30	Suporte de pacotes com limites de latência que podem cessar a inspeção de pacotes quando o limite de latência é excedido.
31	O sistema deve suportar updates de assinaturas automáticas de IPS.
IPS Pré processador	
32	Deve suportar normalização de protocolos e opcionalmente certas funções de deteção de ataques antes do mecanismo IPS.
33	O pré-processador deve ser capaz de desfragmentar de acordo com os seguintes métodos: Windows, BSD, BSD-right, HP-UX, MAC-OS, Linux, Cisco IOS e Solaris.
34	O pré processador deverá prevenir ataques SYN e controlar o máximo de conexões em simultâneo na rede ou num dispositivo.
35	O sistema deverá ser capaz de detetar e descodificar os dados dos pacotes:
36	Que excederam o Length Value;
37	Opções inválidas de IP:
38	Opções obsoletas de TCP;
39	Anomalias no cabeçalho do protocolo.
40	O sistema deve fazer descodificação e/ou normalização DCE/RPC, DNS, FTP, GTP, HTTP, SIP, SMTP, SSH, SSL, SunRPC, ModBus, DNP3.
41	O sistema deve ser capaz de normalizar e controlar sessões TCP. Terá de ser capaz de controlar pequenos segmentos, limitar a duplicação de segmentos, controlar timeouts, controlar o máximo tamanho de TCP window, detectar session hijacking e controlar 'handshake timeout'.
Visibilidade e Controlo Aplicacional	
42	O sistema deve ser capaz de reconhecer e controlar mais de 4000 aplicações e micro aplicações por defeito.
43	O sistema deve suportar OpenAppID
44	O sistema deve suportar a criação de detetores de aplicações simples através de um GUI com parâmetros estáticos e reconhecimento de características aplicacionais através da importação de pacotes capturados.
45	Aplicação ou categorização aplicacional deve estar disponível como uma condição nas políticas de controlo de acessos.
46	O sistema deve ter visibilidade sobre os dispositivos e aplicações existentes na rede, nomeadamente:
47	Aplicações usadas pelo cliente
48	Sistema operativo e respetiva versão de servidores e computadores utilizados na rede
49	Dispositivos móveis
50	Browsers
51	Máquinas virtuais
Host Detection e Capacidades de Profiling	

52	O sistema deve ser capaz de detetar e criar um perfil para cada host com métodos passivos e ativos (ex. NMAP)
53	O sistema de gestão deverá conter uma base de dados de vulnerabilidade que possa ser automaticamente comparada aos perfis de Host.
54	O perfil de host deve incluir: endereços IP, MAC addresses, Last Seen timestamp, User (se disponível), Sistema Operativo, Serviços de Servidor, Aplicações vistas, Protocolos de Host e vulnerabilidades relevantes.
55	O sistema deve ser capaz de correlacionar eventos ativos sobre indicações de comprometimento (IoC) com os perfis dos hosts.
56	Os perfis de host devem suportar atributos customizáveis.
Network Discovery e Capacidades de profiling de Tráfego	
57	O Sistema deve ser capaz de descobrir redes e criar perfis de tráfego para redes e zonas.
58	Os perfis de tráfego devem ser criados com base no tráfego de rede inspecionado na firewall e baseados na informação de Netflow através de exportadores externos de Netflow.
Deteção de Anomalias e Correlação	
59	O Sistema deve ser capaz de detetar anomalias nos perfis de tráfego e nos perfis dos utilizadores
60	O sistema deve ser capaz de correlacionar eventos de IPS, Malware, ficheiros, hosts e novas conexões com eventos relacionados com alterações dos perfis de hosts e dos perfis de tráfego, e com isto aplicar automaticamente medidas para prevenir estes cenários.
61	No caso de ocorrerem eventos de correlação, o sistema deve ser capaz de ativar automaticamente medidas de remediação stardard e customizáveis.
Filtragem por reputação, DNS sinkhole e Geolocalização	
62	O sistema deve suportar feeds de reputação disponibilizados pelo vendedor assim como feeds customizáveis.
63	O sistema deve suportar e processar feeds de reputação através de URL, domínio e IP
64	A reputação do domínio deve ser verificada antes de a comunicação ser iniciada entre um utilizador interno e outro externo.
65	O sistema deve ser capaz de fazer drop ou modificar records A e AAAA quando um pedido é feito para domínios bloqueados ou suspeitos.
66	O feed disponibilizado pelo fornecedor deve ter múltiplas categorias, incluindo as seguintes:
67	Attackers Bogon Bots CnC Dga Exploitkit Malware Open_proxy Open_relay Phishing Spam Suspicious Global Blacklist Global Whitelist.

68	O sistema deve ser capaz de utilizar a informação de geolocalização para criar relatórios, como condição para as políticas de controlo de acessos e em políticas de correlação.
URL Filtering Dinâmico	
69	Deve ser possível através de licenciamento adicional fazer filtragem de páginas web. Esta funcionalidade deve:
70	Ser capaz de determinar a categoria e o nível de risco de URLs.
71	Ter atualizações automáticas à base de dados de URLs e permitir que o sistema consulta uma plataforma na cloud no caso de um URL não ser conhecido.
72	Suportar pelo menos 80 categorias de URLs e a base de dados por trás desta solução deve incluir pelo menos 280 milhões de URLs.
Proteção contra Malware e Controlo de Ficheiros	
73	A solução deve conter um motor anti-malware com as seguintes características:
74	Inspeção de ficheiros e malware tem de suportar os protocolos HTTP, FTP, SMTP, POP3, IMAP e NetBIOS.
75	O motor de inspeção de ficheiros deve ser capaz de reconhecer dinamicamente tipos de ficheiros.
76	Fazer verificação da estrutura de ficheiros executáveis e verificação da sua estrutura contra o serviço de cloud do fornecedor.
77	Antivírus tradicional baseado em assinaturas.
78	Serviço de cloud que verifica apenas hashes no serviço de cloud do fornecedor.
79	Deve ser capaz de enviar ficheiros para sandboxing na cloud ou através de appliances dedicadas de sandboxing.
80	O sistema deve ser capaz de visualizar dinamicamente a trajetória dos ficheiros dentro da rede através de um gráfico temporal.
81	A consola de gestão deve reportar o resultado de ficheiros enviados para a plataforma de sandboxing.
82	O sistema deve suportar eventos retrospetivos. O sistema deve ser capaz de categorizar um ficheiro como malware no caso de este ter passado pelo sistema sem ser detetado, e posteriormente for identificado como malware. Devem ser gerados alertas retrospetivos e deve ser possível visualizar os eventos através de um gráfico onde seja possível identificar o ponto de entrada na rede, a trajetória do ficheiro dentro da rede e os protocolos usados para essa propagação.
Gestão de eventos e Assets	
83	O Sistema deve ter widgests.
84	Os widgets devem ser customizáveis.
85	O sistema deve ser capaz de manter um mapa de rede dinâmico.
86	O sistema deve ser capaz de registrar eventos de conexão com base no tráfego inspecionado e nos dados de Netflow exportados a partir de dispositivos de redes externas.
87	Além dos eventos de conexão, o sistema deve ser capaz de gerar eventos quando:
88	Um novo host for descoberto ou quando os atributos de um host existente mudarem.
89	Uma assinatura do IPS dispara.
90	Existe uma correspondência direta com uma política de malware ou de ficheiros.
91	Existe uma correspondência direta com políticas ou regras de correlação.
92	Existem alterações na configuração do sistema

93	O health status muda
94	O sistema de gestão deve ter uma página de síntese única que exibe informação interativa e detalhada de forma gráfica sobre o status da rede, incluindo dados sobre as aplicações, conexões, geolocalização, indicações de comprometimento, eventos de intrusão, hosts, servidores, utilizadores, ficheiros (incluindo ficheiros com malware) e URL relevantes. Esta página também deve permitir filtrar o que se pretende ver.
95	O sistema de gestão deve ter páginas com dados em tempo real (ou quase) sobre:
96	Eventos de malware
97	Eventos de ficheiros
98	Eventos de ficheiros capturados
99	Eventos de conexões
100	Eventos de indicações de comprometimento para hosts e rede
101	Filtragens baseadas em reputação
102	Perfis dos hosts da rede
103	Análise das aplicações
104	Análise ao comportamento dos utilizadores
105	Análise de vulnerabilidades
Políticas de Controlo de Acessos	
106	As políticas de controlo de acesso devem incluir:
107	Zonas de origem e destino
108	Redes de origem e destino
109	Portos de origem e destino
110	Aplicações
111	Reputação de URLs e Ips
112	Categorias de URLs e níveis de risco
113	VLAN Tag (para implementações inline)
114	Geolocalização
115	As ações suportadas para o controlo de acessos devem ser pelo menos:
116	Aplicar políticas de inspeção de ficheiros e de IPS (diferentes regras de controlo de acessos podem ter políticas de IPS ou ficheiros diferentes)
117	Fazer logging do início e/ou fim das conexões
118	Fazer forwarding sem qualquer inspeção adicional
119	Bloquear com TCP reset
120	Fazer drop ao packet
121	Permitir bloqueios interativos para HTTP(S) para que o utilizador possa aprovar uma Acceptable Use Policy para prosseguir com a conexão.
122	Bloqueio interativo com TCP reset
Desencriptação SSL/TLS	
123	O aparelho proposto deve ser capaz de fazer a desencriptação, inspecionar e voltar a encriptar os dados.
124	Desencriptação SSL/TLS deve ser controlada por uma política que é reutilizável e que permita exceções definidas em regras.
125	Desencriptação SSL/TLS não deve ser limitada a HTTPS, outros protocolos que utilizam criptografia SSL ou TLS devem ser suportados.
Integração	
126	A solução deve disponibilizar um API para integração com terceiros.
127	As integrações com API devem ter a capacidade de utilizar e gerir listas de bloqueio de terceiros (3rd-party block lists)

128	Integrações já pré-definidas para soluções terceiras
129	A consola de gestão central tem de permitir a integração com: email e web security, endpoint security, analítica de rede, autenticação forte, solução de network access control e segurança aplicacional. Deve ainda permitir:
130	Orquestração e automação: deve integrar com as diversas soluções mencionadas e simplificar as operações de segurança permitindo criar e gerir workflows de resposta a incidentes
131	Investigação e resposta a incidente: endereçar indicadores de compromisso (IoC) e efetuar investigações de segurança, disponibilizando informação de fontes de inteligência, analisar o risco e o impacto destes IoCs no contexto dos endpoints e com outros indicadores. Uma vez que a investigação se materialize em incidente de segurança, deverá ser possível desenvolver workflows automáticos e processos de remediação, tais como: bloquear IPs maliciosos, domínios, URL e ficheiros.
132	Disponibiliza dashboards das ferramentas com que integra
133	Disponibiliza single sign-on
Solução de gestão centralizada	
134	A solução de gestão centralizada deve ter um GUI.
135	A solução de gestão deve suportar ambientes – multi-tenant, multi-domain e RBAC (Role Base Access Control)
136	A solução de gestão deve suportar autenticação através de RADIUS ou LDAP para os administradores.
137	A plataforma de gestão deve permitir upgrade de firmwares centralizados para todas as plataformas geridas por ela.
138	A plataforma de gestão deve gerir centralmente as licenças.
139	A plataforma de gestão deve aplicar políticas de monitorização. Estas políticas devem incluir:
140	Monitorização de CPU
141	Monitorização dos módulos de hardware
142	Monitorização do status do cluster
143	Monitorização do uso dos discos
144	Monitorização dos links e interfaces
145	Monitorização dos eventos de intrusão e de ficheiros
146	Monitorização dos feeds de informação reputacional recolhidos da cloud
147	Monitorização da sincronização de tempo

1.3.1.4. Controlo de acessos

Pretende-se a aquisição de um sistema de controlo/identificação de acessos à infraestrutura de rede, permitindo o cumprimento das políticas de segurança, e agilizando o processo troubleshooting/deteção de anomalias de segurança.

Abaixo encontram-se descritas as características da plataforma a adquirir onde devem estar incluídas todas as licenças necessárias para as funcionalidades pretendidas

REQ	Requisito
1	Este sistema deverá permitir obter informação em real time, informação contextualizada sobre a rede, utilizadores e dispositivos, fixos ou móveis.
2	O sistema deverá ser uma plataforma única, com capacidade de suporte para garantir AAA, posture, profiling, gestão de acessos guest, TACACS e capacidades de Enterprise Mobility Management. Não são aceites soluções que tenham estas componentes segmentadas, em equipamentos diferentes, já que se pretende uma solução unificada.
3	O sistema deverá poder ser adquirido em forma de appliances físicas ou virtuais. No caso do formato virtual deverá ser suportado Vmware e Hyper-V.
4	Desta forma o sistema, deverá cumprir com os seguintes requisitos macro:
5	Suporte para gerir de base 500 endpoints e com escalabilidade para gerir até 500.000 endpoints
Suporte compliance	
6	Implementar gestão corporativa através de política de acesso consistente para todos os utilizadores, permitindo fazer a monitorização, auditoria e reporting;
Extensão Segurança	
7	Estender segurança de forma uniforme a toda a infraestrutura de rede, assegurando políticas de segurança consistentes, e que agilizem a mobilidade interna de devices sem que seja necessário a reconfiguração de devices, em função da sua localização dentro da rede da organização;
Aumento eficiência	
8	Redução do OPEX do team IT, através de gestão centralizada, integrada com políticas de enforcement, aliadas ao registo dinâmico de devices, users corportativos ou guest, garantindo assim a experiência do utilizador;
Requisitos específicos:	
9	Suporte de AAA para users e devices
10	Capacidade para garantir Compliance do Endpoint, verificando posture de todos os devices ligados na rede, incluindo ambientes com 802.1X.
11	Capacidade de Descoberta, profiling, controle baseado em políticas e post-monitoring de endpoints
12	Registo de Compliance
13	Gestão do lifecycle de devices
14	Context aware: O sistema deverá ser visto na rede, como “single source of truth”, garantindo a obtenção de:
15	Estado da ligação
16	Identificação do user e device
17	Localização
18	Tempo: Hora a que o device se liga/desliga da rede

19	Estado do device
20	Capacidade para aplicação de políticas de enforcement, independentemente do tipo de acesso: 802.1x wired, wireless, VPN
21	Permitir definir políticas de acesso unificadas independentemente de como o dispositivo se liga (cabo, wi-fi ou VPN)
22	Base de dados para profiling aos equipamentos com updates automatizados.
23	Possibilidade de definir políticas com base do tipo de dispositivo e tipo de utilizador.
24	Permitir deployment em 3 modos (modo monitorização, modo de pouco impacto e modo fechado)
25	Página web (GUI) para gestão centralizada. Garantindo gestão centralizada para devices Wired e Wireless
26	Suportar mecanismos de controlo de acessos:
27	802.1X
28	URL redirect
29	MAB
30	Web Authorization
31	Suporte para alterar dinamicamente VLANs e para downloadable ACLs
32	Suporte do RFC 3176/5176(CoA)
33	Suporte de múltiplos use cases:
34	Single-host
35	Multi-host
36	Multi authentication domain
37	Switch authentication to switch
38	Suporte de dados/voz numa porta
39	Controle de acessos independente da topologia;
40	Garantia da confidencialidade e integridade da informação, através do suporte de IEEE 802.1AE(MACSEC). O sistema de controlo/identificação de acessos ter capacidade para funcionar como authentication e policy server, na comunicação entre um cliente mobile e um switch em 802.1X
41	supplicant provisioning e garantir o onboarding de devices para dispositivos móveis como (iOS, Android) e também workstations (PC, MAC)
42	Permitir no acesso de guest e sem implementar políticas de enforcement, ter um modelo de monitor mode;
43	Suporte de RADIUS para AAA
44	Suporte de protocolos de autenticação como:
45	PAP
46	EAP
47	PEAP
48	EAP-FAST
49	EAP-TLS
50	Na aplicação de controlo associado ao Posture deverá ser possível:
51	Verificar patches do OS
52	Antivírus
53	Spyware
54	Auto-remediation de PC's
55	Validar a existência de software com vulnerabilidades (através da integração com uma ferramenta de deteção de vulnerabilidades)
56	Reavaliação periódica para garantir o cumprimento das políticas

57	Capacidade de Integração com MDM (Mobile device management)
58	Capacidade para Proteção do enpoint permitindo, através de estados do device:
59	Quarentena;
60	shutdown
61	Controlo de políticas associados a telefones IP, impressoras
62	O Sistema deverá ser escalável até 500.000 devices, independentemente se são wired ou wireless;
63	O Sistema deverá ter capacidade de recolher informação da AD (Active Directory)
64	Notificações dos utilizadores tem de ocorrer sem intervenção do IT, devendo a solução ser configurável de forma a providenciar números de suporte aos clientes
65	Deteção/isolamento do dispositivo deve ser agnóstico ao OS e HW
66	Deve ser possível criar exceções personalizadas às políticas implementadas, para grupos de utilizadores
67	Suporte de clientes não 802.1X
68	Suporte para certificados e capacidade de atuar como CA (Certificate Authority) para ambientes BYOD
69	Suporte para TACACS+
70	A nível de monitorização deve ser possível:
71	Incluir um painel de segurança
72	Obter relatórios de compliance: DiaCAP, SOX, COBIT, HIPAA, PCI/DSS
73	Relatório de inventário de devices autenticados / não autenticados/guest
74	Relatório com timestamp, nome de utilizadores, IP, nome de devices dos dispositivos autenticados e guest
75	Envio de alarmes quando as políticas não são aplicadas através de SNMP e syslog

1.3.1.5. MFA (Multi-Factor authentication)

Pretende-se adquirir uma ferramenta de multi fatores de autenticação, para ser utilizada na infraestrutura do IAVE, I.P. para um total de 500 endpoints.

Abaixo encontram-se descritas as características da ferramenta a adquirir onde devem estar incluídas todas as licenças necessárias para as funcionalidades pretendidas.

REQ	Requisito
1	A solução deve permitir que os usuários registrem vários dispositivos para autenticação
2	A solução deve permitir que os usuários selecionem um dispositivo preferencial para autenticação
3	A solução deve permitir que os usuários selecionem um dispositivo alternativo (provisionado para esse usuário) se o dispositivo principal não estiver disponível
4	A solução deve permitir que os usuários gerenciem seus dispositivos com segurança para reduzir a carga de trabalho administrativa configurável por usuário e aplicativo
5	Suporta vários tipos de autenticação: Mobile Push, Soft Token, SMS, Phone Call, U2F, Wearables, Biometrics e Hardware Tokens
6	A solução deve suportar tokens Yubikey

7	A solução deve ser capaz de autenticar com uma senha de uso único gerada a partir de um aplicativo móvel
8	A solução deve fornecer códigos de desvio para autenticar
9	A solução deve fornecer um método de autenticação de segundo fator que possa funcionar sem nenhum dado ou conectividade de rede
10	A solução deve oferecer suporte à lista de permissões de IP/geolocalização
11	A solução deve fornecer visibilidade da integridade da segurança de laptops e desktops
12	A solução deve suportar tokens U2F para autenticação em aplicativos baseados em navegador
13	A solução deve permitir políticas personalizadas para bloquear ou alertar os usuários com software de navegador desatualizado para controlar o risco, com base no grupo ou aplicativo
14	A solução deve permitir que políticas personalizadas bloqueiem ou intensifiquem a autenticação para usuários em localizações geográficas específicas para controlar o risco, com base no grupo ou aplicativo
15	A solução deve permitir políticas personalizadas para bloquear usuários com dispositivos com jailbreak/root para controlar o risco, com base no grupo ou aplicativo
16	A solução deve monitorar e opcionalmente impedir tentativas de autenticação originadas de endereços IP anó nimos conhecidos, como aqueles fornecidos por TOR e I2P, proxies HTTP/HTTPS ou VPNs anónimas
17	A solução deve aplicar políticas com base na localização do usuário
18	A solução deve fornecer ferramentas de provisionamento automático para sincronizar usuários existentes do Active Directory
19	A solução deve permitir que os usuários sejam adicionados por meio de uma importação de CSV
20	A solução deve permitir que os administradores habilitem um processo de autoinscrição para usuários finais para reduzir os prazos de implantação
21	A solução deve permitir que os administradores gerem um código de desvio de uso único com base nos direitos apropriados
22	A solução deve permitir que os administradores configurem um identificador de chamadas de saída para autenticação de chamadas telefónicas
23	O aplicativo móvel deve suportar Apple iOS, Google Android, Palm, Windows Phone 7, Windows Mobile 8.1 e 10 e J2ME/Symbian
24	A solução deve fornecer a capacidade de exportar logs para um SEIM de terceiros
25	A solução deve oferecer suporte a controles de administração baseados em função para administradores
26	A solução deve fornecer uma visão geral do painel de dispositivos em risco com base em sistemas operacionais, navegadores ou plug-ins desatualizados
27	A solução deve permitir branding personalizado com logotipo corporativo
28	A solução deve ser capaz de identificar dispositivos não gerenciados que acedam a aplicativos internos
29	A solução deve fornecer relatórios sobre dispositivos gerenciados versus não gerenciados que acedam a qualquer aplicativo local e baseado em nuvem
30	A solução deve permitir a criação de políticas de segurança para dispositivos não gerenciados que acedam a aplicativos específicos
31	A solução deve se integrar à solução MDM existente para identificar dispositivos confiáveis e não gerenciados

32	A solução deve permitir o grupo piloto de teste de usuários e impedir o acesso de aplicativos de seus dispositivos não gerenciados sem afetar o restante da organização
33	A solução deve ser capaz de permitir que os usuários acedam a sites, aplicativos e servidores SSH locais
34	A solução deve identificar dispositivos corporativos e BYOD
35	Identifique se um agente de terceiros está habilitado no dispositivo

1.3.1.6. Sonda IoT

Pretende-se adquirir uma ferramenta de machine learning que permita controlar os dispositivos não geridos através de algoritmos de inteligência artificial para identificar e classificar com precisão. Abaixo encontram-se descritas as características da ferramenta a adquirir onde devem estar incluídas todas as licenças necessárias para as funcionalidades pretendidas.

REQ	Requisito
Arquitetura	
1	Número de portas 1Gbit/s RJ45 >= 4
2	Disco rígido eMMC >= 128GB
3	Porta USB >= 2
4	Porta de gestão dedicada "Out of Band"
5	Porta de consola RJ45
6	A appliance de FW deverá ter uma arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção.
7	Deverá estar garantido que a appliance de FW quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa.
Performance	
8	Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego) >= 4,4 Gbps
9	Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, URL Filtering e Sandboxing >= 2,4 Gbps
10	Performance da appliance com a funcionalidade de VPN IPSec >= 3,0 Gbps
11	Número de novas sessões por segundo >= 73 000
12	Número máximo de sessões >= 400 000
Segurança de Dispositivos	
13	A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos.
14	A firewall deve colecionar metadados do tráfego de rede dos dispositivos, gerar logs com estas informações e enviá-los para um repositório de dados. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos na rede.

15	A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses.
16	O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: câmara de vigilância), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo.
17	Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms.
18	Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal.
19	A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão, não sendo assim necessário criar regras com base em IPs ou zonas.
20	Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos,etc.
21	O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas ao uso/configuração incorreta dos mesmos. Exemplo: uso de credenciais default.
22	Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB(Cloud Access Security Broker).
23	O repositório de dados deve ter capacidade de armazenamento de logs de 1 TB.

Parte III

Serviços

Artigo 24º
Serviços de assistência técnica e garantias

As atividades a desenvolver no âmbito da assistência técnica e o previsto para as garantias que vigoram durante, pelo menos, três anos, sem prejuízo do que vier a ser convencionado na proposta adjudicada, por força da aplicação dos critérios de adjudicação são as seguintes:

- Suporte técnico diretamente do fabricante para o IAVE, enquanto entidade adjudicante, sem necessidade de recurso a parceiros do fabricante.
- Acesso direto ao portal do fabricante para abertura de casos e respetivo acompanhamento.
- Acesso direto ao portal do fabricante para download de software dos equipamentos sob contrato.
- Acesso direto ao portal do fabricante para substituição de hardware em caso de avaria
- Substituição em caso de avaria no dia útil seguinte. (NBD);
- Suporte técnico telefónico do fabricante durante o período mínimo da vigência das garantias e da assistência técnica.
- Prestação de serviços de suporte e assistência técnica;
- Reparação de avarias;
- Desmontagem/montagem de peças, componentes ou bens defeituosos ou discrepantes;
- Reparação ou substituição de peças, componentes ou bem defeituosos ou discrepantes;
- Fornecimento, montagem ou instalação de peças, componentes ou bens reparados ou substituídos;
- Transporte do equipamento, peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens, entrega das peças ou componentes em falta, reparados ou substituídos;
- Deslocação ao local de instalação dos equipamentos;
- Mão-de-obra.

Artigo 25º
Auditoria à implementação da solução

O Prestador de serviços deverá garantir a execução do contrato através de uma auditoria no final da implementação, com o objetivo de validar e aprovar as metodologias adotadas.

A equipa de auditoria deverá ser constituída por analistas/especialistas dotados de conhecimentos em redes WAN, LAN, e segurança de redes, devendo a equipa cumprir com os requisitos devidamente certificados, ou equivalentes, a saber:

- Dispor, obrigatoriamente, da certificação do fabricante da solução proposta;
- Dispor, obrigatoriamente, da Certificação Lead Auditing 27001;
- Dispor, obrigatoriamente da certificação Certified Information System Security Professional (CISSP) ou Information Technology Infrastructure Library (ITIL) ou equivalente.

A equipa de auditoria deverá ser constituída com as seguintes capacidades:

1. Experiência em auditorias de segurança e análise técnica.
2. Experiência auditorias e testes de penetração (e. g., *Nessus, Acunetix, entre outras*).
3. Experiência comprovada nas seguintes áreas em administração de redes:
    a. WAN
    b. LAN Wired e Wireless
4. Experiência comprovada nos seguintes produtos em gestão de sistemas de segurança de rede;
    a. Firewalls
    b. VPN
    c. Outros sistemas de segurança como:
        - Servidor de autenticação (TACACS, Radius e 802.1x);
        - Ferramentas de diagnóstico (ex. *Wireshark*);
        - Gestão, *hardening* e monitorização dos ativos de rede (SNMPV3, NTP, SSH, etc.)