CONCURSO LIMITADO POR PRÉVIA QUALIFICAÇÃO COM PUBLICIDADE INTERNACIONAL

AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA LÓGICA INTERNA E EXTERNA

2023_040CLPQ

CADERNO DE ENCARGOS

AGOSTO DE 2023

ÍNDICE

CAPÍTULO I
DISPOSIÇÕES GERAIS

Cláusula 1.ª
Objeto

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato de **Aquisição de Solução de Segurança Lógica Interna e Externa** e respetivos serviços de instalação e configuração, migração das plataformas atuais e serviços de manutenção e suporte, a celebrar entre a **AdP VALOR – Serviços Ambientais, S.A.** (doravante **AdP VALOR**) e o **Cocontratante**.

Cláusula 2.ª
Contrato

1. O contrato integra os seguintes elementos:

a) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelos concorrentes e expressamente aceites pelo órgão competente para a decisão de contratar, nos termos do disposto no artigo 50.º do Código dos Contratos Públicos;

b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;

c) O presente Caderno de Encargos e os seus anexos;

d) A proposta;

e) Os esclarecimentos prestados sobre a proposta adjudicada.

2. Sem prejuízo do disposto no número seguinte, em caso de divergência entre os vários documentos que integram o contrato, a prevalência é determinada pela ordem por que vêm enunciados no número anterior.

3. Os ajustamentos propostos pela **AdP VALOR** nos termos previstos no artigo 99.º do Código dos Contratos Públicos e aceites pelo **Cocontratante** nos termos previstos no artigo 101.º do mesmo diploma legal prevalecem sobre todos os documentos previstos no n.º1 da presente cláusula.

Cláusula 3.ª

Prazo contratual

Sem prejuízo da manutenção das obrigações acessórias que perdurem para além do seu termo, o contrato a celebrar é válido desde a data da celebração até à data de conclusão dos trabalhos.

CAPÍTULO II

OBRIGAÇÕES DAS PARTES

SECÇÃO I

OBRIGAÇÕES DO COCONTRATANTE

Cláusula 4.ª

Obrigações do Cocontratante

1. Sem prejuízo de outras obrigações previstas na legislação aplicável e no presente Caderno de Encargos e respetivos anexos, constituem obrigações principais do **Cocontratante** as seguintes:

a) Proceder ao desenvolvimento de uma Solução de Segurança Lógica Interna e Externa de acordo com as especificações técnicas indicadas no **ANEXO I** ao presente Caderno de Encargos;

b) Serviços de Instalação e configuração da respetiva Solução;

c) Efetuar a Migração das plataformas atualmente em funcionamento;

d) Serviços de Manutenção e Suporte;

e) Disponibilizar todos os documentos que sejam necessários para boa e integral utilização de funcionamento da solução implementada;

f) Comparecer a todas as reuniões de trabalho que sejam agendadas pela **AdP VALOR**;

g) Comunicar à **AdP VALOR**, logo que tenha conhecimento, os factos que tornem total ou parcialmente impossível a prestação dos serviços objeto do contrato ou o cumprimento de qualquer das suas obrigações, nos termos do contrato celebrado;

h) Recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução do contrato;

i) Não subcontratar, no todo ou em parte, a execução do objeto do contrato, sem prévia autorização da **AdP VALOR**;

j) Comunicar qualquer facto que ocorra durante a execução do contrato e relacionados com a sua denominação social, os seus representantes legais, a sua situação jurídica, a sua situação comercial e outras, com relevância para o fornecimento;

k) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenha no âmbito da formação e da execução do contrato, não utilizando as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos.

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

Cláusula 5.ª
Local da instalação

A execução do contrato será realizada nos seguintes locais:

a) Edifício Sede da AdP: Rua Visconde Seabra, 3, 1700-421 Lisboa
b) Centro de Desastre: Lugar de Gaído – Barcelos, 4755-045 Areias de Vilar

Cláusula 6.ª
Fases de execução contratual

1. A implementação e respetivos serviços objeto do presente Caderno de Encargos compreende as seguintes 3 (*três*) fases e respetivas atividades, devidamente discriminadas no presente Caderno de Encargos, e que dele faz parte integrante:

a) **FASE 1**:
   i. Atividades Preparatórias;
   ii. *Kick Off* (apresentação do planeamento do projeto, riscos e equipa).

b) **FASE 2**:
   iii. Implementação da solução em ambos os sites;
   iv. Realização de testes integrados e de aceitação;
   v. Formação na vertente técnica;
   vi. Manuais na vertente técnica;
   vii. Arranque da Solução em Produtivo;

c) **FASE 3**:

viii. Suporte após o arranque da Solução;

ix. Garantia;

2. A execução do objeto do contrato a celebrar deve observar as especificações técnicas constantes no **ANEXO I** ao presente Caderno de Encargos e que dele faze parte integrante.

3. Cada uma das fases indicadas no n.º 1 da presente cláusula, encontrar-se-ão **concluídas,** de acordo com os seguintes termos:

a) **FASE 1** – Após a conclusão da etapa *ii.* da alínea *a*) do n.º 1 da presente cláusula e respetiva aceitação pelo Gestor de Contrato.

b) **FASE 2** – Após a conclusão de todas as etapas *iii.* a v*ii.*, conforme preconizado na alínea *b*) do n.º 1 da presente cláusula e respetiva aceitação pelo Gestor de Contrato, reconhecendo assim estarem reunidas condições para o respetivo *Arranque da Solução em Produtivo*, conforme previsto na etapa *viii.* da mesma alínea, que se inicia no dia seguinte à assinatura do auto de aceitação.

c) **FASE 3** – Após o término do período de 3 (*três*) anos, contados do dia do *Arranque da Solução em Produtivo*, conforme previsto na etapa *vii* da alínea *b*) do n.º 1 da presente cláusula.

Cláusula 7.ª
Prazos de execução

1. A execução do contrato deve ser realizada de acordo com as fases previstas na cláusula 6.ª do presente caderno de encargos e tendo em conta os seguintes prazos:

a) **FASES 1 e 2**: devem estar concluídas no prazo máximo de 2 (*dois)* meses a contar da data de assinatura do contrato.

b) **FASE 3**: terá a duração de 3 *(três)* anos após o *Arranque da Solução em Produtivo*.

Cláusula 8.ª
Equipa a afetar à execução do contrato

1. Para a execução dos serviços que lhe venham a ser solicitados durante a vigência do contrato, o **Cocontratante** deve afetar à execução dos mesmos elementos com formação técnica, académica e experiência profissional adequadas à boa execução da natureza das tarefas a realizar, nos termos dos números seguintes.

2. A equipa do **Cocontratante** deverá ser composta pelo menos por 1 (*um*) técnico certificado, em pelo menos 3 (*três*) das 4 (*quatro*) competências técnicas das principais áreas de integração da solução:

a) Técnico certificado em tecnologia Check Point (mínimo, CCSM-E) (**obrigatório**);

b) Técnico certificado em tecnologia Cisco;

c) Técnico certificado em tecnologia VMWare;

d) Técnico certificado na tecnologia proposta (mínimo nível 7) (**obrigatório**).

3. Durante a execução do contrato, a **AdP VALOR** pode solicitar ao **Cocontratante** a substituição dos elementos da equipa afeta ao contrato, mediante decisão justificada e comunicada com uma antecedência de 5 (*cinco*) dias em relação à data de produção de efeitos da substituição.

4. Caso, por motivo devidamente justificado e aceite pela **AdP VALOR**, o **Cocontratante** tenha que designar outro elemento, deve a designação ser instruída com informação relativa à sua formação académica e profissional.

5. Qualquer alteração dos elementos da equipa técnica previstos no n.º 2 da presente cláusula deve observar os requisitos de habilitação e experiência estipulados na proposta adjudicada para a categoria respetiva.

6. A **AdP VALOR** deve afetar uma equipa interna para acompanhamento de todas as atividades da prestação de serviços.

Cláusula 9.ª
Metodologia da prestação de serviços

1. No prazo de 4 (*quatro*) dias a contar da data de celebração do contrato será realizada uma reunião de arranque, destinada à apresentação da equipa de trabalho da **AdP VALOR** e da equipa do **Cocontratante**.

2. Após o início dos trabalhos, serão efetuadas reuniões de ponto de situação, com uma periodicidade semanal, ou outra que, entretanto, se considere mais adequada, que visam aferir a concretização das tarefas das diversas fases de execução contratual, com vista a prestar os esclarecimentos que se considerem necessários.

3. Todos os trabalhos resultantes das fases referidas na cláusula 6ª do presente caderno de encargos devem ser validados e aceites pelo Gestor de Contrato designado pela **AdP VALOR.**

4. No prazo de (até) 5 (*cinco*) dias úteis a contar da data de finalização dos trabalhos referidos em cada fase, o Gestor de Contrato designado pela **AdP VALOR** procede à respetiva análise com vista a verificar se os mesmos se mostram conformes com as instruções e objetivos definidos e às observações resultantes das reuniões de trabalho.

5. No âmbito da análise a que se refere o número anterior, o **Cocontratante** deve prestar à **AdP VALOR** toda a cooperação e todos os esclarecimentos necessários.

6. No caso da **AdP VALOR** não aprovar os trabalhos desenvolvidos pelo **Cocontratante**, fica o mesmo obrigado a proceder, no prazo razoável que for determinado pela **AdP VALOR** e sem quaisquer custos adicionais, às alterações e serviços complementares necessários para garantir o cumprimento das solicitações realizadas.
7. Após a realização pelo **Cocontratante** das alterações e dos serviços complementares necessários no prazo determinado pela **AdP VALOR**, esta procede a nova análise, nos termos do disposto nos números anteriores.
8. Durante os prazos de análise dos trabalhos desenvolvidos, suspende-se o prazo de execução do contrato, mormente o prazo de execução da fase respetiva, iniciando-se no dia seguinte após a resposta da aprovação dos documentos pela **AdP VALOR**.
9. Caso a **AdP VALOR** comprove a conformidade dos elementos entregues pelo **Cocontratante**, comunicará a aprovação dos trabalhos desenvolvidos iniciando-se no dia seguinte a contagem do prazo parcial da fase subsequente.

Cláusula 10.ª
Aceitação da solução implementada

1. Após a conclusão das **FASES 1** e **2** previstas na cláusula 6.ª do presente caderno de encargos e verificando-se a total operacionalidade da solução, bem como a sua conformidade com as exigências legais, e não sejam detetados quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente caderno de encargos e na proposta adjudicada, deve ser emitido, no prazo máximo de 10 (*dez*) dias, um auto de aceitação, assinado pelos representantes do **Cocontratante** e da **AdP VALOR**, conforme **ANEXO II.**
2. Com a declaração de aceitação a que se refere o número anterior, ocorre a transferência da posse e da propriedade do bem para a **AdP VALOR**, incluindo o risco de deterioração ou perecimento do mesmo, sem prejuízo das obrigações de garantia que impendem sobre o **Cocontratante**.
3. A assinatura do auto a que se refere o n.º 1 não implica a aceitação de eventuais defeitos ou de discrepâncias da solução com as exigências legais ou com as características, especificações e requisitos técnicos previstos no presente caderno de encargos.

Cláusula 11.ª
Garantia Técnica

1. O **Cocontratante** garante a solução disponibilizada contra qualquer defeito ou anomalia

no seu funcionamento ou qualquer desconformidade com as Especificações Técnicas definidas no **ANEXO I** ao presente Caderno de Encargos, bem como com outros requisitos injuntivos exigidos por lei, que venham a ser identificados e se justifique a sua exigência durante o prazo de execução do Contrato.

2. A garantia técnica compreende as obrigações de o **Cocontratante** proceder à correção ou eliminação dos defeitos, anomalias ou desconformidades referidas no número anterior, incluindo a obrigação de proceder à reformulação das funcionalidades da solução se outro meio não se revelar apto a assegurar estes resultados.
3. O **Cocontratante** fica obrigado a corrigir qualquer defeito, anomalia ou desconformidade referida no n.º 1, no prazo de 24 (*vinte* e *quatro*) horas a contar da sua comunicação por parte da **AdP VALOR**.
4. O **Cocontratante** deve assegurar uma garantia sobre o funcionamento da solução por um período de 3 (*três*) anos, após a entrada em produção.

Cláusula 12.ª
Patentes, Licenças, Marcas e Equipamentos

1. São da responsabilidade da **Cocontratante** quaisquer encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças.
2. Caso a **AdP VALOR** venha a ser demandada por ter infringido a execução do contrato, qualquer dos direitos mencionados no número anterior, o **Cocontratante** indemniza-a de todas as despesas.
3. Todos os equipamentos entregues têm que ser novos, adquiridos através dos canais oficiais e com suporte assegurado pelo menos em *back-to-back* com os respetivos fabricantes.

Cláusula 13.ª
Dever de sigilo

1. Toda a informação ou documentação relativa às empresas do Grupo Águas de Portugal, oral ou escrita, técnica, comercial ou de índole diversa, transmitida, revelada ou trocada com a **AdP VALOR** ou com qualquer uma das empresas participadas, através dos respetivos administradores, diretores ou trabalhadores, bem como quaisquer outros colaboradores, incluindo prestadores de serviços, é considerada como informação confidencial.
2. A informação confidencial obtida, transmitida ou facultada constitui propriedade da **AdP VALOR** ou das suas empresas participadas, o mesmo se aplicando a todas as cópias que desta vierem a ser efetuadas.

3. O **Cocontratante** obriga-se a não divulgar qualquer informação confidencial relativa à **AdP VALOR** ou empresas do Grupo AdP de que venha a ter conhecimento ao abrigo ou em relação com a execução do contrato.
4. O **Cocontratante** obriga-se a não utilizar as informações obtidas para fins alheios à execução do contrato.
5. O **Cocontratante** compromete-se a não transmitir, de forma completa ou parcial, a terceiros, pessoa singular ou coletiva, qualquer informação confidencial obtida, transmitida ou facultada pelas empresas do grupo AdP, sem o expresso consentimento por escrito da **AdP VALOR**.
6. Quando autorizado a transmitir informação confidencial, total ou parcialmente, a terceiros, o **Cocontratante** deve transmitir e impor-lhes todas as obrigações a que está vinculado pelo presente Caderno de Encargos.
7. O **Cocontratante** deve garantir que todos os seus administradores, diretores, trabalhadores e colaboradores com acesso a informação confidencial têm conhecimento das disposições do presente Caderno de Encargos, incumbindo-lhe zelar pelo cumprimento do mesmo.
8. Não podem ser feitas quaisquer cópias da informação confidencial sem o expresso consentimento por escrito da **AdP VALOR** devendo as que vierem a ser feitas ser classificadas como protegidas e garantidas por obrigações de confidencialidade nos termos previstos no presente Caderno de Encargos.
9. Para efeitos do presente Caderno de Encargos, não é considerada informação confidencial:

    a) Informação que era do domínio público na data da sua transmissão ou divulgação ao **Cocontratante**;

    b) Informação confidencial que se tenha tornado pública depois de revelada pela **AdP VALOR** ou por qualquer uma das empresas participadas, por meio de publicações ou outros meios, designadamente, relatórios de contas ou de atividades, sem que o **Cocontratante** tenha violado o seu dever de confidencialidade;

    c) Informação que o **Cocontratante** já tivesse na sua posse na data da sua transmissão ou divulgação pela **AdP VALOR** ou por qualquer uma das suas empresas participadas, e que não tivesse sido, direta ou indiretamente obtida através de administradores, trabalhadores ou consultores das empresas do grupo AdP;

    d) Informação confidencial obtida licitamente de terceiros, que não tenha sido direta ou indiretamente proveniente de administradores, trabalhadores ou consultores das empresas do grupo AdP;

e) Informação desenvolvida independentemente pelo **Cocontratante**, desde que este, ao desenvolvê-la, não tenha acedido ou utilizado informação confidencial.

10. O ónus da prova quanto à natureza não confidencial da informação prevista na cláusula anterior incumbe ao **Cocontratante**.

11. O **Cocontratante** é responsável pelo cumprimento do dever de sigilo por parte dos seus colaboradores, qualquer que seja a natureza jurídica do vínculo, inclusivamente após a cessação deste, independentemente da causa da cessação.

12. O **Cocontratante** é ainda responsável perante a **AdP VALOR** em caso de violação do dever de sigilo pelos terceiros por si subcontratados, bem como por quaisquer colaboradores desses terceiros.

13. Em caso de incumprimento pelo **Cocontratante** de qualquer uma das obrigações ou garantias decorrentes do presente Caderno de Encargos em matéria de confidencialidade, por efeito de ação ou omissão dos seus responsáveis, trabalhadores, colaboradores ou terceiros, este fica obrigado a pagar à **AdP VALOR** a quantia de € 2.500,00 (*dois mil e quinhentos euros*), por cada incumprimento ocorrido.

14. Para efeitos do número anterior, considera-se que cada informação ou documento transmitido ou utilizado, relativamente a cada uma das empresas beneficiárias e da entidade adjudicante, constitui um incumprimento do estabelecido no presente Caderno de Encargos.

15. Sem prejuízo do disposto nos números anteriores, o **Cocontratante** fica obrigado a indemnizar a **AdP VALOR** por todos os danos e prejuízos sofridos em consequência de tal incumprimento, a par da responsabilidade devida a administradores, trabalhadores ou colaboradores do grupo AdP que tenham sido individualmente lesados, direta ou indiretamente, pelo cocontratante.

16. O **Cocontratante** compromete-se igualmente a substituir a **AdP VALOR** ou a empresa participada do grupo AdP visada em qualquer demanda, litígio, reclamação ou ação judicial propostos ou desencadeados por terceiros em virtude da violação do disposto no presente Caderno de Encargos.

17. O **Cocontratante** obriga-se a remover e destruir no termo final do prazo contratual todo e qualquer registo, em papel ou eletrónico, que contenha dados ou informações referentes ou obtidas na execução do contrato e que a **AdP VALOR** lhe indique para esse efeito.

18. O dever de sigilo mantém-se em vigor até ao termo do prazo de 2 (*dois*) anos após a extinção das obrigações decorrentes do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

19. O **Cocontratante** respeitará os termos relativos ao tratamento, conservação e transferência de dados pessoais constantes deste Caderno de Encargos.

Cláusula 14.ª
Tratamento de Dados Pessoais

1. No caso de o **Cocontratante** necessitar de aceder a dados pessoais no decurso da execução do contrato, deve fazê-lo exclusivamente na medida do estritamente necessário para integral e adequada prossecução dos fins constantes do contrato, na qualidade de subcontratante, e por conta e de acordo com as instruções da **AdP VALOR**, nos termos da legislação aplicável à proteção de dados pessoais.

2. O **Cocontratante** não pode proceder à reprodução, gravação, cópia ou divulgação dos dados pessoais para outros fins que não constem do contrato, ou para proveito próprio.

3. O **Cocontratante** deve cumprir rigorosamente as instruções da **AdP VALOR** no que diz respeito ao acesso, registo, transmissão ou qualquer outra operação de tratamento de dados pessoais.

4. O **Cocontratante** deve proceder à implementação de medidas de segurança de tratamento de dados pessoais e adotar medidas técnicas e organizativas para proteger os dados contra destruição acidental ou ilícita, perda acidental, alterações, difusão ou acesso não autorizados, e contra qualquer outra forma de tratamento ilícito dos mesmos.

5. O **Cocontratante** deve tomar as medidas adequadas para assegurar a idoneidade dos seus trabalhadores ou colaboradores, a qualquer título, que tenham acesso aos dados pessoais fornecidos pela **AdP VALOR**, ou por quem atue em representação deste.

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 **Cocontratante** deve assegurar que o acesso aos dados pessoais é limitado às pessoas que efetivamente necessitam de aceder aos mesmos para cumprir com as obrigações impostas pelo presente Caderno de Encargos e que os trabalhadores, colaboradores ou subcontratados assumiram um compromisso de confidencialidade ou estão sujeitos a adequadas obrigações legais de confidencialidade, e que conhecem e se comprometem a

cumprir todas as obrigações aqui previstas, sendo o **Cocontratante** responsável pela utilização dos dados pessoais por parte dos mesmos.

8. Mediante solicitação escrita da **AdP VALOR**, o **Cocontratante** deve, no prazo de 15 (*quinze*) dias, informar quais as medidas tomadas para assegurar o cumprimento dos deveres referidos nos números anteriores.

9. O **Cocontratante** deve comunicar de imediato à entidade adjudicante quaisquer reclamações ou questões colocadas pelos titulares dos dados pessoais.

10. O **Cocontratante** encontra-se adstrito a notificar de imediato à **AdP VALOR** de qualquer monitorização, auditoria ou controlo por parte de entidades reguladoras/de supervisão de que seja objeto.

11. Se o **Cocontratante** tomar conhecimento, ou suspeitar, de violações de dados pessoais que resultem, ou possam resultar, na destruição acidental ou não autorizada de dados, na perda, alteração, acesso ou revelação não autorizada dos dados, deve notificar, por escrito, à entidade adjudicante disponibilizando-lhe uma descrição da violação de dados ocorrida, informando-o das categorias e número de titulares de dados afetados, das prováveis consequências da violação, assim como fornecer-lhe qualquer outra informação que a entidade adjudicante possa razoavelmente solicitar.

12. Quando se verifique uma violação de dados pessoais, por causas imputáveis ao **Cocontratante**, este compromete-se a adotar as seguintes medidas, sem quaisquer custos adicionais paras a **AdP VALOR**:

a) Tomar de imediato as medidas necessárias para investigar a violação ocorrida, identificar e prevenir a repetição dessa violação, e encetar esforços razoáveis para mitigar os efeitos dessa violação;

b) Desenvolver as ações necessárias para remediar a violação; e

c) Documentar todas as circunstâncias referentes à violação para efeitos de controlo por parte da autoridade de supervisão.

13. O **Cocontratante** obriga-se a ressarcir a **AdP VALOR** por todos os prejuízos em que este venha a incorrer em virtude da utilização ilegal e/ou ilícita de dados pessoais, nomeadamente por indemnizações e despesas em que tenha incorrido na sequência de reclamações ou processos propostos pelos titulares dos dados, bem como por taxas, coimas e multas que tenha de pagar.

14. O incumprimento dos deveres estabelecidos na presente cláusula por parte do **Cocontratante** e a verificação de inexistência de garantias de *compliance* do cocontratante é fundamento de resolução do presente contrato com justa causa pela **AdP VALOR**, podendo implicar o dever de indemnização por eventuais violações que lhe sejam imputadas.

Cláusula 15.ª
Conservação de dados pessoais

1. O **Cocontratante** deve apagar e destruir os dados pessoais tratados quando os mesmos deixarem de ser necessários para a execução do contrato, e sempre em prazo não superior a 1 (*um*) ano após a cessação do contrato que esteve na base da licitude do seu tratamento e de acordo com as instruções dadas pela **AdP VALOR.**

2. Dependendo da opção da **AdP VALOR**, o **Cocontratante** apagará ou devolverá todos os dados pessoais, depois de concluída a execução do contrato, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo da legislação aplicável.

Cláusula 16.ª
Transferência de dados pessoais

O **Cocontratante** não pode transferir quaisquer dados pessoais para outra entidade, independentemente da sua localização, salvo autorização prévia e escrita da **AdP VALOR**, exceto se o **Cocontratante** for obrigado a fazê-lo pela legislação aplicável, ficando obrigado a informar, nesse caso, a **AdP VALOR** antes de proceder a essa transferência.

Cláusula 17.ª
Dever de cooperação

O **Cocontratante** deve cooperar com a **AdP VALOR** ou com qualquer outra empresa do Grupo AdP, mediante solicitação, designadamente nas seguintes situações:

a) Quando um titular de dados pessoais exerça os seus direitos ou cumpra as suas obrigações nos termos da legislação aplicável, relativamente aos dados pessoais tratados pelo **Cocontratante** em representação da **AdP VALOR**;

b) Quando qualquer das empresas do Grupo AdP deva cumprir ou dar sequência a qualquer avaliação, inquérito, notificação ou investigação da Comissão Nacional de Proteção de Dados ou entidade administrativa com atribuições e competências legais equiparáveis.

SECÇÃO II
OBRIGAÇÕES DA ENTIDADE ADJUDICANTE

Cláusula 18.ª
Preço base e preço contratual

1. O preço base contratual não pode ser superior a **€250.000,00** (*duzentos e cinquenta mil euros*), não incluindo o IVA legalmente devido.

2. Pela prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a **AdP VALOR** deve pagar ao **Cocontratante** o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

3. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à **AdP VALOR**, incluindo despesas de alojamento, alimentação, deslocação de meios humanos, despesas de aquisição, transporte, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes, licenças, desenhos ou outros direitos de propriedade intelectual necessários ao cumprimento das obrigações objeto do contrato.

Cláusula 19.ª
Condições de pagamento

1. O pagamento do preço contratual definido na proposta do **Cocontratante** será efetuado numa única prestação, após conclusão da **FASE 2**, conforme prevista na alínea b), do n.º 3 da cláusula 6.ª, e que será efetivada através da assinatura do auto de aceitação por ambas as partes.

2. A(s) quantia(s) devida(s) pela **AdP VALOR** deve(m) ser paga(s) no prazo de 30 (*trinta*) dias após a receção pela mesma das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.

3. Em caso de discordância por parte da **AdP VALOR** quanto aos valores indicados nas faturas, esta deve comunicar, ao **Cocontratante**, por escrito, os respetivos fundamentos,

ficando o este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

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

Cláusula 20.ª
Faturação

1. As faturas emitidas pelo **Cocontratante** devem conter os elementos necessários a uma completa, clara e adequada compreensão dos valores faturados, os quais devem ser apresentados de forma desagregada.

2. A faturação deve ser acompanhada da informação relativa aos serviços prestados durante o período de faturação.

3. As faturas eletrónicas a emitir pelo **Cocontratante** devem ser enviadas para o Portal FE-AP, de receção de documentos em formato eletrónico (EDI), sistema suportado pela empresa eSPap – Entidade de Serviços Partilhados da Administração Pública, I.P..

4. Caso o **Cocontratante** não tenha ainda aderido ao Portal referido no número anterior deve efetuar os seguintes passos:

   a) Consultar a informação sobre a fatura eletrónica em https://www.espap.gov.pt/spfin/Paginas/spfin.aspx#maintab .
   b) Consultar a informação especifica do processo de adesão dos fornecedores https://www.espap.gov.pt/spfin/onboarding/Paginas/onboarding%20de%20Fornecedores.aspx#maintab1 .
   c) Preencher o formulário de adesão: https://pt.surveymonkey.com/r/FE-AP_CIUS .

5. Em caso de incumprimento dos termos da faturação resultante de facto não imputável à **AdP VALOR**, não acrescem quaisquer juros de mora.

6. As faturas eletrónicas devem cumprir o estabelecido na versão em vigor do documento "Águas de Portugal – Manual de Boas Práticas – Faturação Eletrónica Inbound (Fornecedores)", disponível em https://www.adp.pt/pt/faturacao-eletronica/?id=240 .

7. A emissão de segundas vias das faturas solicitada pela Contraente Pública não será objeto de qualquer cobrança adicional.

8. No caso do **Cocontratante** ser uma micro, pequena ou média empresa, a obrigação de emissão da faturação eletrónica produz efeitos após 01/01/2024.

SECÇÃO III

ACOMPANHAMENTO E FISCALIZAÇÃO DA EXECUÇÃO DO CONTRATO

Cláusula 21.ª

Acompanhamento e fiscalização do modo de execução do contrato

1. A execução do contrato é permanentemente acompanhada por um gestor de contrato designado pela **AdP VALOR**, a identificar no contrato.

2. No exercício das suas funções, o gestor do contrato pode acompanhar, examinar e verificar, presencialmente, a execução do contrato pelo **Cocontratante**.

3. Para o acompanhamento do Contrato, o **Cocontratante** fica obrigado a manter com uma periocidade semestral, reuniões de coordenação com o gestor do Contrato e outros representantes designados pela **AdP VALOR.**

4. As reuniões previstas no número anterior são convocadas pela **AdP VALOR**, a qual deve enviar a ordem de trabalhos de cada reunião.

5. Caso o gestor do contrato detete desvios, defeitos ou outras anomalias na execução do contrato, comunica-os, de imediato, ao órgão competente, propondo em relatório fundamentado as medidas que, em cada caso, se revelem adequadas à correção dos mesmos.

6. O desempenho das funções de acompanhamento e fiscalização do modo de execução do contrato não exime o **Cocontratante** de responsabilidade por qualquer incumprimento ou cumprimento defeituoso das suas obrigações.

CAPÍTULO III

MODIFICAÇÃO, INCUMPRIMENTO E EXTINÇÃO DO CONTRATO

Cláusula 22.ª

Cessão da posição contratual e subcontratação do Cocontratante

1. Além da situação prevista na alínea *a)* do n.º 1 do artigo 318.º do Código dos Contratos Públicos, o **Cocontratante** pode ceder a sua posição contratual, na fase de execução do contrato, mediante autorização da **AdP VALOR**.

2. Para efeitos da autorização a que se refere o número anterior, o **Cocontratante** deve apresentar uma proposta fundamentada e instruída com os documentos previstos no n.º 2

do artigo 318.º do Código dos Contratos Públicos.

3. A **AdP VALOR** deve pronunciar-se sobre a proposta do **Cocontratante** no prazo de 30 (*trinta*) dias a contar da respetiva apresentação, desde que regularmente instruída, considerando-se o referido pedido rejeitado se, no termo desse prazo, o mesmo não se pronunciar expressamente.

4. A subcontratação pelo **Cocontratante** depende de autorização da **AdP VALOR,** nos termos do Código dos Contratos Públicos.

Cláusula 23.ª
Sanções Contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a **AdP VALOR** pode exigir do **Cocontratante** o pagamento de sanções contratuais, de montante a fixar em função da gravidade do incumprimento.

2. Na determinação da gravidade do incumprimento, a **AdP VALOR** tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do **Cocontratante** e as consequências do incumprimento.

3. A **AdP VALOR** pode, designadamente, exigir do **Cocontratante** o pagamento de sanções contratuais, nos seguintes termos:

    a) 400 € *(quatrocentos euros) a 600€ (seiscentos euros)* por cada dia de atraso na conclusão do projeto, tendo em conta os prazos definidos na cláusula 7.ª do presente Caderno de Encargos;

    b) 100 € (*cem euros*) a 200 € (*duzentos euros)* por cada dia de atraso, relativamente ao prazo que venha a ser fixado nos termos no n.º 6 da cláusula 8.ª do presente Caderno de Encargos;

    c) Caso se registem atrasos em diversas fases de execução contratual, podem ser aplicadas sanções cumulativas.

4. Nas situações em que, sem autorização da **AdP VALOR**, o **Cocontratante** proceder à alteração da constituição da equipa afeta ao Projeto, quer na designação dos técnicos, quer no número de elementos que a integrem, ser-lhe-á aplicada, por cada alteração, uma sanção pecuniária de 5% *(cinco por cento)* do preço contratual respeitante à fase correspondente.

5. O valor acumulado das sanções contratuais a aplicar não poderá exceder o limite máximo de 20% do preço contratual.

6. Nos casos em que seja atingido o limite de 20% e a **AdP VALOR** decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.

7. Ao valor da sanção contratual previsto no número anterior são deduzidas as importâncias pagas pelo **Cocontratante** ao abrigo do n. °1, relativamente aos serviços objeto do contrato cujo atraso na respetiva conclusão tenha determinado a respetiva resolução.

8. A **AdP VALOR** pode compensar os pagamentos devidos ao abrigo do contrato com as sanções contratuais devidas nos termos da presente cláusula.

9. As sanções contratuais previstas na presente cláusula não obstam a que a **AdP VALOR** exija uma indemnização pelo dano excedente.

Cláusula 24.ª
Caução

1. A caução prestada para bom e pontual cumprimento das obrigações decorrentes do Contrato, pode ser executada pela **AdP VALOR**, sem necessidade de prévia decisão judicial ou arbitral, para satisfação de quaisquer créditos resultantes de mora, cumprimento defeituoso, incumprimento definitivo pelo **Cocontratante** das obrigações contratuais ou legais, incluindo o pagamento de sanções contratuais, ou para quaisquer outros efeitos resultantes do Contrato ou da lei.

2. A resolução do Contrato pela **AdP VALOR** não impede a execução da caução nos termos da lei ou do Contrato.

3. Salvo no caso previsto no número anterior, a execução parcial ou total da caução constitui o **Cocontratante** na obrigação de proceder à sua reposição pelo valor existente antes da execução, no prazo de 15 (*quinze*) dias, após a notificação da **AdP VALOR**.

4. A caução a que se referem os números anteriores é liberada nos termos do artigo 295.° do Código dos Contratos Públicos.

Cláusula 25.ª
Força maior

1. Não podem ser impostas penalidades ao **Cocontratante**, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior.

2. Para efeitos do contrato, só são consideradas de força maior as circunstâncias que,

cumulativamente e em relação à parte que as invoca:

a) Impossibilitem o cumprimento das obrigações emergentes do contrato;

b) Sejam alheias à sua vontade;

c) Não fossem por ela conhecidas ou previsíveis à data da celebração do contrato;

d) Não lhe seja razoavelmente exigível contornar ou evitar os efeitos produzidos por aquelas circunstâncias.

3. Não constituem força maior, designadamente:

a) Circunstâncias que não constituam força maior para os subcontratados do **Cocontratante,** na parte em que intervenham;

b) Greves ou conflitos laborais limitados às sociedades do **Cocontratante** ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;

c) Determinações governamentais, administrativas ou judiciais de natureza sancionatória, ou de outra forma resultantes do incumprimento pelo **Cocontratante** de deveres ou ónus que sobre ele recaiam;

d) Manifestações populares devidas ao incumprimento pelo **Cocontratante** de normas legais;

e) Incêndios ou inundações com origem nas instalações do **Cocontratante** 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 **Cocontratante** não devidas a sabotagem;

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

4. A parte que invocar caso de força maior deve comunicar e justificar tal situação à outra parte, logo após a sua ocorrência, bem como informar o prazo previsível para restabelecer o cumprimento das obrigações contratuais.

5. A suspensão, total ou parcial, do cumprimento pelo **Cocontratante** das suas obrigações contratuais fundada em força maior, por prazo superior a 30 (*trinta*) dias, autoriza a **AdP VALOR** a resolver o contrato ao abrigo do n.º 1 do artigo 335.º do Código dos Contratos Públicos, não tendo o **Cocontratante** direito a qualquer indemnização.

Cláusula 26.ª

Resolução do contrato por parte da AdP VALOR

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a **AdP VALOR** pode resolver o contrato, a título sancionatório, no caso de o **Cocontratante** violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.

2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao **Cocontratante** e não implica a repetição das prestações já realizadas pelo mesmo, nos termos previstos no presente Caderno de Encargos, a menos que tal seja expressamente determinado pela **AdP VALOR**.

Cláusula 27.ª

Resolução do contrato por parte do Cocontratante

1. O **Cocontratante** pode resolver o contrato com os fundamentos previstos no artigo 332.º do Código dos Contratos Públicos.

2. Salvo na situação prevista na alínea *c)* do n.º 1 do artigo 332.º do Código dos Contratos Públicos, o direito de resolução é exercido por via judicial.

3. A resolução do contrato não determina a repetição das prestações já realizadas pelo **Cocontratante**, cessando, porém, todas as obrigações deste ao abrigo do contrato.

Cláusula 28.ª

Seguros

1. É da responsabilidade do **Cocontratante** a cobertura, através de contrato de seguro, dos riscos inerentes à atividade objeto do contrato a celebrar, designadamente:

   a) Acidente de trabalho;

   b) Responsabilidade civil;

2. A **AdP VALOR** pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos no número anterior, devendo o **Cocontratante** prestá-la no prazo de 2 (*dois*) dias.

CAPÍTULO IV
DISPOSIÇÕES FINAIS

Cláusula 29.ª
Deveres de informação

1. Cada uma das partes deve informar sem demora a outra de quaisquer circunstâncias que cheguem ao seu conhecimento e possam afetar os respetivos interesses na execução do contrato, de acordo com a boa-fé.
2. Em especial, cada uma das partes deve avisar de imediato a outra de quaisquer circunstâncias, constituam ou não força maior, que previsivelmente impeçam o cumprimento ou o cumprimento tempestivo de qualquer uma das suas obrigações.
3. No prazo de 15 (*quinze*) dias após a ocorrência de tal impedimento, a parte deverá informar a outra do tempo ou da medida em que previsivelmente será afetada a execução do contrato.

Cláusula 30.ª
Comunicações

1. Salvo quando o contrário resulte do contrato, quaisquer comunicações entre a **AdP VALOR** e o **cocontratante** relativas ao contrato devem ser efetuadas através de carta registada com aviso de receção ou correio eletrónico.
2. Qualquer comunicação feita por carta registada é considerada recebida na data em que for assinado o aviso de receção ou, na falta dessa assinatura, na data indicada pelos serviços postais.
3. Qualquer comunicação feita por correio eletrónico é considerada efetuada na data constante do respetivo recibo de receção e leitura remetido pelo recetor ao emissor.

Cláusula 31.ª
Foro competente

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

Cláusula 32.ª

Direito aplicável e natureza do contrato

O contrato rege-se pelo direito português e tem natureza administrativa.

Cláusula 33.ª

Contagem dos prazos

Os prazos previstos no presente caderno de encargos são contínuos, correndo em sábados, domingos e dias feriados, aplicando-se à contagem dos prazos as demais regras constantes do artigo 471.º do Código dos Contratos Públicos.

ANEXO I

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1) Requisitos gerais

No âmbito do projeto, a proposta deverá considerar o fornecimento de uma solução de segurança composta por "**Firewall Externa (Internet), Firewall de Core(L3), numa topologia de 2 (dois) níveis 2 (duas) tecnologias & Firewall Aplicacional (WAF – web application firewall)**", bem como a sua instalação, configuração e integração na infraestrutura da AdP VALOR, garantindo o cumprimento dos objetivos definidos no procedimento, bem como o suporte e manutenção nos termos definidos neste documento, pelo período de **36 (trinta e seis) meses**, sendo a solução composta, no mínimo, pelos seguintes itens:

- ITEM 1 – Solução Firewall Externa (Site Principal – Sede AdP em Lisboa), upgrade solução existente;
- ITEM 2 – Solução Firewall Core (Site Principal – Sede AdP em Lisboa), nova solução;
- ITEM 3 – Solução Firewall Aplicacional/Reverse Proxy (WAF), virtual;
- ITEM 4 – Solução Firewall Externa & Core (Site DR – em Barcelos), nova solução;
- ITEM 5 – Serviços de instalação, configuração, suporte e manutenção.

2) ITEM 1 – Firewall Externa (Site Principal – sede AdP em Lisboa)

A solução a fornecer deverá ser baseada em *appliances físicas (hardware)* numa arquitetura em *cluster*. Esta infraestrutura visa disponibilizar à AdP VALOR uma solução de firewall de perímetro, com as seguintes funcionalidades base:

- Cluster de firewall de 2 (duas) *appliances* físicas;
- Funcionalidades de *Next Generation Threat Prevention and SandBlast;*
- Gestão centralizada (através da solução existente, devendo ser renovado o UC: 0005725586, respetivamente CPAP-NGSM405, CPSB-MOB-200);
- Suporte e subscrições necessárias para as funcionalidades solicitadas com duração de 36 (trinta e seis) meses.

a) Requisitos, funcionalidades e capacidades da solução.

A solução efetuará a interligação com a infraestrutura da AdP VALOR, composta por 2 (dois) equipamentos, com funcionalidades de mínimas de: IPS, Application Control e URL Filtering, Anti-Bot, DNS Security, Thread Emulation (Sandboxing), Threat Extraction e funcionalidades de Zero Phishing.

a.1) Funcionalidades gerais

- Suporte de clustering em Ativo-Ativo e Ativo-Passivo
- Suporte de clustering com mais de 2 membros num mesmo cluster
- Deteção em tempo real de protocolos dinâmicos (ex: FTP, SIP, H323, etc.)
- Deteção/bloqueio de serviços como P2P e IM por aplicação (voz/vídeo/file share)
- Agrupamento de regras
- NAT de aplicações em tempo real
- PAT
- NAT/PAT baseado em regras
- Autenticação de serviços
- Integração com Active Directory e com LDAP
- Base de dados local de utilizadores
- Autenticação de 2 fatores (p. ex. tokens físicos, soft tokens, SMS e email)
- Geração interna e entrega de One Time Password (OTP) para autenticação
- Implementação de regras com data de expiração ou em intervalos de tempo
- Regras com objetos baseados na geografia
- Identificação automática de utilizadores no sistema de logs
- Reputação de Clientes
- Suporte a proxy de HTTP e HTTPS
- Regras por utilizador ou grupo de utilizadores
- Captive Portal para autenticar utilizadores que não pertencem à rede
- Contas Guest com gestão independente
- Identificação de dispositivos (incluindo Fabricante e SO)
- Regras baseadas em dispositivos ou grupos de dispositivos
- Possibilidade de controlo de endpoints
- Opção de criação de gateways virtuais na mesma plataforma.

a.2) Networking

- Suporte Múltiplos Links WAN – Redundância e Balanceamento de carga
- Routing baseado em políticas
- Rotas Estáticas
- Ipv6
- 802.1q- VLAN Tagging
- DHCP Relay e DHCP Server
- Spanning-Tree (802.1d)
- Suporte 802.3.ad e LACP – Agregação de Links (Ativo-Ativo ou Ativo-Passivo)

- Suporte de Dead Gateway Detection
- Job Scheduler
- Suporte TOS/DiffServ
- Suporte para Virtual Switches e para Virtual Routers
- Instalação em modo Router e modo Transparente

a.3) Networking em Ipv6

- Rotas estáticas
- RIPv6
- BGP4+
- OSPFv3
- DNS
- Endereçamento de interfaces
- Ipv6 Tunnel sobre Ipv4
- Ipv4 tunnel sobre Ipv6
- Packet e network sniffing
- NAT
- Troubleshooting específico Ipv6

a.4) Protocolos de Routing

- OSPFv2 and v3
- BGP
- RIP
- IGMP v2 and v3
- Static and Multicast routes
- Policy-based routing
- PIM SM
- PIM SSM
- PIM DM

a.5) Acessos VPN

- Serviço integrado nativamente e interno nas gateways
- Licenciamento para um mínimo de 200 VPN Client to Site em simultâneo, expansível a ilimitado apenas restringido pelo hardware instalado
- Suporte de IKEv1 e IKEv2
- Suporte de criptografia para 3DES e AES-256 para IKE Phase I e II IKEv2

- Suporte de pelo menos os seguintes grupos de Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit)
- IKE Phase2 – Encriptação de dados (DES, 3DES, AES-128, AES-192, AES-256 e NULL) e suporte de integridade dos dados (MD5, SHA1, SHA256, SHA384, SHA512 e NULL)
- VPNs Site to Site: Full Mesh (all to all) ou Star (Remote to center)
- Suporte de IKE com PKI e pre-shared Secret
- Aprovisionamento automático de VPNs site-to-site
- Gestão automática de túneis IPSec de backup
- Suporte de routing dinâmico em VPN IPSec
- Clientes VPN para Windows, MacOS e iOS, Android
- Suporte OTP para VPN sem recurso a terceiros fabricantes ou servidores adicionais
- Aplicação de políticas e restrições de acesso por utilizador ou grupos de utilizadores
- Single Sign On VPN
- Administração a partir da consola central

a.6) IDS/IPS

- Serviço integrado nativamente e interno nas gateways
- Atualização automática de assinaturas
- Criação de perfis e existência de perfis pré-definidos para utilização imediata
- Capacidade de captura de tráfego na consola de gestão para proteções específicas
- Proteção contra Denial of Service
- Funcionalidade de bypass em caso de carga excessiva
- Regras de bloqueio automático por países
- Importação e conversão de proteções de SNORT
- Capacidade de inspecionar tráfego com criptografia SSL
- Motor com mecanismos de deteção de assinaturas de exploits, anomalias protocolares, controlos de aplicação e deteção comportamental
- Suporte de motor de deteção de Antibot
- Protocol Tunneling Recognition
- Criação de perfis de proteção para apenas clientes, servidores e ambos
- Capacidade de aplicação de diferentes perfis de proteção em diferentes fluxos
- Administração a partir da consola central

a.6) Application Control e URL Filtering

- Serviço integrado nativamente e interno nas gateways

- Atualização automática de assinaturas
- Reconhecimento de >= 4.000 aplicações
- Reconhecimento de >= 250.000 widgets (sub aplicações dentro das principais App Web 2.0, como por ex. Farmville dentro do Facebook)
- Categorização realizada a >= 200 milhões URLs com cobertura de mais de 85% da Alexa's Top 1 Milhão de sites
- Controlo por largura de banda de cada aplicação Web 2.0
- Inspeção SSL (tráfego inbound e outbound, ainda que em SSL encriptado)
- Criação de assinaturas personalizadas e privadas
- Criação de regras pelo índice de criticidade de segurança, índice de popularidade, categoria, tecnologia e fabricante de aplicações
- Controlo de utilizadores em ambientes VDI e Terminal Services
- Administração a partir da consola central

a.7) Anti-Bot e Antivírus

- Serviço integrado nativamente e interno nas gateways
- Atualização automática e em tempo real de assinaturas
- Capacidade de detetar e parar comportamentos anómalos na rede
- Deteção em arquitetura multicamada com reputação de IP, URLs e endereços DNS
- Deteção de padrões de comunicação de bots
- Análise das ações de bots
- Bloqueio do acesso a sites mal-intencionados
- Bloqueio de entrada de ficheiros maliciosos
- Capacidade de definição de políticas granulares e eficazes.
- Capacidade de inspecionar tráfego com criptografia SSL
- Correlação centralizada de eventos e mecanismos de reporting
- Administração a partir da consola central

a.8) Proteção de ataques Zero-Day / Sandboxing

A solução proposta deve incluir de forma nativamente integrada as funcionalidades necessárias para a proteção contra os ataques desconhecidos do tipo "Zero Day" através de técnicas de sandboxing e emulação que permitam:

- Proteger contra os ataques do tipo "Zero Day" antes de serem criadas as assinaturas estáticas contra o malware
- Análise e deteção de ataques 'Zero Day' diversos tipos de ficheiros, nomeadamente Adobe PDF, Microsoft Office, EXE, arquivos ZIP, Flash, Java Applets e PIF

- Sanitização em tempo-real (entrega segura aos utilizadores, livre de scripts e similares) de ficheiros habituais de trabalho como Microsoft Office e Adobe PDF
- Emulação de ataques contra vários ambientes do sistema operativo Microsoft Windows, nas versões Windows XP, Windows 7 e Windows 8
- Zero falsos positivos (não existência de falsos positivos)
- Possibilidade de incremento da capacidade de segurança através da partilha de informações de novos ataques detetados noutras gateways com geração automática das assinaturas para bloqueio
- Emulação/sandboxing com capacidade de inspecionar e bloquear ataques por HTTPS sem recurso a dispositivos adicionais
- Capacidade de execução On-Premise e com recurso a serviços cloud
- Possibilidade de implementação de sandboxing em modo 'in-line' na cloud, em equipamento out-of-band ou com MTA (Mail Transfer Agent)
- Análise ao nível do CPU para mitigação do risco de evasão
- Administração a partir da consola central

a) Solução/Configuração

O Proponente deve garantir as seguintes características e capacidades:

All-In-One – Funcionalidades/Capacidade	
Solução	**Requisito**
N° de equipamentos – 2 (dois)	Obrigatório
Solução não pode ocupar mais que 4 Us em bastidor	Obrigatório
Suporte 36 meses	Obrigatório
Características de hardware, por equipamento	Requisito
Mínimo de 10 portas a Gigabit em cobre (RJ45)	Obrigatório
Mínimo de 4 portas (slots) GE / SFP, 10 GE / SFP+	Obrigatório
Fornecimento de 2 x transceivers em fibra a 10GE / SFP+ short-range	Obrigatório
1 x Porta USB e 1 x Porta de consola (RJ45)	Obrigatório
1 x Porta LOM	Obrigatório
Fontes de alimentação redundantes	Obrigatório
Discos interno com mínimo de 480G SSD	Obrigatório
1 x CPU, com o mínimo de 6 Cores 30plicaç (12 virtuais)	Obrigatório
Mínimo 32GB de RAM	Obrigatório
Possibilidade de adicionar cartas com portas a 40G (QSFP+), mínimo 2, com aquisição de carta.	Obrigatório

Características/capacidade, por equipamento	Requisito
Firewall throughput mínimo de 38 Gbps (1518 byte, UDP)	Obrigatório
Mínimo de 2 milhões de sessões concorrentes	Obrigatório
Mínimo de 164 mil novas sessões por segundo	Obrigatório
IPS throughput mínimo de 19 Gbps	Obrigatório
Threat Protection Throughput mínimo de 5,8 Gbps	Obrigatório
Possibilidade de implementar 10 sistemas (firewalls) virtualizados, com licenciamento adicional	Obrigatório

3) ITEM 2 – Firewall Core/L3 (Site Principal – Sede AdP em Lisboa)

A solução a fornecer deverá ser baseada em *appliances físicas (hardware)* numa arquitetura em *cluster*. Esta infraestrutura visa disponibilizar à AdP VALOR uma solução de firewall de Core/L3, proteção ao nível do datacenter, com as seguintes funcionalidades base:

- Cluster de firewall de 2 (duas) appliances físicas;
- Funcionalidades de *Unified Threat Protection*:
- Capacidade de segregação em ambientes virtuais, com um mínimo de 10 (dez) licenciados;
- Gestão/loging centralizada (em VM e compatível com VMWare);
- Suporte e subscrições necessárias para as funcionalidades solicitadas com duração de 36 (trinta e seis) meses.

b) Requisitos, funcionalidades e capacidades da solução.

A solução efetuará a interligação com a infraestrutura da AdP VALOR, composta por 2 (dois) equipamentos do tipo **All-in-one/Unified Threat Management (Firewall, Threat Protection[IPS, Web-filtering, Anti-Malware, SSL inspection])** em cluster e com fontes de alimentação redundantes. O S.O. deve dispor de funcionalidades de Firewall, Routing e Intrusion Prevention/Detection System (IPS/IDS), com aceleração de tráfego por hardware dedicado na firewall.

b.1) Ao nível de **Firewall** deverão ser suportadas as seguintes funcionalidades:

- Modos de operação NAT/route e transparente/bridge;
- Agendamento de políticas, recorrentes ou apenas uma vez;
- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)

- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pin holing
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por secção
- 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 endereços IP, Geografia e FQDN
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT
- 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).

b.2) Ao nível de **IPS/IDS** deverão ser suportadas as seguintes funcionalidades:

- Mínimo de 7.000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, update de assinaturas manual ou automático (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados.
- Ações de IPS: por defeito na assinatura, monitorizar, bloquear, reset 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

b.3) Ao nível de **Threat Protection** deverão ser suportadas as seguintes funcionalidades:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, antivírus, filtragem WEB e DLP
- Deteção e bloqueio de BOTNETs com base em listas de reputação de Ips globais;
- Suporte de antivírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de antivírus, em modo flow, nos protocolos: HTTP/HTTPS,

SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, NNTP

- Integração com solução de Sandboxing (cloud ou premises)
- Suporte de antivírus em modo proxy, incluindo:
- Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, NNTP:
    - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
    - Listas de ficheiros autorizados/negados
    - Opção de análise heurística
- Deteção de sites WEB (web filtering):
    - Suporte de diferentes mecanismos de deteção de sites Web (proxy-based, flowbased 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 com mais de 250 milhões de sites categorizados, em mais de 50 idiomas e 77 categorias
    - 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 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 de tráfego encriptado (SSL) em 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, apontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação proxy por deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Suporte a 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 ações de: registar, bloquear, quarentena de utilizador / IP /Interface
- Filtros pré-definidos, incluindo cartões de crédito e número de Seg. 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 detetado para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB

b.4) Ao nível de **Alta Disponibilidade** deverão ser suportadas as seguintes funcionalidades:

- Alta disponibilidade nos modos ativo-passivo, ativo-ativo
- 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 rápido "em menos de 10 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 com equipamentos em modo Standalone

b.5) Ao nível de **Administração, Monitorização e Diagnósticos** deverão ser suportadas as seguintes funcionalidades:

- 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 específico para gestão gráfica
- Suporte a múltiplos idiomas de administração com acesso gráfico, incluindo Português e Inglês

- 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 e Syslog
- 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.

b.6) **Registo de Eventos e Relatórios**, com suporte para as seguintes funcionalidades:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória e/ou discos rígidos locais, 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
- Opção para registo encurtado ou completo de eventos
- Resolução de nomes de endereços IP e protocolos

b.7) Simultaneamente, os equipamentos deverão ter as seguintes **Certificações**:

- Certificações ICSA de Firewall, Ipsec, IPS, Antivírus, SSL-VPN
- Certificação USGv6/Ipv6

c) Solução/Configuração

O Proponente deve garantir as seguintes características e capacidades:

All-In-One – Funcionalidades/Capacidade	
Solução	**Requisito**

N° de equipamentos – 2 (dois)	Obrigatório
Solução não pode ocupar mais que 4 Us em bastidor	Obrigatório
Suporte 36 meses em regime de 24x7	Obrigatório
Características de hardware, por equipamento	Requisito
Mínimo de 16 portas a Gigabit em cobre (RJ45)	Obrigatório
Mínimo de 8 portas (slots) em SFP a Gigabit	Obrigatório
Mínimo de 4 portas (slots) GE / SFP, 10 GE / SFP+ (Ultra Low Latancy)	Obrigatório
Mínimo de 4 portas (slots) GE / SFP, 10 GE / SFP+	Obrigatório
Fornecimento de 2 x transceivers em fibra a 10GE / SFP+ short-range	Obrigatório
1 x Porta USB 3.0 e 1 x Porta de consola (RJ45)	Obrigatório
Fontes de alimentação hot-swap redundantes	Obrigatório
Discos internos com mínimo de 480G SSD x 2	Obrigatório
Características/capacidade, por equipamento	Requisito
Firewall throughput mínimo de 70 Gbps em IPV4 e IPV6 (1518 byte, UDP)	Obrigatório
Mínimo de 7,8 milhões de sessões concorrentes	Obrigatório
Mínimo de 500 mil novas sessões por segundo	Obrigatório
Latência inferior a 2,5 µs (com pacotes de 64 byte, UDP) mas portas "Ultra Low Latancy"	Obrigatório
IPS throughput mínimo de 12 Gbps	Obrigatório
Threat Protection Throughput mínimo de 9 Gbps	Obrigatório
SSL Inspection Throughput mínimo de 8 Gbps	Obrigatório
Application Control Throughput mínimo de 28 Gbps	Obrigatório
Licenciamento incluído para 10 sistemas (firewalls) virtualizados	Obrigatório
Possibilidade de gestão de AP (pontos de acesso wifi), até 128 equipamentos	Obrigatório

4) ITEM 3 – Firewall Aplicacional (WAF)

A solução a fornecer deverá ser baseada em infraestrutura Virtual (*VM*) e numa arquitetura *standalone*. A arquitetura visa disponibilizar à AdP VALOR uma solução de firewall aplicacional, normalmente designadas por WAF e/ou Revers Proxy e sintetizar as seguintes funcionalidades base:

- Solução – Firewall Aplicacional WAF (*Web Aplication Firewall*), a implementar em plataforma de VMWare existente, do mesmo fabricante do ITEM 3;
- Suporte 24x7 com duração de 36 (trinta e seis) meses

a) Solução/Configuração

O Proponente deve garantir as seguintes características e capacidades descritas nos pontos

seguintes:

a.1) Modos de integração em rede

As seguintes funcionalidades deverão ser suportadas:

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

a.2) Segurança Web

As seguintes funcionalidades deverão ser suportadas:

- AI-based Machine Learning
- Profiling automático (37plic 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)

a.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)

a.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

a.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

a.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 SSL de cliente
- CAPTCHA e Real Browser Enforcement (RBE)

a.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
- REST 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 39plicações39ção 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)

a.8) Integração em redes

As seguintes funcionalidades deverão ser suportadas:

- VLANs (802.1Q) e agregação de portas(802.3ad)
- Support de Ipv6
- Alta disponibilidade ativo-passivo e ativo-ativo
- 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 autoaprendizagem
- 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

b) Solução.

O Cocontratante deve garantir as seguintes características e capacidades.

All-In-One VM – Funcionalidades/Capacidade	
Solução	Requisito
N° de equipamentos – 1 (uma) VM (Virtual Appliance)	Obrigatório
Solução certificada para VMWare	Obrigatório
Suporte 36 meses em regime de 24x7	Obrigatório
Características da VM, por equipamento	Requisito
Permitir alocar, no mínimo, 2 vCPUs	Obrigatório
Permitir alocar, no mínimo, 500G de disco	Obrigatório
Não ter limitação de RAM, au nível do licenciamento	Obrigatório
Características/capacidade, por equipamento	Requisito
Permitir no mínimo, 100Mbps de throughput em http	Obrigatório
Não ter limite de utilizadores	Obrigatório
Não ter limite de 40plicações/sites publicados	Obrigatório

5) ITEM 4 – Firewall Externa/Core (Site DR em Barcelos)

A solução a fornecer deverá ser baseada em *appliance física (hardware)* numa arquitetura simples. Esta infraestrutura visa disponibilizar à AdP VALOR uma solução de firewall de perímetro e L3 para o site de DR em Barcelos, com as seguintes funcionalidades base:

- Cluster de firewall de 1 (uma) appliance física;
- Funcionalidades de *Next Generation Threat Prevention;*
- Gestão centralizada (através da solução existente Checkpoint);
- Suporte e subscrições necessárias para as funcionalidades solicitadas com duração de 36 (trinta e seis) meses.

a) Requisitos, funcionalidades e capacidades da solução.

A solução efetuará a interligação com a infraestrutura da AdP VALOR, composta por 1 (um) equipamentos, com funcionalidades de mínimas de: IPS, Application Control e URL Filtering, Anti-Bot e DNS Security.

a.1) Funcionalidades gerais

- Suporte de clustering em Ativo-Ativo e Ativo-Passivo
- Suporte de clustering com mais de 2 membros num mesmo cluster
- Deteção em tempo real de protocolos dinâmicos (ex: FTP, SIP, H323, etc.)
- Deteção/bloqueio de serviços como P2P e IM por aplicação (voz/vídeo/file share)
- Agrupamento de regras
- NAT de aplicações em tempo real
- PAT
- NAT/PAT baseado em regras
- Autenticação de serviços
- Integração com Active Directory e com LDAP
- Base de dados local de utilizadores
- Autenticação de 2 fatores (p. ex. tokens físicos, soft tokens, SMS e email)
- Geração interna e entrega de One Time Password (OTP) para autenticação
- Implementação de regras com data de expiração ou em intervalos de tempo
- Regras com objetos baseados na geografia
- Identificação automática de utilizadores no sistema de logs
- Reputação de Clientes
- Suporte a proxy de HTTP e HTTPS
- Regras por utilizador ou grupo de utilizadores
- Captive Portal para autenticar utilizadores que não pertencem à rede
- Contas Guest com gestão independente
- Identificação de dispositivos (incluindo Fabricante e SO)
- Regras baseadas em dispositivos ou grupos de dispositivos
- Possibilidade de controlo de endpoints
- Opção de criação de gateways virtuais na mesma plataforma.

a.2) Networking

- Suporte Múltiplos Links WAN – Redundância e Balanceamento de carga
- Routing baseado em políticas
- Rotas Estáticas
- Ipv6

- 802.1q- VLAN Tagging
- DHCP Relay e DHCP Server
- Spanning-Tree (802.1d)
- Suporte 802.3.ad e LACP – Agregação de Links (Ativo-Ativo ou Ativo-Passivo)
- Suporte de Dead Gateway Detection
- Job Scheduler
- Suporte TOS/DiffServ
- Suporte para Virtual Switches e para Virtual Routers
- Instalação em modo Router e modo Transparente

a.3) Networking em Ipv6

- Rotas estáticas
- RIPv6
- BGP4+
- OSPFv3
- DNS
- Endereçamento de interfaces
- Ipv6 Tunnel sobre Ipv4
- Ipv4 tunnel sobre Ipv6
- Packet e network sniffing
- NAT
- Troubleshooting específico Ipv6

a.4) Protocolos de Routing

- OSPFv2 and v3
- BGP
- RIP
- IGMP v2 and v3
- Static and Multicast routes
- Policy-based routing
- PIM SM
- PIM SSM
- PIM DM

a.5) Acessos VPN

- Serviço integrado nativamente e interno nas gateways

- Licenciamento para um mínimo de 50 VPN Client to Site em simultâneo, expansível a ilimitado apenas restringido pelo hardware instalado
- Suporte de IKEv1 e IKEv2
- Suporte de criptografia para 3DES e AES-256 para IKE Phase I e II IKEv2
- Suporte de pelo menos os seguintes grupos de Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit)
- IKE Phase2 – Encriptação de dados (DES, 3DES, AES-128, AES-192, AES-256 e NULL) e suporte de integridade dos dados (MD5, SHA1, SHA256, SHA384, SHA512 e NULL)
- VPNs Site to Site: Full Mesh (all to all) ou Star (Remote to center)
- Suporte de IKE com PKI e pre-shared Secret
- Aprovisionamento automático de VPNs site-to-site
- Gestão automática de túneis IPSec de backup
- Suporte de routing dinâmico em VPN IPSec
- Clientes VPN para Windows, MacOS e iOS, Android
- Suporte OTP para VPN sem recurso a terceiros fabricantes ou servidores adicionais
- Aplicação de políticas e restrições de acesso por utilizador ou grupos de utilizadores
- Single Sign On VPN
- Administração a partir da consola central

a.6) IDS/IPS

- Serviço integrado nativamente e interno nas gateways
- Atualização automática de assinaturas
- Criação de perfis e existência de perfis pré-definidos para utilização imediata
- Capacidade de captura de tráfego na consola de gestão para proteções específicas
- Proteção contra Denial of Service
- Funcionalidade de bypass em caso de carga excessiva
- Regras de bloqueio automático por países
- Importação e conversão de proteções de SNORT
- Capacidade de inspecionar tráfego com criptografia SSL
- Motor com mecanismos de deteção de assinaturas de exploits, anomalias protocolares, controlos de aplicação e deteção comportamental
- Suporte de motor de deteção de Antibot
- Protocol Tunneling Recognition
- Criação de perfis de proteção para apenas clientes, servidores e ambos
- Capacidade de aplicação de diferentes perfis de proteção em diferentes fluxos

- Administração a partir da consola central

a.6) Application Control e URL Filtering

- Serviço integrado nativamente e interno nas gateways
- Atualização automática de assinaturas
- Reconhecimento de >= 4.000 aplicações
- Reconhecimento de >= 250.000 widgets (sub aplicações dentro das principais App Web 2.0, como por ex. Farmville dentro do Facebook)
- Categorização realizada a >= 200 milhões URLs com cobertura de mais de 85% da Alexa's Top 1 Milhão de sites
- Controlo por largura de banda de cada aplicação Web 2.0
- Inspeção SSL (tráfego inbound e outbound, ainda que em SSL encriptado)
- Criação de assinaturas personalizadas e privadas
- Criação de regras pelo índice de criticidade de segurança, índice de popularidade, categoria, tecnologia e fabricante de aplicações
- Controlo de utilizadores em ambientes VDI e Terminal Services
- Administração a partir da consola central

a.7) Anti-Bot e Antivírus

- Serviço integrado nativamente e interno nas gateways
- Atualização automática e em tempo real de assinaturas
- Capacidade de detetar e parar comportamentos anómalos na rede
- Deteção em arquitetura multicamada com reputação de IP, URLs e endereços DNS
- Deteção de padrões de comunicação de bots
- Análise das ações de bots
- Bloqueio do acesso a sites mal-intencionados
- Bloqueio de entrada de ficheiros maliciosos
- Capacidade de definição de políticas granulares e eficazes.
- Capacidade de inspecionar tráfego com criptografia SSL
- Correlação centralizada de eventos e mecanismos de reporting
- Administração a partir da consola central

b) Solução/Configuração

O Proponente deve garantir as seguintes características e capacidades:

All-In-One – Funcionalidades/Capacidade

Solução	Requisito
N° de equipamentos – 1 (um)	Obrigatório
Solução não pode ocupar mais que 2 Us em bastidor	Obrigatório
Suporte 36 meses	Obrigatório
Características de hardware, por equipamento	Requisito
Mínimo de 10 portas a Gigabit em cobre (RJ45)	Obrigatório
Mínimo de 4 portas (slots) em SFP a Gigabit	Obrigatório
1 x Porta USB 1 x Porta de consola (RJ45)	Obrigatório
Fontes de alimentação hot-swap redundantes	Obrigatório
1 x porta LOM	Obrigatório
Disco interno com mínimo de 240G/SSD	Obrigatório
1 x CPU com 2 cores físicos (4 virtuais)	Obrigatório
Possibilidade de adicionar uma carta com 4 portas a 10G (SFP+)	Obrigatório
Características/capacidade, por equipamento	Requisito
Firewall throughput mínimo de 17 Gbps (1518 byte, UDP)	Obrigatório
Mínimo de 2 milhões de sessões concorrentes	Obrigatório
Mínimo de 67 mil novas sessões por segundo	Obrigatório
IPS throughput mínimo de 4,5 Gbps	Obrigatório
Threat Protection Throughput mínimo de 1,8 Gbps	Obrigatório

6) ITEM 5 – Serviços de instalação, configuração, suporte e manutenção

Na proposta, deverá o Cocontratante considerar os serviços de instalação e configuração das novas soluções bem como a migração das atuais políticas para os novos equipamentos.

a) Requisitos dos serviços de instalação, configuração e integração

No âmbito dos serviços de instalação, configuração e integração na infraestrutura da AdP VALOR, deverão ser consideradas, pelo menos, as seguintes tarefas:

- Levantamento dos pré-requisitos para a implementação;
- Identificação de possíveis riscos na implementação e de medidas de mitigação;
- Definição do cronograma de implementação da solução;
- Instalação dos vários equipamentos e VMs;
- Instalação e configuração de todas as componentes e funcionalidades necessárias ao cumprimento dos requisitos definidos nas especificações técnicas;
- Configuração nos equipamentos já existentes da infraestrutura da AdP VALOR de todos

os parâmetros que permitam a correta integração e funcionamento da solução proposta, incluindo, ainda que não exclusivamente, eventuais alterações de switching e routing;

- Implementação de políticas base nas firewalls de Core/L3 (migração do Cisco ASA e Switch de Core);
- Implementação de nova política de firewall de perímetro Internet e L3, no site de DR;
- Ajuste das políticas existentes na firewall de perímetro Internet, existente no DC, para correto funcionamento da arquitetura global;
- Implementação e integração de todas as gateways novas da Check Point nas consolas de gestão e reporting existentes;
- Instalação e configuração da solução de proteção aplicacional (WAF), com publicação de até 5 (cinco) sites;
- Workshop de transferência de conhecimentos, com uma duração mínima de 2 (dois) dias;
- Documentação da solução.

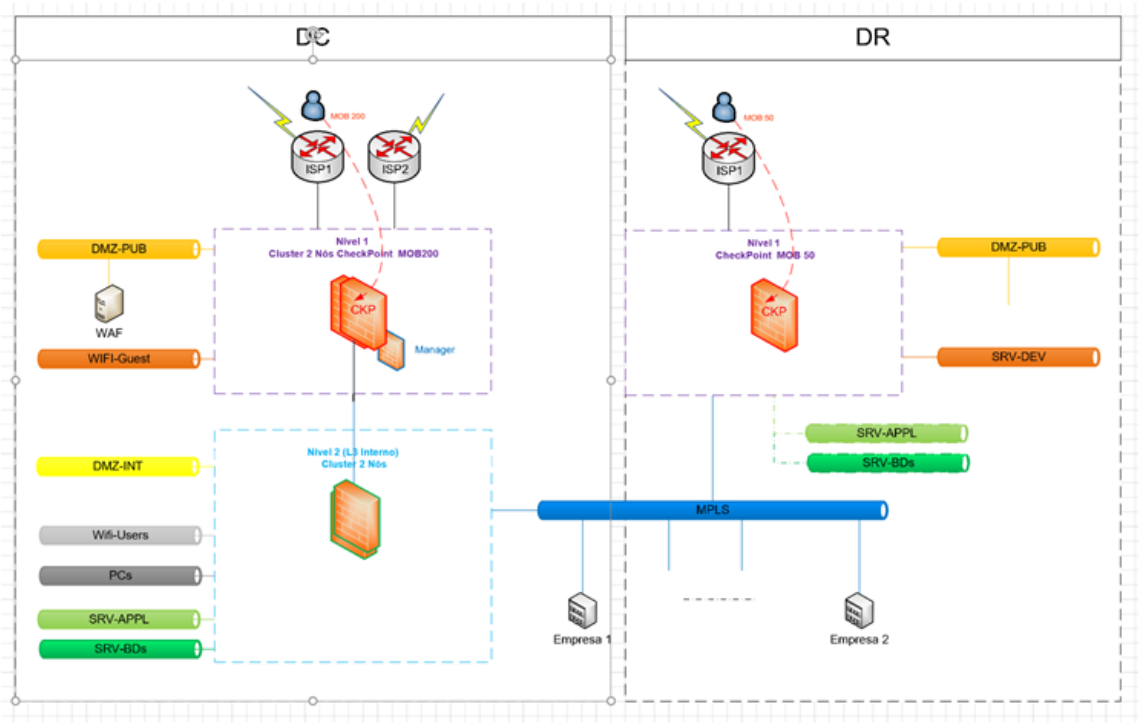
Ainda que seja o Proponente a assumir a totalidade dos serviços necessários ao correto funcionamento das soluções propostas, a AdP VALOR, fixa os serviços de instalação, configuração e integração com uma duração mínima de **15 (quinze) dias**.

b) Requisitos dos serviços de suporte e manutenção.

Os serviços de suporte e manutenção, bem como eventuais subscrições associadas, deverão ser fornecidos obrigatoriamente com *back-to-back* com o fabricante, pelo período contratado de 36 (trinta e seis) meses, pretendendo ainda a AdP VALOR que sejam prestados os seguintes serviços:

- Suporte do fabricante da solução (nova e existentes) no regime de 24x7;
- Subscrição de fontes de informação (atualização de assinaturas) e similares;
- Pacote de **150 (cento e cinquenta)** horas de serviços de suporte técnico local, a utilizar em tarefas de fine tuning, troubleshooting e apoio na exploração das soluções aos longo do 36 (*trinta e seis*) meses.

7) ARQUITETURA DA SOLUÇÃO


DC
DR
MOB 200
ISP1
ISP2
MOB 50
ISP1
DMZ-PUB
WAF
WIFI-Guest
Nível 1
Cluster 2 Nós CheckPoint MOB200
CKP
Manager
Nível 1
CheckPoint MOB 50
CKP
DMZ-PUB
SRV-DEV
SRV-APPL
SRV-BDs
DMZ-INT
Nível 2 (L3 Interno)
Cluster 2 Nós
MPLS
Wifi-Users
PCs
SRV-APPL
SRV-BDs
Empresa 1
Empresa 2

ANEXO II
AUTO DE ACEITAÇÃO

Ao dia __ do mês de _____ do ano de 2023, nos termos e para os efeitos do disposto no na cláusula 9.ª do Contrato de ***Aquisição de Solução de Segurança Lógica Interna e Externa***, celebrado a [●] com o Cocontratante [●], declara-se que foi comprovado o fornecimento dos bens objeto do referido Contrato, em conformidade com as exigências aplicáveis.

Em consequência, decidiu-se notificar o Cocontratante da respetiva aceitação, através do presente auto.

E nada mais havendo a tratar, foi lavrado o presente auto.

_____

AdP VALOR

(Nome do Representante da Entidade Adjudicante)

_____

[●]

(Nome do Representante do Cocontratante)