Agência para a Energia

Assinado por : **ANA CRISTINA SEQUEIRA PEREIRA**
Num. de Identificação: BI098109065
Data: 2022.10.21 14:54:12+01'00'

CONCURSO PÚBLICO N.º ADENE_CP_041_2022_USTI

AQUISIÇÃO DE SERVIÇOS DE INTERNET FIXA E SEGURANÇA DA REDE (FIREWALL)

CADERNO DE ENCARGOS

2022

Capítulo I

Âmbito do contrato

Cláusula 1.ª

Objeto

O presente Caderno de Encargos compreende as cláusulas a incluir no Contrato a celebrar na sequência do procedimento de Concurso Público para a *Aquisição de Serviços de Internet Fixa e Segurança da Rede (Firewall).*

Cláusula 2.ª

Contrato

1. O Contrato é composto pelo respetivo clausulado contratual e os seus anexos, incluindo os ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos ("CCP")[1] e aceites pelo adjudicatário nos termos do disposto no artigo 101.º do mesmo Código.
2. O Contrato a celebrar integra ainda os seguintes elementos:
   a) Os suprimentos dos erros e das omissões do Caderno de Encargos identificados pelo concorrente, desde que esses erros e omissões tenham sido expressamente aceites pelo Conselho de Administração da ADENE – Agência para a Energia ("ADENE"), na qualidade de órgão responsável pela decisão de contratar;
   b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
   c) O presente Caderno de Encargos;
   d) A proposta adjudicada, sem prejuízo do disposto no n.º 4 do artigo 96.º do CCP;
   e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo

[1] Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua atual redação.

99.º do CCP e aceites pelo Prestador de serviços nos termos do disposto no artigo 101.º do mesmo Código.

Cláusula 3.ª

Set-up e Duração do Contrato

1. O contrato inicia a sua vigência na data da respetiva assinatura e termina 36 (trinta e seis) meses após a conclusão da fase de *set-up*, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do Contrato.
2. A fase de *set-up* corresponde a um período máximo de 3 meses, a contar do início de vigência do contrato, que o adjudicatário terá para concluir a instalação das várias componentes do serviço nos termos e nos prazos indicados nas Especificações Técnicas constantes do Anexo ao presente Caderno de Encargos.

Capítulo II

Obrigações contratuais

Secção I.

Prestador de Serviços

Cláusula 4.ª

Obrigações do Prestador de Serviços

1. Sem prejuízo de outras obrigações previstas na legislação e regulamentação aplicáveis, no presente Caderno de Encargos, seus anexos ou nas cláusulas contratuais, da celebração do Contrato decorrem para o prestador de serviços as seguintes obrigações principais:
   a) Assegurar a adequada e atempada prestação de serviços de "*Aquisição de Serviços de Internet Fixa e Segurança da Rede (Firewall)*", nos termos previstos no Anexo ao presente Caderno de Encargos, que dele faz parte integrante e na proposta adjudicada;
   b) Cumprir o disposto na Cláusula 5.ª e Cláusula 6.ª, em matéria de confidencialidade;
   c) Cumprir o disposto na Cláusula 7.ª, em matéria de proteção de dados pessoais;

d) Designar um Gestor do Contrato, com vista a assegurar uma interligação eficaz com a ADENE;

e) Comunicar à ADENE qualquer facto que ocorra durante a execução do Contrato e que altere, designadamente, a sua denominação social, os seus representantes legais, a sua situação jurídica e a sua situação comercial;

f) Comunicar à ADENE a ocorrência de qualquer das circunstâncias previstas no artigo 55.º do CCP, no decurso da execução do Contrato;

g) Cumprir a legislação em vigor relativamente a questões ambientais nomeadamente a relacionada com resíduos, assumindo exclusiva responsabilidade pelo cumprimento da legislação ambiental aplicável às atividades desenvolvidas no âmbito do Contrato;

h) Prestar à ADENE toda a cooperação e todos os esclarecimentos necessários, devendo ainda comunicar à ADENE, antecipadamente ou logo que deles tome conhecimento, factos que tornem total ou parcialmente impossível a realização de alguma das ações ou o cumprimento de algumas das obrigações assumidas no Contrato.

2. O prestador de serviços deve observar as condições gerais aplicáveis à sua atividade profissional, comprometendo-se a colocar à disposição da ADENE todas as suas capacidades técnicas, bem como a realizar todos os trabalhos com a diligência, qualidade e imparcialidade exigíveis para este tipo de serviços.

3. O prestador de serviços fica ainda obrigado a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação dos serviços, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 5.ª

Confidencialidade e obrigação de destruição de dados

1. O prestador de serviços assume obrigação de estrita confidencialidade relativamente a toda a informação e documentação, técnica e não técnica, comercial ou outra, de que venha a ter conhecimento, por qualquer entidade, ao abrigo ou em relação com a execução do Contrato.

2. A informação e a documentação abrangidas pela obrigação de confidencialidade não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do Contrato.

3. O disposto nos números anteriores é extensivo à informação a que os trabalhadores, agentes, subcontratados e consultores do prestador de serviços tenham acesso em virtude da celebração do Contrato.

4. Exclui-se da obrigação de confidencialidade a informação e a documentação que:

   a) Fosse já comprovadamente pública à data da respetiva obtenção pelo prestador de serviços, seus trabalhadores, agentes, subcontratados e consultores; ou

   b) Tenha sido prévia e legitimamente divulgada por terceiros; ou

   c) O prestador de serviços, seus trabalhadores, agentes, subcontratados e consultores sejam legalmente obrigados a revelar, por força da lei, de processo judicial ou a solicitação de autoridades reguladoras ou outras entidades administrativas competentes, desde que observados os procedimentos estabelecidos para o efeito.

5. O prestador de serviços fica ainda obrigado a manter um registo de todos os colaboradores que, no decurso da execução do Contrato, tenham acesso aos dados a que se refere o número anterior.

6. Nos termos da execução do Contrato, o prestador de serviços fica obrigado a destruir todos os dados aos quais teve acesso em virtude da execução do Contrato a celebrar, bem como a emitir e entregar à ADENE um auto de destruição desses dados.

Cláusula 6.ª

Prazo da obrigação de confidencialidade

A obrigação de confidencialidade mantém-se em vigor até ao termo do prazo de 5 (cinco) anos a contar do cumprimento ou cessação, por qualquer causa, do Contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de direitos comerciais ou da credibilidade, prestígio ou confiança devida às pessoas coletivas.

Cláusula 7.ª

Proteção de dados pessoais

As Partes obrigam-se a cumprir todas as disposições legais aplicáveis em matéria de tratamento de dados pessoais, designadamente, as disposições contidas no Regulamento (UE) 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 na Lei n.º 58/2019, de 8 de agosto, ou outra que a venha a substituir, em relação aos dados pessoais a que acedam no âmbito do Contrato.

Cláusula 8.ª

Forma e local de prestação dos serviços

1. O prestador de serviços deve assegurar total disponibilidade para a realização de reuniões de coordenação e de reuniões de trabalho, sempre que solicitadas pela ADENE.
2. Para além das reuniões previstas no número anterior, o prestador de serviços deve ainda manter total disponibilidade para a realização de reuniões com entidades terceiras, sempre que solicitado para o efeito.
3. O prestador de serviços obriga-se a acatar todas as instruções que lhe sejam transmitidas pela ADENE para o exato e pontual cumprimento de todos os serviços objeto do presente Caderno de Encargos.
4. Todas as comunicações e demais documentos elaborados pelo prestador de serviços devem ser integralmente redigidos em português.
5. Os serviços previstos no presente Caderno de Encargos são disponibilizados anualmente, sendo que o serviço relativo à implementação apenas é devido uma única vez, durante todo o período de vigência do Contrato.

Cláusula 9.ª

Direitos de propriedade intelectual

1. O prestador de serviços é responsável por quaisquer encargos decorrentes da utilização, no âmbito do Contrato, de marcas ou patentes registadas ou licenças.
2. Caso a ADENE venha a ser demandada por ter infringido, no âmbito do Contrato, quaisquer direitos mencionados no número anterior, o prestador de serviços deverá indemnizar a ADENE por todas as despesas em que, em consequência, esta haja incorrido.
3. O prestador de serviços é responsável por qualquer violação das normas legais ou direitos de terceiros em relação a direitos de autor ou direitos conexos, bem como quaisquer direitos de propriedade industrial por ele utilizados no âmbito do Contrato.

Cláusula 10.ª

Organização e meios do prestador de serviços

1. O prestador de serviços fica obrigado a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação dos serviços, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.
2. A ADENE pode ordenar ao prestador de serviços que retire da equipa afeta à execução do Contrato qualquer elemento que revele deficiente desempenho das funções que lhe estão cometidas, que desrespeite os trabalhadores daquela, seus colaboradores ou quaisquer outras entidades intervenientes na execução do Contrato ou ainda que provoque indisciplina no desempenho dos seus deveres, devendo tal ordem ser fundamentada e emitida por escrito.
3. No caso previsto no número anterior, o prestador de serviços deve substituir o membro da equipa no prazo determinado pela ADENE por um outro elemento com o perfil, qualificações e competências iguais ou análogos ao membro substituído.
4. O prestador de serviços deve cumprir todas as obrigações legais com respeito aos seus trabalhadores, nomeadamente laborais e de segurança social.

Cláusula 11.ª

Seguros

1. O prestador de serviços é responsável, perante a ADENE, pelos seguros cuja celebração e manutenção seja devida aos seus trabalhadores que sejam afetos à execução do Contrato.
2. O prestador de serviços apresentará à ADENE, sempre que tal lhe seja solicitado, os comprovativos do pagamento dos respetivos prémios.

Secção II.

ADENE

Cláusula 12.ª

Obrigações da ADENE

Constituem obrigações da ADENE:

a) Proceder ao pagamento do preço contratual de acordo com as condições previstas na Cláusula 14.ª e Cláusula 15.ª;

b) Facultar ao prestador de serviços o acesso à informação relevante por este solicitada para a execução do objeto do Contrato e mantê-lo informado, durante a duração do Contrato, de toda a informação relevante de que tenha conhecimento;

c) Designar um Gestor do Contrato, com vista a assegurar uma interligação eficaz com o prestador de serviços, nos termos do disposto no artigo 290.º-A do CCP.

Cláusula 13.ª

Gestor do Contrato

O Gestor do Contrato procederá ao acompanhamento permanente da execução do Contrato, cabendo-lhe, entre outras:

a) Dar instruções ao prestador de serviços acerca do modo de cumprimento das obrigações previstas no Contrato;

b) Verificar se, e em que termos, são cumpridas as obrigações previstas no Contrato;

c) Analisar e validar a(s) fatura(s) emitida(s) pelo prestador de serviços com vista ao(s) respetivo(s) pagamento(s);

d) Determinar ao prestador de serviços, fundamentadamente, alterações à organização e meios do prestador de serviços nos termos contratualmente previstos;

e) Propor, fundamentadamente, ao órgão competente da ADENE a adoção de outras medidas corretivas do cumprimento defeituoso do Contrato;

f) Propor, fundamentadamente, ao órgão competente da ADENE a aplicação de quaisquer sanções que considere serem legal ou contratualmente devidas.

Cláusula 14.ª

Preço base, Preço contratual e Forma de pagamento

1. O preço máximo (preço base) que a ADENE se dispõe a pagar pela execução de todas as prestações que constituem o objeto do Contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, é de 204.650,00 € (duzentos e quatro mil e seiscentos e cinquenta euros).

2. Pela prestação dos serviços objeto do Contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a ADENE paga ao prestador de serviços os preços unitários constantes da proposta adjudicada, arredondados à segunda casa decimal, nos termos do Anexo II ao Programa do Procedimento, em função dos serviços que hajam de facto sido prestados.

3. Aos valores previstos nos números anteriores acresce o IVA à taxa legal em vigor que seja devido.

4. Os preços referidos nos números anteriores incluem todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à ADENE, incluindo, sem limitar, as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transportes, armazenamento e manutenção de meios materiais, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes e ou direitos de propriedade industrial ou licenças, e ainda quaisquer outros meios necessários ao exato e pontual cumprimento das obrigações contratuais.

5. Não há lugar a revisão de preços.

Cláusula 15.ª

Condições de pagamento

1. Não há lugar a pagamentos antecipados ao prestador de serviços.
2. As quantias devidas pela ADENE, nos termos da cláusula anterior, são pagas no prazo de 30 (trinta) dias após a receção, por esta, da(s) respetiva(s) fatura(s), a(s) qual(is) só pode(m) ser emitida(s) após o vencimento da obrigação respetiva.
3. Para os efeitos do número anterior, a obrigação considera-se vencida com a emissão da declaração de aceitação pela ADENE, devendo esta ser emitida após a conclusão dos serviços de instalação e configuração e até ao 5.º dia após o termo do mês a que respeita cada mensalidade consoante o caso.
4. A(s) fatura(s) deve(m) ser remetidas para o endereço de correio eletrónico contasapagar@adene.pt, com o conhecimento do Gestor do Contrato e de compras@adene.pt, incluindo os seguintes elementos:
   a) Número do Contrato: ADENE_CP_041_2022_USTI;
   b) Número de Compromisso;
   c) Descrição, referindo o(s) documento(s) que a suporta(m);
   d) IBAN, para efeitos de transferência bancária;
   e) Incidência do IVA, em separado;
   f) Documentação de suporte;
   g) Emissão em nome de 'ADENE – AGÊNCIA PARA A ENERGIA'.
5. Em caso de discordância, por parte da ADENE, quanto ao(s) valor(es) indicado(s) na(s) fatura(s), deve esta comunicar ao prestador de serviços, por escrito, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.
6. O atraso no pagamento de qualquer (quaisquer) fatura(s) regularmente emitida(s) não autoriza o prestador de serviços a invocar a exceção de não cumprimento de qualquer das obrigações que lhe incumbem por força do Contrato, salvo nos casos previstos no artigo 327.º do CCP.

7. O não pagamento atempado da(s) fatura(s) devida(s) confere ao prestador de serviços o direito de reclamar juros de mora, nos termos previstos no artigo 326.º do CCP.

8. Os valores contestados pela ADENE e que vierem a ser objeto de correção não vencem juros de mora em caso de não pagamento.

9. No que respeita à faturação eletrónica, o prestador de serviços deve obedecer ao disposto no artigo 299.º-B do CCP e no Decreto-Lei n.º 123/2018, de 28 de dezembro, conforme aplicável.

10. Desde que devidamente emitida e observado o disposto nos números anteriores, a fatura é paga através de transferência bancária.

Capítulo III

Penalidades contratuais e resolução

Cláusula 16.ª

Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do Contrato, imputáveis ao prestador de serviços, a ADENE pode exigir-lhe o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, até 0,025% do preço contratual por cada dia de atraso na conclusão da instalação e configuração da solução e por cada dia de incumprimento dos níveis de serviço indicados nas Especificações Técnicas constantes do anexo ao presente Caderno de Encargos.

2. Na determinação da gravidade do incumprimento, a ADENE tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do prestador de serviços e as consequências do incumprimento.

3. Em caso de resolução do Contrato por incumprimento do prestador de serviços, a ADENE pode exigir-lhe uma pena pecuniária de até 20% do preço contratual.

4. Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo prestador de serviços ao abrigo do n.º 1, em conformidade com o disposto no n.º 2 do artigo 329.º do CCP.

5. A ADENE pode compensar os pagamentos devidos ao abrigo do Contrato com as penas pecuniárias devidas nos termos da presente cláusula.

6. As penas pecuniárias previstas na presente cláusula não obstam a que a ADENE exija uma indemnização pelo dano excedente, nos termos gerais de Direito.

Cláusula 17.ª

Resolução por parte da ADENE

1. A ADENE pode resolver o Contrato a título sancionatório em qualquer das seguintes situações previstas no n.º 1 do artigo 333.º do CCP:

   a) Incumprimento definitivo do Contrato por facto imputável ao prestador de serviços;

   b) Incumprimento, por parte do prestador de serviços, de ordens, diretivas ou instruções transmitidas no exercício do poder de direção sobre matéria relativa à execução das prestações contratuais;

   c) Oposição reiterada do prestador de serviços ao exercício dos poderes de fiscalização da ADENE;

   d) Cessão da posição contratual ou subcontratação realizadas com inobservância dos termos e limites previstos na lei ou no contrato, desde que a exigência pelo prestador de serviços da manutenção das obrigações assumidas pela ADENE contrarie o princípio da boa-fé;

   e) Se o valor acumulado das sanções contratuais com natureza pecuniária exceder o limite previsto no n.º 2 do artigo 329.º do CCP;

   f) Incumprimento pelo prestador de serviços de decisões judiciais ou arbitrais respeitantes ao Contrato;

   g) O prestador de serviços se apresente à insolvência ou esta seja declarada pelo tribunal.

2. Considera-se que existe incumprimento definitivo do prestador de serviços se se verificar qualquer uma das seguintes situações:

   a) Violação da obrigação de confidencialidade prevista na Cláusula 5.ª;

   b) Violação de proteção de dados prevista na Cláusula 7.ª.

3. É ressalvado o direito de indemnização nos termos gerais, nomeadamente pelos prejuízos decorrentes da necessidade de adoção de novo procedimento de formação de contrato.

4. O direito de resolução exerce-se mediante declaração enviada ao prestador de serviços e não determina a repetição das prestações já realizadas.

Cláusula 18.ª

Resolução por parte do prestador de serviços

1. O prestador de serviços pode resolver o Contrato nos casos e nos termos previstos no artigo 332.º do CCP.
2. O direito de resolução exerce-se nos termos dos n.os 3 e 4 do artigo 332.º do CCP e não determina a repetição das prestações já realizadas pelo prestador de serviços, cessando, porém, todas as obrigações deste ao abrigo do Contrato.

Capítulo IV

Vicissitudes contratuais

Cláusula 19.ª

Força maior

1. Nenhuma das partes é responsável pelo incumprimento ou pelo cumprimento defeituoso das obrigações emergentes do Contrato na estrita medida em que estes resultem de casos de força maior.
2. São considerados casos de força maior as circunstâncias que impossibilitem o cumprimento das obrigações emergentes do Contrato, 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.
3. Os requisitos do conceito de força maior estipulados no número anterior são cumulativos.
4. Podem constituir força maior, no caso de se verificarem os pressupostos do n.º 2, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, desastres nucleares, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

5. Não constituem força maior, designadamente:

   a) Greves ou conflitos laborais limitados ao prestador de serviços ou a grupos de sociedades em que se integre;

   b) Determinações governamentais, administrativas ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;

   c) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;

   d) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;

   e) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços;

   f) Eventos que estejam ou devam estar cobertos por seguros.

6. A ocorrência de circunstâncias que possam consubstanciar força maior deve ser imediatamente comunicada à outra parte, devendo a parte que a invoca indicar as obrigações emergentes do Contrato cujo cumprimento, no seu entender, se encontra impedido ou dificultado por força de tal ocorrência, e as medidas que pretende pôr em prática a fim de mitigar o impacto da referida situação e os respetivos prazos e custos.

7. A comunicação a que se refere o número anterior tem lugar no prazo máximo de 5 (cinco) dias a contar da verificação do facto ou do respetivo conhecimento.

8. Quando uma das partes não aceite por escrito que certa ocorrência invocada pela outra constitua força maior, cabe a esta fazer prova dos respetivos pressupostos.

9. A verificação de uma situação de 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.

10. No caso referido no número anterior, o prestador serviços deve requerer à ADENE, na comunicação prevista nos n.os 6 e 7, a prorrogação de prazo aplicável.

Cláusula 20.ª

Subcontratação e cessão da posição contratual

A subcontratação pelo prestador de serviços e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do CCP.

Cláusula 21.ª

Foro competente

Para resolução de todos os litígios decorrentes do Contrato fica estipulada a competência do tribunal administrativo de círculo de Lisboa, com expressa renúncia a qualquer outro.

Capítulo V

Disposições finais

Cláusula 22.ª

Comunicações e notificações

1. As Partes designam os seguintes gestores do Contrato:

   1.1. Para a ADENE: [●]

   Correio eletrónico: [●]@adene.pt

   Telefone: [●]

   1.2. Para o prestador de serviços: [●]

   Correio eletrónico: [●]@[●]

   Telefone: [●]

2. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as Partes do Contrato, estas devem ser dirigidas, nos termos do CCP, para o domicílio ou sede contratual ou para o correio eletrónico de cada uma das Partes identificadas no Contrato:

   2.1. Para a ADENE: [●]

   Endereço: Avenida 5 de Outubro, n.º 208, 2.º andar, 1050-065 Lisboa

   Correio eletrónico: [●]@adene.pt

Telefone: [●]

2.2. Para o prestador de serviços: [●]

Endereço: [●]

Correio eletrónico: [●]@[●]

Telefone: [●]

3. Qualquer alteração das informações de contacto constantes do Contrato deve ser comunicada à outra Parte, nos termos do n.º 2.

Cláusula 23.ª

Contagem dos prazos

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

Cláusula 24.ª

Legislação aplicável

1. O Contrato é regulado pela legislação portuguesa.
2. Em tudo o que o presente Caderno de Encargos for omisso, observar-se-á o disposto no CCP e demais legislação aplicável.

ANEXO: ESPECIFICAÇÕES TÉCNICAS

adene

Agência para a Energia

ANEXO

ESPECIFICAÇÕES TÉCNICAS

NECESSIDADE DE ALTO NÍVEL

A ADENE pretende implementar uma solução de internet e *firewall*, que satisfaça as necessidades existentes da ADENE em termos de segurança e largura de banda de internet que permita ter acesso a aplicações de forma rápida e eficaz, definir políticas de acesso por colaborador ou departamento como também controlar tentativas de ataques informáticos ou exploração de vulnerabilidades de aplicações.

Dentro desta solução incluímos diversos serviços, como acesso VPN com dupla autenticação, módulo para publicação de portais de forma mais eficiente, expansão da rede *wifi* e testes de intrusão aos *emails* dos colaboradores.

SERVIÇOS E EQUIPAMENTOS

Pretende-se a disponibilização dos seguintes serviços e/ou equipamentos.

#	Descrição
1	Serviço de internet
2	Sistema de *Firewall*
3	Serviço de VPN
4	Sistema de Rede WIFI
5	Outros serviços
6	Suporte, Garantias e Níveis de Serviço

SERVIÇO DE INTERNET

1. Indicamos as necessidades para o serviço de internet.

#	Item
1.1 Links de internet	• 2 *links*, um como principal e outro como *backup*; • Redundantes e dedicados de 1GB cada, simétrico de *download* e *upload* (MPLS ou equivalente); • Chegada física dos *links* à entrada do edifício por 2 caminhos

#	Item
	distintos; • Equipamento terminal com portas RJ45 ou fibra, necessárias para interligar com rede da ADENE e criar redundância na ligação com os equipamentos de *firewall* (responsabilidade da ADENE); • 16 IP´s públicos incluídos.
1.2 Acréscimo de 500mbps	• Possibilidade de aumento de 500mbps em cada *link*; • Aumento do *link* será opcional e durante a vigência do contrato.
1.3 Link 100mbps	• 1 *link* simétrico de *download* e upload e do tipo doméstico; • Deve ser fornecido com router WIFI que permita interligar com os *switches* da ADENE e criar VLAN para distribuir a rede pelos diversos pisos e pontos de rede fixos (responsabilidade da ADENE).
1.4 Acréscimo de IP´s públicos	• Aquisição de mais IP´s públicos; • Pacotes de 8 endereços; • Aquisição destes IP´s será opcional e durante a vigência do contrato.
1.5 Garantia e Suporte	• O prestador de serviços deverá ainda assegurar a conservação e reparação de cada um dos circuitos, bem como das infraestruturas/equipamentos associados, de forma pró-ativa.
1.6 Instalação	• O prestador de serviços (concorrente), deve indicar na sua proposta, todos os custos associados à instalação dos serviços de internet. • A instalação dos serviços deverá ser assegurada na ADENE, sita na Avenida 5 de outubro, 208, 4. ° piso, 1050-065 Lisboa, com as coordenadas geográficas 38° 44' 37. 5" N 9° 08' 56. 6" W. • Poderá ser visitada a instalação, no endereço acima referido, durante as horas de expediente (das 9:30 às 13 horas e das 14:30 às 18 horas), desde o dia da publicação do anúncio no Diário da República até ao termo do prazo fixado para a apresentação das propostas, através de marcação prévia solicitada por mensagem na plataforma eletrónica. • A instalação deverá estar concluída no prazo de 3 meses a contar do início da vigência do contrato.

SISTEMA DE *FIREWALL*

2. Indicamos as necessidades para o serviço de *firewall*

#	Item
2.1 Equipamentos de *firewall*	• 2 equipamentos físicos para criar redundância; • Capacidade para suportar o circuito de internet indicado e seu acréscimo opcional; • Capacidade para suportar 200 utilizadores conectados em simultâneo e 500 equipamentos em média; • Deverá realizar todo o tipo de proteção contra as principais ameaças (IPS, SSL *inspection*, Antivírus, etc.); • Capacidade para criar diversos tipos de relatórios; • Capacidade para utilizar a função de ZTNA.
2.2 *Appliance* virtual para recolha de *logs*	• Servidor para análise de *logs* e eventos.
2.3 Instalação e configuração	• Instalação e configuração dos equipamentos físicos, criação de políticas novas, e migração e/ou configuração de todas as políticas que existem na *firewall* atual (interfaces, políticas, VIPs, serviços, etc); • Incluídas 2 horas mensais de suporte ou para novas configurações; • A instalação deverá estar concluída no prazo de 3 meses a contar do início da vigência do contrato.

2.1 Equipamentos de *firewall*

Elencamos com mais detalhe as caraterísticas e funcionalidades que os equipamentos devem ter.

2.1.1 Integração com redes de comunicações

As seguintes funcionalidades deverão ser suportadas:

- Servidor de DHCP, NTP e DNS incluído
- Funcionalidade de DNS Proxy
- Múltiplos modos de configuração de interfaces:
  - *Sniffer*
  - Agregação de portas (802.3ad)
  - *Loopback*

- VLANs (802.1Q e *trunk*)
- *Software switch*

- *Routing* estáticos e baseado em políticas (PBR – *Policy Based Routing*)
- SD-WAN
  - *Application Awareness & Steering* (3000+ *Applications Supported*)
  - *Dynamic WAN Path Controller*
  - NGFW *with* SSL *Inspection*
  - *Dynamic failover times*
  - *Secure* VPN *Overlays*
  - *Single Management Console for Security* & SD-WAN
  - *Zero-touch provisioning*
- Balanceamento e redundância de múltiplos *links*;
- Suporte para protocolos de *routing* dinâmico: RIPv1, RIPv2, RIPng, OSPFv2 e OSPFv3, ISIS, BGP4+
- Suporte de tráfego *multicast*: PIM, *sparse e dense mode*
- *Routing* baseado em conteúdos: WCCP e ICAP
- *Proxy* explícito com suporte PAC e WPAD
- Suporte de Ipv6
  - Gestão por Ipv6
  - Protocolos de *routing* dinâmico com suporte para Ipv6
  - *Tunneling* de Ipv6
  - Processamento *firewall* e UTM de Ipv6
  - NAT64
  - NAT46
  - VPN IPSec Ipv6
- Suporte *Dual Stack* Ipv4 e Ipv6 em simultâneo
- Suporte VXLAN
- Controlador *Wireless* integrado

- Controlador *Switch* integrado
- Virtualização da solução em contextos.

2.1.2 Identificação de utilizadores e dispositivos

As seguintes funcionalidades deverão ser suportadas:

- Base de dados local de utilizadores;
- Autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+
- Sistema de *Single Sign-on* de utilizadores:
  - *Windows* AD
  - *Kerberos*
  - *Novell eDirectory*
  - Cliente VPN
  - *Citrix* e *Terminal Server*
  - *Radius* (*5ntermedia message*)
  - Autenticação de utilizadores no acesso (802.1x, portal cativo)
- PKI e certificados:
  - Certificados X.509
  - Suporte SCEP
  - Criação de *Certificate Signing Request* (CSR)
  - Autorrenovação de certificados antes da data de expiração
  - Suporte OCSP
- Autenticação de 2 fatores
  - Servidor integrado de autenticação por *tokens* físicos, *tokens* por *software* e SMS
  - Integração com terceiras partes
- Identificação de dispositivos
  - Reconhecimento de dispositivo e sistema operativo
  - Classificação automática de dispositivos

- Gestão de inventário de dispositivos
- Suporte de autenticação e *bypass* feitos por *MAC Address*

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

2.1.3 Firewall

As seguintes funcionalidades deverão ser suportadas:

- Modos de operação NAT/*route* e transparente/*bridge*
- Agendamento de políticas: recorrentes ou apenas uma vez
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT transversal,
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por pares de interfaces
- Definição de objetos para utilização em políticas incluindo: predefinidos, customizados, agrupamento de objetos, *tagging* e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, *Subnet*, intervalo de Ips, Geografia e FQDN
- Utilização de objetos de serviços Internet (ex: *Azure*, *Office365*) com atualização automática das gamas de IP e portos.
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, *Full Cone* NAT, STUN
- *Traffic shaping* e QOS: *shaping* de tráfego partilhado por política, *shapping* por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de *Type of Service* (TOS) e *Differentiated Services* (DiffServ)
- Processamento de tráfego de *firewall* IP4 e Ipv6 feito em processador dedicado e desenhado para o efeito.

2.1.4 VPN

As seguintes funcionalidades deverão ser suportadas:

- IPSEC VPN:
  - Suporte para *peers* remotos: clientes *dialup* compatíveis com IPSEC, *peers* com IP estático ou DNS dinâmico
  - Mecanismos de autenticação: certificados ou *pre-shared key*
  - Opções de aceitação de *peers*: qualquer ID, ID específico, ID num grupo de utilizadores *dialup*
  - Suporte de IKEv1, IKEv2 (RFC 4306)
  - Suporte de IKE *mode configuration* (como servidor ou cliente)
  - Phase 1/Phase 2 *Proposal encryption*: DES, 3DES, AES128. AES192, AES256
  - Phase 1/Phase 2 *Proposal authentication*: MD5, SHA1, SHA256, SHA384, SHA512
  - Phase 1/Phase 2 *Diffie-Hellman Group support*: 1, 2, 5, 14
  - Suporte *Xauth* como cliente ou servidor
  - *Xauth* para *7nterme dialup*: *Server type option* (PAP, CHAP, Auto), NAT *Traversal option*
  - Duração configurável da chave de encriptação IKE e da frequência do NAT *traversal keepalive*
  - *Dead peer detection*
  - *Replay detection*
  - *Autokey keep-alive na Phase* 2 SA
- Implementação de VPNs IPSEC nos seguintes modos: *gateway-to-gateway*, *hub-and-spoke*, *full mesh*, *redundant-tunnel*, terminação de VPNs em modo transparente
- Suporte ADVPN
- Suporte de configuração *full-mesh* VPN *One-click*
- Opções de configuração de VPNs IPSec: baseado em *routing* (*route-based*) ou baseado em políticas (*policy-based*)

- VPNs SSL
    - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (*bookmarks*) mecanismos de ligação, *download* de cliente
    - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
    - Atalhos (*bookmarks*) com single *sign-on*: permite reutilizar um *login* anterior ou credenciais pré-definidas para aceder a recursos internos
    - Gestão de atalhos (*bookmarks*) pessoais
    - Gestão de utilizadores concorrentes
    - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
    - Suporte de VPN SSL em modo *web*:
        - Para clientes remotos equipamentos apenas com um *browser web*
        - Disponibiliza suporte *web* para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix
    - Suporte para VPN SSL em modo túnel:
        - Para acesso a partir de computadores que necessitam utilizar qualquer *software* do tipo cliente-servidor.
        - Disponível para MAC OSX, Windows, IOS, Android e Windows Mobile
    - Validação da integridade do dispositivo cliente e do sistema operativo;
    - Opção para limpeza de *cache* aquando da terminação da sessão VPN SSL
    - Opção de utilização de *desktop* virtual que permite isolar a sessão VPN SSL no ambiente de trabalho do computador cliente
- Monitorização de VPNs IPSec e SSL com diferentes níveis de detalhe
- Suporte para outras VPNs como L2TP (modo cliente e servidor), L2TP over IPSec, PPTP e GRE over IPSec

- Processamento de tráfego de IPSec feito em processador dedicado e desenhado para o efeito.

2.1.5 IPS – Deteção e prevenção de intrusões

As seguintes funcionalidades deverão ser suportadas:

- Suporte de IPS, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (*push* ou *pull*), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados
- Diferentes ações de IPS: definido por defeito na assinatura, monitorizar, bloquear, *reset* de sessão ou quarentena (IP do atacante, IP de atacante e vítima, interface de entrada) com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS especificas com base em Ips
- Proteção DoS sobre Ipv4 e Ipv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer
- Possibilidade de criar novas assinaturas

2.1.6 Controlo de aplicações

As seguintes funcionalidades deverão ser suportadas:

- Deteção de mais de 3000 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas
- Controlo avançado de aplicações de IM e Facebook
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco, e/ ou protocolo)

- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade
- Deteção de aplicações mesmo dentro de ligações proxy
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização, aplicação de gestão de largura de banda
- Inspeção SSL

2.1.7 Proteção contra ameaças

As seguintes funcionalidades deverão ser suportadas:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, filtragem WEB e DLP
- Capacidade de desencriptação de sessões SSL com cópia de tráfego desencriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Deteção e bloqueio de BOTNETs com base em listas de reputação de Ips globais;
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP
- Suporte de anti-vírus em modo proxy, incluindo:
    - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
    - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
    - Listas de ficheiros autorizados/negados

- Opção de análise heurística

- Integração com solução de Sandboxing (cloud ou on-premises)
- Deteção de sites WEB (web filtering):
  - Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS)
  - Possibilidade de definição manual de filtragem sites com base em URL, conteúdo web e cabeçalho MIME
  - Categorização dinâmica em tempo real, baseada na cloud.
  - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
  - Deverá ser possível ter a opção para activar as seguintes funcionalidades:
    - Filtrar Java Applet, ActiveX e/ou cookies
    - Bloquear HTTP Post
    - Registar termos/palavras utilizados nas pesquisas em motores de busca
    - Identificar imagens pelo URL
    - Bloquear redirect de HTTP de acordo com a categoria
    - Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
    - Definição de quotas de utilização WEB com base em categorias
  - Definição de categorias customizada e sobreposição de categorização
  - Mecanismos de exceção à utilização de perfis pré-definidos;
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação,

bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS

- Prevenção e proteção de fugas de informação – DLP
  - Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
    - Possibilidade de executar as acções: registar, bloquear, quarentena de utilizador/IP/Interface
    - Filtros pré-definidos incluindo cartões de crédito e número de segurança Social
  - Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
    - Opções de filtragem disponíveis, tais como tamanho, tipo de ficheiro, watermark, conteúdo e deteção de encriptação
  - Utilização de mecanismos de DLP watermarking, com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
  - Fingerprinting de ficheiros
  - Arquivamento de ficheiros detetados para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB
- Integração nativa com plataformas externas de filtragem de email, sandbox e WAF
- Feeds de ameaças por Domain Name e/ou IP Address

2.1.8 Alta disponibilidade

As seguintes funcionalidades deverão ser suportadas:

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover)
  - Monitorização de portas e links (locais e remotos)

- Sem perda de sessões
- Failover em menos de 1 segundo
- Notificações de eventos de failover

- Diferentes opções de arquitetura
  - HÁ com agregação de links
  - Full mesh HÁ
  - Suporte para HÁ com equipamento geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico.

2.1.9 Administração, Monitorização e Diagnósticos

As seguintes funcionalidades deverão ser suportadas:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica
- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: português, inglês, espanhol, francês, japonês, chinês simplificado, chinês tradicional e Coreano
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.
- Integração com outras soluções (incluído de terceiras partes) através de scripts CLI e APIs.

- Wizards de configuração para implementação rápida da solução.
- Integração com soluções de Public SDN:
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform (GCP)
- Integração com solução de Private SDN:
  - Kubernetes
  - Vmware ESXi

2.1.10 Registo de eventos e relatórios

As seguintes funcionalidades deverão ser suportadas:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195)
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless
- Opção para registo encurtado ou completo de eventos
- Resolução de nomes de endereços Ips e protocolos
- Mecanismo nativo de visualização de eventos de forma estática, com ferramentas de busca e drill-down disponível através de recurso com web browser.

2.1.11 Certificações

Os equipamentos deverão ter no mínimo as seguintes certificações:

- Certificação: ICSA Labs: Firewall, Ipsec, IPS, Antivirus, SSL-VPN, Ipv6

2.1.12 Conectividade

As seguintes interfaces mínimas deverão ser asseguradas:

- Interfaces 10G SFP+ Slots: 4
- Interfaces 1GbE SFP Slots: 8
- Interfaces GbE 10/100/1000: 16
- GE RJ45 Management / HA Ports: 1
- Console Port (RJ45): 1
- Fornecer SFP 10Gbps: 4 (2 por máquina)

2.1.13 Desempenho

As seguintes características mínimas deverão ser asseguradas:

- Aceleração do tráfego de Firewall e IPSec por hardware: Hardware dedicado
- Aceleração de tráfego NGFW por hardware: Hardware dedicado
- Débito firewall Ipv4 (pacotes UDP de 1518 / 512 / 64 bytes): 27 / 27 / 11 Gbps
- Latência de firewall (pacotes UDP de 64 bytes): 4.78 µs
- Débito firewall (pacotes por segundo): 16.5 Mpps
- Sessões TCP concorrentes: 3 Milhões
- Novas sessões/15nterme (TCP): 280.000
- Políticas de firewall: 10.000
- Débito VPN IPSec (pacotes 512 bytes): 13 Gbps
- Túneis Ipsec Gateway-to-Gateway: 2.500
- Túneis IPSec cliente 15nterm: 16.000
- Débito VPN SSL: 2 Gbps
- VPN SSL – Máximo recomendado de utilizadores simultâneos: 500

- Débito IPS: 5 Gbps
- Débito de inspeção SSL: 3.5 Gbps
- Inspeção SSL CPS (IPS, HTTPS diversas cifras): 3.500
- Débito de inspeção SSL para sessões concorrentes: 300.000
- Débito de Application Control: 13 Gbps
- Débito NGFW: 3.5 Gbps
- Débito Threat Protection: 3 Gbps
- Domínios Virtuais (por defeito / máximo): 10 / 10
- Máximo de Tokens: 5.000
- Licenciamento ilimitado de utilizadores: SIM

2.1.14 Garantia e Suporte

Os equipamentos a fornecer deverão ter garantia e suporte 24x7, a ser providenciado diretamente pelo fabricante, pelo período de 3 anos. Durante o período do contrato deverá ser disponibilizado o acesso a updates de software, documentação e suporte técnico por telefone ou Web.

2.2 Appliance virtual para recolha de logs e eventos

Pretende-se a implementação de uma appliance no formato virtual para recolha de log's e eventos centralizados da solução a implementar, devendo esta possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

2.2.1 Relatórios e Ferramentas de Visualização

As seguintes funcionalidades deverão ser suportadas:

- Visualização e filtragem dos Top Users utilização das VPNs
- Visualização dos endereços dos destinos, sites web e ameaças
- Deverá ter por omissão vários modelos de relatórios tipo
- Relatórios com o sumário do UTM e Tráfego
- Capacidade de monitorizar e alertar o administrador de TI sobre eventos importantes
- Capacidade de Importar/Exportar modelos de relatórios já criados para repositório de logs e eventos.

2.2.2 APIs JSON e XML (Serviços Web)

As seguintes funcionalidades deverão ser suportadas:

- Suporte para APIs:
  - JSON API – Permite MSSPs e grandes empresas manipularem os relatórios do colector de logs e eventos, charts/datasets e objetos
  - XML API – Permite aos administradores aprovisionarem/configurarem o colector de logs e eventos e gerar relatórios

2.2.3 Visualização de Logs

As seguintes funcionalidades deverão ser suportadas:

- Visualização de Logs em tempo real ou por histórico
- Visualizar pelo tipo de tráfego ou por logs de segurança
- Visualizar pelo tipo de device, ADOM
- Filtragem de Logs
- Visualização de Logs de forma granular
- Apresentação dos Logs com pictogramas das bandeiras do países e aplicações
- NOC View
- Capacidade IoC (Indicator of Comprimise)

2.2.4 Gestão de Eventos

As seguintes funcionalidades deverão ser suportadas:

- Criar alertas de forma simples
- Desencadear alertas consoante o nível de severidade, eventos específicos, por tipo de ações e destinos
- Definir vários limites pelo número de eventos por um determinado tempo
- Visualizar ou procurar alertas através do histórico
- Notificar por email/SNMP ou enviar eventos por syslog

2.2.5 Capacidade

As seguintes características mínimas deverão ser asseguradas:

- Devices/ ADOMs/ VDOMs Suportados (Máximo): 10.000

- Capacidade de armazenamento (Mínimo / Máximo): 500 GB / +100 TB
- GB/Dia de Logs (Mínimo / Máximo): 1 GB / +2 TB

2.2.6 Máquina Virtual

- Suporte de Hypervisor:
  - Vmware ESX/ESXi;
  - Microsoft Hyper-V;
- Suportar vCPU (Mínimo / Máximo): 2 / Unlimited
- Suporte de Memória (Mínimo / Máximo): 4 GB / Unlimited
- Interfaces de rede (Mínimo / Máximo): 1 / 4
- Serviço Indicator of Compromise (IOC): Sim

2.2.7 Licenciamento

Deverá ser assegurado o licenciamento mínimo para:

- 10 GB/ Dia para Log's;

2.2.8 Suporte

A solução devera ter suporte por parte do fabricante pelo período de 3 anos 24x7.

SERVIÇO DE VPN

3. Indicamos as necessidades para o serviço de VPN

#	Item
3.1 Clientes VPN	• Clientes VPN para instalação nos computadores dos colaboradores; • Capacidade para ZTNA; • Deverá incluir um sistema de gestão centralizada para efetuar *deploys* massivos dos clientes VPN, realizar atualizações de versões e validar ocorrências nos computadores;
3.2 Tokens MFA	• *Tokens* para dupla autenticação na VPN (opcionais)
3.3 Solução de gestão de	• *Appliance* virtual para gestão e configuração de acesso à rede

#	Item
acesso à rede	
3.4 Instalação e configuração	• Instalação e configuração

3.1 Clientes VPN

Elencamos com mais detalhe as caraterísticas e funcionalidades dos clientes VPN e sistema de gestão centralizada.

3.1.1 Requisitos de sistema de gestão centralizada

As seguintes funcionalidades deverão ser suportadas:

- Suporte para instalação em Windows server 2019;
- Suporte para gestão de clientes, pelo menos, em Windows, Mac, Linux, IOS e Android;
- Suporte para ZTNA;

3.1.2 Aprovisionamento

As seguintes funcionalidades deverão ser suportadas:

- Inventário de software instalado nas máquinas cliente;
- Integração com Windows AD;
- Informação do endpoint em tempo real;
- Painel de vulnerabilidades;
- Aprovisionamento e distribuição centralizada de software;
- Atribuição automática de grupos;
- Telemetria em tempo real do endpoint;
- Controlo de acesso dinâmico para imposição da conformidade, criando grupos que podem ser utilizados por uma NGFW para controlos de acesso dinâmicos;
- Resposta automatizada sem intervenção manual;
- Split Tunnel baseado em aplicações
- Filtros Web com pesquisa por palavra-chave/ filtros de YouTube

3.1.3 Telemetria e monitorização

As seguintes funcionalidades deverão ser suportadas:

- Informação do cliente (versão do cliente, Sistema Operativo, IP, MAC address, perfil assignado, avatar do utilizador);
- Envio de relatório de estado para plataforma externa;

3.1.4 Segurança do cliente e componente VPN

As seguintes funcionalidades deverão ser suportadas:

- Funcionalidade de filtragem web;
- Suportar Ipsec VPN;
- Suportar SSL VPN;
- Controlo de equipamentos USB;
- Possibilidade de ligar à VPN antes do login no Windows;
- Sistemas operativos:
  - Windows 10 (32 bits e 64 bits) ou posterior;
  - Windows server 2016 ou posterior;
  - Mac OS;
  - iOS;
  - Android;
  - Ubuntu ou Debian.

3.1.5 Licenciamento e Suporte

A solução deverá ter suporte 24x7 e licenciamento por parte do fabricante, válidos por um período mínimo de 3 anos.

3.2 Tokens MFA

Elencamos com mais detalhe as caraterísticas e funcionalidades dos tokens MFA (multifactor authentication), associados aos clientes VPN:

- Atribuição de token a cada colaborador, que deverão ser geridos a partir da plataforma de gestão de acessos à rede, indicado no ponto 3.3;

- A autenticação de dois fatores deverá ser realizada no mínimo através de email, SMS e mobile, através da instalação de uma aplicação móvel, no mínimo em IOS e Android, para geração aleatória do código multifator;
- Aquisição opcional dos tokens durante a vigência do contrato;
- Deverão indicar na proposta se os tokens são vendidos separadamente ou em pacotes com quantidade mínima. Caso seja em pacotes, deverão indicar a quantidade de tokens por pacote e o seu valor.

3.3 Solução de gestão de acesso à rede

Pretende-se a implementação de uma solução, em formato de appliance virtual, que permita adicionar mecanismos de segurança relativamente à forma como os utilizadores se ligam à sua rede.

3.3.1 Funcionalidades mínimas

- Suporte para mínimo de 2100 autenticações em simultâneo;
- Integração com Microsoft AD e LDAP;
- Controlo de acessos 802.1X para redes wired e wireless;
- Realizar identificação através dos seguintes métodos:
  - Active Directory Polling;
  - Agente de Single Sing-On;
  - Authenticação através de portais web;
  - RADIUS 21ntermedia login;
- Realizar gestão de tokens para realização de autenticação de dois fatores, através de email, sms e mobile push;
- A solução deverá incluir 150 licenças de agentes para funcionalidades de SSO;
- Permitir realizar funções de root e 21ntermediar Certificate Authority;
- Realizar gestão de utilizadores Guests e BYOD;
- SAML SP/IdP web SSO;
- Suporte para SNMP v1, v2 e v3;
- Incluir informação gráfica sobre as autenticações com sucesso e insucesso;

- Deverá realizar log de todos os eventos localmente ou através de syslog;
- Deverá suportar políticas de "lock-out" por um determinado tempo, caso se atinga um número máximo de tentativas falhadas na autenticação;
- Deverá providenciar mecanismos de "self-registration", com e sem aprovação.
- Integração com as seguintes plataformas para realização de Social login: Facebook, Google+, Linkedin e Twitter;
- RFC Compliance: RFC 2865; RFC 1305; RFC 4510; RFC 5280; RFC 2716; RFC 3280; RFC 2986; RFC 2560
- Suporte do fabricante para 3 anos 24x7.

SISTEMA DE REDE WIFI

4. Indicamos as necessidades para o serviço de access point para distribuição de rede wifi

#	Item
4.1 AP´s	• Equipamentos de rede wifI com adaptador de teto
4.2 Instalação e configuração	• Configuração dos AP´s na firewall a adquirir • A instalação deverá, preferencialmente, estar concluída no prazo de 3 meses a contar do início da vigência do contrato. Sistema não critico

4.1 AP´s

Sendo uma parte fundamental da rede, em particular do acesso dos dispositivos à Rede, os Access Points (APs) a fornecer deverão respeitar uma série de normas e requisitos com vista a permitir não só uma conexão dos dispositivos móveis de forma segura, mas também uma elevada eficiência, performance e escalabilidade. Em particular, e por forma a estar o mais independente da arquitetura central a instalar, os Aps devem poder funcionar de diversas formas, nomeadamente:

- Gerido através de uma firewall;
- Gerido através de uma plataforma cloud

Por forma a assegurar uma boa eficiência aplicacional e Segurança, cada um dos Aps deve ser capaz de suportar o mínimo de 16 SSIDs.

No mesmo SSID deve ser possível implementar:

- Políticas de controlo de acesso;
- Gestão do espectro RF;
- Deteção de Rogue AP;

É considerada fundamental a possibilidade de extração de dados de tráfego ao nível do Access Point por forma a gerar estatísticas, acessos, relatórios e obter a informação sobre o uso da rede. Assim, a solução a propor deve disponibilizar, à partida:

- Visibilidade do tipo de tráfego e aplicações utilizadas na rede wireless;
- Tipo de clientes que se estão a ligar na rede:
    - Tipo de dispositivo;
    - Sistema operativo;
- Perfis de serviço com determinação de:
    - Largura de banda máxima por SSID ou utilizador;
    - Tipos de aplicações e categorias autorizadas;
    - Ips e domínios de destino autorizados;
- Funcionalidade de modo de análise de espectro nas bandas 2,4GHz e 5GHz
- A solução deverá possibilitar a integração com tecnologias de localização de equipamentos (Asset Tracking)

4.1.1 Especificações técnicas dos AP's

Os Aps a fornecer no âmbito deste procedimento deverão ter as seguintes características:

- AP de interior, rádio triplo 802.11ax
- Radio 1: até 574 Mbps,
- Radio 2: até 1200 Mbps
- Interfaces:
    - 2× 10/100/1000Base-T

- Antena
  - Antenas omnidirecionais integradas para o MIMO 2x2, com ganho máximo de antena de 4.5dBi em 2,4 GHz e 5.5 dBi em 5 GHz. As antenas integradas deverão ser otimizadas para orientação horizontal do ponto de montagem no teto.
  - Antena BLE integrada com potência de transmissão de até 4dBm
- Segurança
  - 802.11i
  - Wi-Fi Protected Access 2/3 (WPA2/3)
  - 802.1X
  - WEP, TKIP
  - WIDS/WIPS
  - Portal page authentication
- Standards IEEE
  - IEEE 802.11a/b/g/n/ac/ax
  - IEEE 802.11e
  - IEEE 802.11h, 802.11i,
  - 802.11k Radio Resource Management
  - 802.11v BSS Transition Management
  - 802.11r Fast Roaming
- Certificação Wi-Fi Alliance

OUTROS SERVIÇOS

5. Indicamos as necessidades para outros serviços associados a este contrato

#	Item
5.1 Simulador de Phishing	• Serviço de simulação de phishing a 150 colaboradores (formato cloud), podendo escolher o tipo de ameaça, colaboradores de destino e agendar o ataque simulado. Capacidade para analise e identificar utilizadores de risco.

#	Item
5.2 WAF	• Appliance virtual para serviço de publicação de portais (tipo WAF)
5.3 Suporte	• Horas mensais de suporte adicional
5.4 Instalação	• Instalação e configuração dos serviços indicados acima no ponto 5 • A instalação deverá estar concluída no prazo de 3 meses a contar do início da vigência do contrato.

5.2 WAF

Elencamos as principais caraterísticas que a solução virtual (do tipo WAF) para serviço de proxy ou balanceamento para publicação de portais e/ou serviços para a internet, que permita reduzir o número de IP´s públicos utilizados, deve ter:

Especificação técnica	Valor
Sistema Virtual	
Hypervisors suportados	VMware, Microsoft Hyper-V, Open Source Xen, Virtualbox, KVM, Amazon Web Services (AWS), Microsoft Azure,
vCPUs suportados (Máximo)	2
vNICs suportados (Máximo)	10
Armazenamento interno (Mínimo/ Máximo)	40 GB / 2 TB
Memória suportada (Mínimo/ Máximo)	1.024 MB / Unlimited for 64-bit
Alta-Disponibilidade	Ativo/Standby, Ativo/Ativo
Desempenho do sistema	
Débito HTTP	100 Mbps
Domínios de Administração (Máximo)	64
Licenciamento ilimitado de aplicações	SIM

5.2.1 Modos de integração em rede

As seguintes funcionalidades deverão ser suportadas:

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

- WCCP

5.2.2 Segurança Web

As seguintes funcionalidades deverão ser suportadas:

- AI-based Machine Learning
- Profiling automático (white Lists)
- Assinaturas de servidor web e aplicações (black list)
- Reputação de IPs
- Geolocalização de IPs
- Validação de compliance com RFC de HTTP
- Suporte nativo para HTTP/2
- Verificação de OpenAPI 3.0
- Proteção de WebSocket e enforcement de assinaturas
- Proteção de ataques do tipo Man in the Browser (MiTB)

5.2.3 Proteção contra ataques aplicacionais

Os seguintes ataques deverão ser mitigados:

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Integração com Third-party scanner (virtual patching)
- Análise de ficheiros com antivírus e sandbox

5.2.4 Serviços de segurança

As seguintes funcionalidades deverão ser suportadas:

- Assinaturas de serviços Web
- Conformidade de protocolos XML e JSON
- Deteção de malware

- Patching virtual
- Validação de protocolos
- Proteção contra ataques do tipo Brute force
- Assinatura e encriptação de cookies
- Pontuação e ponderação de ameaças
- Deteção de ataques SQLi baseados na syntax
- Segurança dos headers de HTTP
- Gestão de mensagens e códigos de erro customizados
- Assinaturas de deteção de Sistema operativo
- Proteção contra ataques conhecidos e do tipo zero-day
- Stateful Firewall L4
- Prevenção de ataques DoS
- Mecanismos de proteção avançada com recurso a múltiplos elementos de segurança
- Proteção contra fugas de informação
- Proteção contra web defacement

5.2.5 Balanceamento aplicacional

As seguintes funcionalidades deverão ser suportadas:

- Balanceamento de servidores L7
- Reescrita de URLs
- Routing aplicacional baseado em conteúdos
- Offloading de HTTPS/SSL
- Compressão de HTTP
- Caching de conteúdos

5.2.6 Autenticação

As seguintes funcionalidades deverão ser suportadas:

- Autenticação ativa e passiva
- Publicação de sites e SSO (Single sign-on)

- Acesso RSA para autenticação de 2 fatores
- Suporte para LDAP, Radius e SAML
- Suporte para certificados cliente
- CAPTCHA e Real Browser Enforcement (RBE)

5.2.7 Gestão e Reporting

As seguintes funcionalidades deverão ser suportadas:

- Acesso de gestão através de interface gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica
- Ferramentas gráficas de análise e reporting
- Suporte para gestão centralizada de múltiplos equipamentos
- Suporte para Alta Disponibilidade Ativo/Ativo
- RESTful API
- Suporte para Logging e Reporting centralizado
- Identificação e rastreamento de utilizadores/dispositivos
- Dashboards para visualização de informação em tempo real
- Dashboards para Bots
- Categorização de ataques OWASP Top 10
- Analítica de informação de geolocalização de IPs
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, Syslog e Email (Logging e monitorização)
- Suporte de domínios administrativos com controle de acesso baseado em funções (RBAC)

5.2.8 Integração em redes

As seguintes funcionalidades deverão ser suportadas:

- VLANs (802.1Q) e agregação de portas(802.3ad)
- Support de IPv6

- Alta disponibilidade activo-passivo e activo-activo
- Tradução de HTTP/2 para HTTP 1.1
- Integração com plataformas HSM
- Integração simplificada com plataformas PKI
- Análise de anexos em aplicações ActiveSync/MAPI, Outlook Web Access e FTP
- Alta disponibilidade com sincronização de configurações entre múltiplos dispositivos ativos
- Deve permitir a configuração automatizada e incluir definições por defeito para instalação simplificada
- Deve incluir wizards de configuração para aplicações e bases de dados comuns
- Mecanismos de auto-aprendizagem
- Deve incluir por defeito alguns perfis de inspeção e proteção
- Pré-configurado para aplicações Microsoft, como Exchange, OWA e Sharepoint
- Deve incluir políticas de segurança pré-definidas para aplicações Drupal e Wordpress
- Suporte de OPENSTACK
- Suporte de Websockets

5.3 Suporte

Bolsa de horas para suporte a todo o serviço prestado no contrato.

SUPORTE, GARANTIA E NÍVEIS DE SERVIÇO

6. Identificamos requisitos de suporte, garantia do serviço e equipamentos, níveis de serviço e obrigatoriedades.

#	Item
6.1	• Deverá ser atribuído à ADENE um Gestor de Conta que a represente diretamente em todos os assuntos comerciais e técnicos

#	Item
6.2	• A ADENE deverá dispor de um serviço de suporte (helpdesk) operacional
6.3	• Assegurar a disponibilidade anual do serviço de internet no mínimo de 99,90%, independentemente da opção tecnológica adotada devendo, se necessário, incluir mecanismos de securitização dos serviços
6.4	• Todos os equipamentos (físicos ou virtuais) devem ter suporte do fabricante para os 3 anos de contrato
6.5	• Todos os equipamentos e software indicados no ponto 2, 3, 4 e 5 deverão pertencer ao mesmo fabricante. Pretende-se uma solução integrada que permita fazer todas ou quase todas as configurações na mesma consola ou *backoffice*. Os equipamentos e software propostos devem ter uma gestão simplificada e de fácil manutenção. • Todo o sistema de firewall, equipamentos de wifi, configurações de VPN, sistema de publicação e controlo de portais web devem poder ser geridos por uma consola centralizada.
6.5	• Garantir que o tempo médio anual de reposição do serviço de internet afetado após participação da anomalia por parte da entidade adjudicante não excede o máximo de 4 (quatro) horas seguidas.