

ÁGUAS DO NORTE, S.A.

CONCURSO PÚBLICO

**PRC_0128/2020_STI – ATUALIZAÇÃO,RENOVAÇÃO DE
LICENCIAMENTO E MANUTENÇÃO DA INFRAESTRUTURA DE
FIREWALL DA ÁGUAS DO NORTE (CHEK POINT)**

CADERNO DE ENCARGOS

CAPÍTULO I
DISPOSIÇÕES GERAIS
Cláusula 1.^a
Objeto

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual cujo objeto principal consiste na prestação, pelo adjudicatário, de serviços de atualização, renovação de licenciamento e manutenção da infraestrutura de firewall Check Point da Águas do Norte adiante designado por “*Atualização, Assistência Técnica, Licenciamento e Manutenção da Firewall Checkpoint*”, com observância das especificações constantes do **Anexo I** ao presente Caderno de Encargos.
2. Está incluído no objeto do presente contrato:
 - Atualização da infraestrutura atual para suportar alta disponibilidade;
 - O fornecimento e renovação do licenciamento;
 - A prestação de assistência técnica especializada;
 - Serviços Técnicos Especializados - 8x5 – Checkpoint;
 - Serviços Técnicos Especializados - 24x7x365 – Checkpoint;
 - Elaboração Relatórios Mensais;
 - O fornecimento e instalação de atualizações.

Cláusula 2.^a
Elementos do Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
 - a) O suprimento dos erros e das omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pela AdNorte para a decisão de contratar;
 - b) Os esclarecimentos e as retificações relativos ao caderno de encargos;
 - c) O presente caderno de encargos;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os elementos referidos no número anterior, a prevalência é determinada pela ordem pela qual são indicados nesse número.

4. Em caso de divergência entre os documentos referidos no número 2 e o clausulado contratual, prevalecem os primeiros salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos (CCP) e aceites pelo adjudicatário nos termos do disposto no artigo 101.º deste Código.

Cláusula 3.ª

Preço Base

1. O preço base do presente procedimento é de 75.000,00 EUR (cinquenta mil euros).
2. Não obstante o referido no número anterior, são ainda fixados os preços base unitários constantes do Anexo IV do Programa de Procedimento.
3. O parâmetro base fixado nos preceitos anteriores representa o preço máximo que a AdNORTE se dispõe a pagar pela aquisição objeto do contrato a celebrar.

Cláusula 4.ª

Prazo de vigência

1. O contrato a celebrar terá a duração de 3 (três) anos a contar da data da respetiva celebração, cessando o contrato no final desse período ou no momento em que a AdNorte, tenha pago ao Adjudicatário o preço total estimado da proposta adjudicada.
2. Sem prejuízo do disposto no número anterior, o adjudicatário dispõe do prazo máximo de 1 (semana) para instalar o licenciamento na mais recente versão.
3. A atualização para a nova arquitetura, integração, e configuração dos serviços solicitados para a solução, deve ficar concluído no prazo máximo de 1 (um) mês a contar da celebração do contrato.
4. A assistência técnica especializada e manutenção evolutiva da solução, é prestada durante o prazo de vigência do contrato nos termos estipulados no presente caderno de encargos.

CAPÍTULO II

OBRIGAÇÕES DAS PARTES

SECÇÃO I

OBRIGAÇÕES DO ADJUDICATÁRIO

Cláusula 5.ª

Obrigações do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável e no presente Caderno de Encargos, constituem obrigações principais do adjudicatário as seguintes:
 - a) Obrigação de fornecer as licenças e prestar os serviços de manutenção;
 - b) Obrigação de execução dos serviços identificados na sua proposta;
 - c) Disponibilizar o número suficiente de técnicos com qualificação técnico-científica adequada, de forma a garantir uma eficiente concretização dos objetivos definidos

no presente Caderno de Encargos, além de uma correta articulação entre o prestador de serviços e os representantes da AdNorte;

- d) Designar um responsável pela prestação de serviços de *Atualização, Assistência Técnica, Licenciamento e Manutenção da Firewall Checkpoint*;
 - e) Executar o serviço de “*Atualização, Assistência Técnica, Licenciamento e Manutenção da Firewall Checkpoint*” que lhe for adjudicado, tal como descrito no presente Caderno de Encargos, com absoluta subordinação aos princípios da ética profissional, isenção, independência, zelo e competência;
 - f) Cumprir as condições fixadas para a execução da “*Atualização, Assistência Técnica, Licenciamento e Manutenção da Firewall Checkpoint*”;
 - g) Sujeitar-se à ação fiscalizadora da AdNorte;
 - h) Garantir o sigilo quanto à informação a que o pessoal envolvido nos trabalhos venha a ter acesso;
 - i) Prestar as informações que forem solicitadas pela AdNorte;
 - j) Realizar todos os trabalhos previstos no Caderno de Encargos, nas condições de prazo e preço contratados;
 - k) A comunicação à AdNorte, logo que tenha conhecimento, dos factos que tornem total ou parcialmente impossível a execução do contrato ou a deteção de eventuais falhas que alterem a qualidade da prestação do serviço conforme especificado;
 - l) A informação, de forma correta e fidedigna, referente às condições em que se processa a execução contratual, bem como a prestação de todos os esclarecimentos solicitados pela AdNorte, designadamente pelo gestor de contrato que esta designar;
2. Comunicação de qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação social ou os seus representantes legais;
 3. A título acessório, o adjudicatário fica também 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.
 4. O adjudicatário é ainda responsável perante a AdNorte por qualquer defeito ou discrepância dos recursos materiais e informáticos afetos à prestação do serviço de *Atualização, Assistência Técnica, Licenciamento e Manutenção da Firewall Checkpoint*.
 5. O Adjudicatário obriga-se a cumprir a legislação em vigor em matéria de proteção jurídica dos programas de computador, nomeadamente o DL n.º 252/94, de 20 de Outubro, na sua atual redação, o Código do Direito de Autor e dos Direitos Conexos, aprovado pelo DL n.º 63/85, de 14 de Março, na sua atual redação e o Código da Propriedade Industrial, aprovado pelo DL n.º 36/2003, de 05 de Março, na sua atual redação.
 6. O Adjudicatário obriga-se ainda a observar o estabelecido em matéria de proteção de dados pessoais, nomeadamente com as orientações e determinações emanadas pelo Regulamento (EU) 2016/679, de 27 de abril de 2016 e demais normativos conexos.

Subsecção I
Âmbito dos serviços a fornecer

Cláusula 6.^a
Componente de assistência técnica e manutenção evolutiva

1. Os serviços relacionados com as componentes de assistência técnica e de manutenção evolutiva da solução serão prestados tendo como âmbito as instalações administrativas, técnicas e operacionais AdNorte, SA que constituem o Sistema Multimunicipal de Abastecimento de Água e Saneamento da Águas do Norte e serão executados na sede localizada em Vila Real e no pólo da ETA de Areias de Vilar (Barcelos).
2. A prestação dos serviços relacionados com a componente de manutenção evolutiva da solução inclui:
 - a) O fornecimento de novas versões e atualizações que compõem a infraestrutura de firewall, conforme descrito no **Anexo I** do presente Caderno de Encargos, bem como o acesso a correções do mesmo;
 - b) A disponibilização de novas funcionalidades que venham a ser desenvolvidas em cada um dos módulos, conforme descrito no **Anexo I** do presente Caderno de Encargos;
3. A prestação dos serviços relacionados com a componente de assistência técnica do inclui:
 - a) A assistência técnica especializada às ações de instalação, configuração e utilização da solução, conforme descrito no **Anexo I** do presente Caderno de Encargos, incluindo a
 - b) Correção de erros, anomalias e incidentes, assim como a verificação da implementação das aplicações previstas nas alíneas anteriores, nomeadamente através da realização de ciclos de teste e monitorização da conformidade;
 - c) A assistência técnica especializada, no modelo de bolsa de disponibilidade de horas, para a realização de trabalhos que envolvam suporte técnico especializado a prestar pelo adjudicatário.
4. Os serviços de suporte técnico especializado serão objeto de prévia solicitação pela AdNorte ou por sua prévia aprovação, neste último caso, se a iniciativa pertencer ao adjudicatário.
5. O suporte técnico especializado será prestado *in situ* nos locais indicados no número I da presente cláusula;
6. O suporte técnico especializado, se previamente autorizado pela AdNorte, além de adequada e tecnicamente suportado, pode ser prestado com base em acesso remoto às aplicações instaladas. Para tal, a AdNorte, poderá disponibilizar o referido acesso, dentro de um quadro de procedimentos de segurança a que o adjudicatário se encontra obrigado a observar.

7. As intervenções de suporte técnico especializado serão solicitadas, no *helpdesk* da AdNorte (SICO), originando o pedido de incidente, projeto ou de serviço, comunicado via correio eletrônico.
8. Nos termos deste Caderno de Encargos e relativos às componentes de manutenção evolutiva de *software* e assistência técnica especializada, serão considerados serviços não previstos quaisquer ações ou trabalhos que não possam ser enquadráveis em qualquer dos trabalhos previstos nos números anteriores.
9. Relativamente às mesmas componentes, quaisquer serviços não previstos só serão realizados por solicitação expressa da AdNorte, ou por proposta do adjudicatário, mediante acordo prévio da AdNorte, sendo sempre efetuados dentro das condições aqui definidas, ou outras que venham a ser para o efeito acordadas.

Cláusula 8.^a **Níveis de serviço – SLA**

- I. A resposta aos pedidos de intervenção, operacional ou funcional, no sistema InLAB deve ser executada dentro dos seguintes prazos:

A. Intervenção Operacional

- a) 2 (*duas*) horas, contadas a partir da receção de pedido de suporte técnico especializado, independentemente do meio utilizado, classificadas de prioridade elevada e que respeitem a pedidos que visem a resolução de problemas com consequências muito graves, que impeçam a realização de tarefas críticas para a AdNorte, designadamente por completa falha ou paragem do sistema, bem como por erros de funcionamento que afetem as principais funções;
- b) 4 (*quatro*) horas, contadas a partir da receção de pedido de suporte técnico especializado, independentemente do meio utilizado, classificadas de prioridade normal e que respeitem a pedidos que visem a resolução de problemas que impeçam a realização de tarefas para a AdNorte, designadamente, em consequência da inoperacionalidade ou erro de funções gerais;

B. Intervenção funcional

- a) 4 (*quatro*) horas, contadas a partir da receção de pedido de suporte técnico, independentemente do meio utilizado, classificadas de prioridade muito elevada e que respeitem a pedidos de configuração, parametrização e/ou planeamento com carácter muito urgente;
- b) 1 (*um*) dia útil, contadas a partir da receção de pedido de suporte técnico, independentemente do meio utilizado, classificadas de prioridade elevada e que respeitem a pedidos de configuração, parametrização e/ou planeamento com carácter urgente;
- c) 5 (*cinco*) dias úteis, contadas a partir da receção de pedido de suporte técnico, independentemente do meio utilizado, classificadas de prioridade normal e que respeitem a pedidos de configuração, parametrização e/ou planeamento com carácter intermédio;
- d) 2 (*duas*) semanas, contadas a partir da receção de pedido de suporte técnico, independentemente do meio utilizado, classificadas de prioridade baixa e que

respeitem a pedidos de configuração, parametrização e/ou planeamento com caracter baixo;

2. As intervenções de manutenção e suporte devem ser realizadas em dias úteis, exceto em caso de indicação em contrário por parte da entidade adjudicante.
3. Os pedidos de suporte, ainda que possam ser remetidos por qualquer meio, serão sempre enviados / confirmados, por escrito, para o email a indicar pelo adjudicatário, sendo que o prazo para execução de cada um dos serviços inicia, desde logo, com o pedido inicial.

Cláusula 9.^a

Demonstração de conformidade, testes e aceitação dos serviços

1. Efetuada a execução dos serviços relativos à componente de fornecimento e instalação do licenciamento, a AdNorte, por si ou através de terceiro por ela designado, procede, no prazo de 5 (*cinco*) dias, à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar, respetivamente, se estes correspondem às quantidades estabelecidas no presente Caderno de Encargos e se reúnem as características, especificações e requisitos técnicos e operacionais definidos no presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.
2. No caso da demonstração de conformidade e os testes previstos na cláusula anterior não comprovarem a total operacionalidade dos serviços objeto do contrato, bem como a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos definidos no presente Caderno de Encargos, a AdNorte deve disso informar, por escrito, o adjudicatário.
3. No caso previsto no número anterior, o adjudicatário deve proceder, à sua custa e no prazo razoável que for determinado pela AdNorte, ao suprimento e correção das irregularidades e desconformidades apresentadas, garantindo o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
4. Durante a fase de realização das correções, o adjudicatário deve prestar à AdNorte toda a cooperação e todos os esclarecimentos entendidos necessários, através de pessoas devidamente credenciadas para o efeito.
5. Os encargos com a realização das correções, devidamente comprovados, são da responsabilidade do adjudicatário.
6. Após a realização das substituições necessárias pelo adjudicatário, no prazo respetivo, a AdNorte procede à realização de novos testes de aceitação, nos termos da cláusula anterior.
7. Caso as verificações e os testes a que se refere o ponto 1 da presente cláusula comprovem a total operacionalidade dos serviços objeto do contrato, bem como a sua conformidade com as exigências legais e neles não sejam detetados quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos, a AdNorte deve disso informar, por escrito, o adjudicatário.
8. O adjudicatário obriga-se a manter os serviços objeto do presente contrato, durante todo o prazo da sua execução, em total operacionalidade e observância das

características, especificações e requisitos técnicos definidos no presente Caderno de Encargo, bem como a sua conformidade com as exigências legais.

Cláusula 10.^a
Direitos de propriedade intelectual e industrial

1. O adjudicatário terá que demonstrar ser titular de todas as licenças, autorizações ou demais atos de consentimento legalmente necessários à utilização de *software* e demais soluções ou produtos por si utilizados na execução do contrato a celebrar.
2. O adjudicatário obriga-se a manter válidas as licenças, autorizações ou demais atos de consentimento a que se refere o número anterior, até à integral execução dos serviços contratados.

Cláusula 11.^a
Conformidade e garantia técnica

O adjudicatário fica sujeito, com as devidas adaptações e no que se refere aos elementos entregues à AdNorte em execução do contrato, às exigências legais, às obrigações do fornecedor e prazos respetivos aplicáveis aos contratos de aquisição de serviços, nos termos do Código dos Contratos Públicos e demais legislação aplicável.

SUBSECÇÃO I
DEVER DE SIGILO

Cláusula 12.^a
Objeto do dever de sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à AdNorte, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 13.^a
Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor depois de terminado o 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.

SECÇÃO II
OBRIGAÇÕES DA ADNORTE
Cláusula 14.^a
Preço contratual

1. O preço contratual corresponderá ao somatório dos valores resultantes da aplicação dos preços unitários da proposta adjudicada aos bens e serviços que efetivamente venham a ser fornecidos e executados, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à AdNorte, nomeadamente os relativos ao alojamento, alimentação e deslocação de meios humanos, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 15.^a
Condições de pagamento

1. As quantias devidas pela AdNorte, nos termos da(s) cláusula(s) anterior(es), deve(m) ser paga(s) no prazo de 30 (*trinta*) dias após a receção pela AdNorte das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. A obrigação considera-se vencida quando for efetuada a entrega de bens, e após a realização dos serviços solicitados pela AdNorte.
3. As faturas a apresentar pelo Adjudicatário à AdNorte, devem conter os elementos necessários a uma completa, clara e adequada compreensão dos valores faturados, os quais devem ser apresentados de forma desagregada em documento anexo a cada fatura. Em caso de discordância por parte da AdNorte quanto aos valores indicados nas faturas, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. Desde que devidamente emitidas e observado o disposto nos pontos anteriores, da presente Cláusula, as faturas devem ser apresentadas até ao dia 4 do mês seguinte a que se referem, conter a menção da respetiva nota de encomenda e são pagas através de transferência bancária.

CAPÍTULO III
PENALIDADES CONTRATUAIS E RESOLUÇÃO
Cláusula 16.^a
Penalidades contratuais

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

- a) Pelo incumprimento das datas e prazos de execução dos serviços prestados objeto do contrato, até 10% do valor do contrato;
- b) Pelo incumprimento da obrigação de garantia técnica, até 5% do valor do contrato;
- 2. Em caso de resolução do contrato por incumprimento do adjudicatário, a AdNorte pode exigir-lhe uma pena pecuniária até 20% do valor global do contrato.
- 3. Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo adjudicatário ao abrigo da alínea a) do n.º I, relativamente aos bens objeto do contrato cujo atraso na entrega tenha determinado a respetiva resolução.
- 4. Na determinação da gravidade do incumprimento, a AdNorte tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.
- 5. A AdNorte 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 AdNorte exija uma indemnização pelo dano excedente.

Cláusula 17.ª

Força maior

- 1. Não podem ser impostas penalidades ao adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
- 2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
- 3. Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que 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 adjudicatário de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;

- e) Incêndios ou inundações com origem nas instalações do adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do adjudicatário não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros;
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
 5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 18.^a **Resolução por parte da AdNorte**

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a AdNorte pode resolver o contrato, a título sancionatório, no caso de o adjudicatário 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 adjudicatário e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pela AdNorte.

Cláusula 19.^a **Resolução por parte do adjudicatário**

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o adjudicatário pode resolver o contrato quando:
 - a) Qualquer montante que lhe seja devido esteja em dívida há mais de 6 (seis) meses ou o montante em dívida exceda 20% do preço contratual, excluindo juros.
2. O direito de resolução é exercido por via judicial.
3. Nos casos previstos na alínea a) do n.º 1, o direito de resolução pode ser exercido mediante declaração enviada à AdNorte, que produz efeitos 30 (*trinta*) dias após a receção dessa declaração, salvo se este último cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.
4. A resolução do contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pelo adjudicatário, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do Código dos Contratos Públicos.

CAPÍTULO IV
SEGUROS
Cláusula 20.^a
Seguros

1. O adjudicatário é obrigado a celebrar e a manter válido, um seguro de responsabilidade civil profissional, garantindo a responsabilidade por danos decorrentes de ações ou omissões praticadas no exercício da sua atividade conexas com o objeto desta prestação de serviços, abrangendo quaisquer pessoas de que se sirva na sua atividade.
2. O capital mínimo a segurar é de 150.000,00 EUR (cento e cinquenta mil euros).
3. O referido seguro deverá ser contratado junto de uma seguradora autorizada a exercer a atividade em Portugal.
4. O adjudicatário obriga-se também a celebrar e a manter válido um seguro de acidentes de trabalho
 - a) O adjudicatário ficará responsável pelo pagamento de todos os encargos sociais estabelecidos na lei a todo o seu pessoal.
 - b) O adjudicatário obriga-se a efetuar apólices de seguro que cobrirão acidentes de trabalho e doenças profissionais, bem como a mantê-las válidas até à conclusão do contrato, nos termos da legislação em vigor.
5. O adjudicatário obriga-se ainda a segurar os meios de transporte que sejam empregues na aquisição de serviço, bem como todas as pessoas nelas transportadas na qualidade de passageiros, seja quem for, estas últimas, com valor ilimitado de responsabilidade civil.
6. Os encargos referentes aos seguros impostos por este Caderno de Encargos, bem como qualquer dedução efetuada pela Seguradora a título de franquia, em caso de sinistro indemnizável, serão por conta do adjudicatário.
7. A AdNorte pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos na presente cláusula, devendo o adjudicatário fornecê-la no prazo 5 (cinco) dias.

CAPÍTULO V
RESOLUÇÃO DE LITÍGIOS
Cláusula 21.^a
Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Mirandela com expressa renúncia a qualquer outro.

CAPÍTULO VI
DISPOSIÇÕES FINAIS
Cláusula 22.^a
Subcontratação e cessão da posição contratual

A subcontratação pelo adjudicatário e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do Código dos Contratos Públicos.

Cláusula 23.^a
Comunicações e notificações

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

Cláusula 24.^a
Contagem dos prazos

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

Cláusula 25.^a
Legislação aplicável

O contrato é regulado pela legislação portuguesa.

ANEXO I

ESPECIFICAÇÕES TÉCNICAS

1. Âmbito

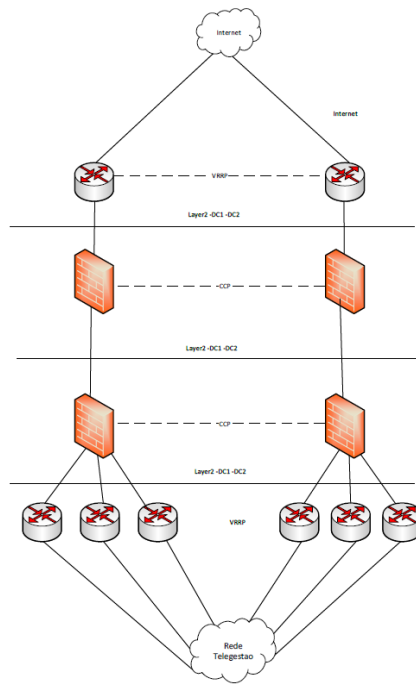
A Águas do Norte pretende renovar a atual infraestrutura de segurança de firewall Checkpoint (pólo de Barcelos) e a atualização da solução de Disaster Recovery (Porto). Assim deve ser previsto um upgrade da solução existente, contemplando a eliminação de máquinas virtuais e devem ser contemplados 2 (dois) equipamentos para Alta Disponibilidade. A solução deve ser compatível e integrada com a atual solução checkpoint instalada da Águas do Norte e toda ela gerida através da mesma consola.

Toda a solução deve ser baseada em *software* Checkpoint, devendo ser alterada e configurada, com a inclusão da Sandbox de validação de ameaças. A proposta deve incluir uma bolsa de horas de serviços de instalação, configuração, migração de serviços, testes e documentação da infraestrutura, em horário laboral, bem como a transferência de conhecimentos de operação à equipa técnica da Águas do Norte que lhe permita a operação e gestão da solução. A proposta deve incluir ainda uma bolsa de horas de serviços de manutenção reativa e proactiva, em complemento ao suporte (reativo) disponibilizado pelos respetivos fabricantes, que deverá ser utilizada indiscriminadamente pela Águas do Norte para apoio e consultoria relativamente à solução implementada, em tarefas de melhoria, otimização da infraestrutura, apoio à utilização da solução e instalação (reativa ou proactiva) de atualizações e/ou novas versões. Mensalmente o fornecedor deve entregar um relatório, identificando os seguintes pontos, para cada pedido de trabalhos:

- Número: Incidente (I), Serviço (S) ou Projeto (P) gerado previamente pelo ISTM da AdNorte;
- Descrição genérica;
- Ações realizadas;
- Pessoas envolvidas em cada trabalho (interno e externo);
- Número de horas consumidas;
- Impacto (se aplicável);
- Propostas de melhoria (se aplicável).

2. Solução

2.1. Arquitetura



2.2. Funcionalidades gerais

- Suporte de clustering em Activo-Activo e Activo-Passivo
- Suporte de clustering com mais de 2 membros num mesmo cluster
- Detecção em tempo real de protocolos dinâmicos (ex: FTP, SIP, H323, etc.)
- Detecção/bloqueio de serviços como P2P e IM por aplicação (voz, vídeo ou file sharing)
- Agrupamento de regras
- NAT de aplicações em tempo real
- PAT
- NAT/PAT baseado em regras
- Autenticação de serviços
- Integração com Active Directory, LDAP e/ou base de dados local de utilizadores
- Autenticação de 2 fatores (p. ex. tokens físicos, soft tokens, SMS e email)
- 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 criação de gateways virtuais

2.3. Networking

- Suporte Múltiplos Links WAN - Redundância e/ou Balanceamento de carga
- Routing baseado em políticas
- Rotas Estáticas
- 802.1q- VLAN Tagging

- DHCP Relay e DHCP Server
- Spanning-Tree (802.1d)
- Suporte 802.3ad e LACP - Agregação de Links (Activo-Activo ou Activo-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

2.4. 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

2.5. 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

2.6. VPN (integrado na gateway)

- 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 de OTP para VPN sem recurso a terceiros fabricantes ou servidores adicionais
- Aplicação de políticas e restrições de acesso por utilizador ou por grupo de utilizadores
- Single Sign On VPN

2.7. IDS/IPS (integrado na gateway)

- 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
- Motor com mecanismos de deteção de assinaturas de exploits, anomalias protocolares, controlos de aplicação e deteção comportamental
- Motor com proteções existentes de SCADA
- Suporte de motor de deteção de Antibot
- Protocol Tunneling Recognition
- Capacidade de criação de perfis de proteção para apenas cliente, servidores ou ambos

2.8. Application Control e URL Filtering (integrado na gateway)

- Atualização automática de assinaturas
- Reconhecimento de ≥ 4.000 aplicações
- Reconhecimento de ≥ 250.000 widgets (sub aplicações dentro das principais Apps 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 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

2.9. Anti-Bot e Antivírus (integrado na gateway)

- Atualização automática e em tempo real de assinaturas
- Capacidade de detetar e parar comportamentos anómalos na rede
- Deteção em arquitetura multicamada que inclua reputação de IPs, 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 seletivamente tráfego com criptografia SSL
- Correlação centralizada de eventos e mecanismos de reporting

2.10. Sistema de Prevenção de Intrusão

A solução deve ter um sistema *Intrusion Prevention System* (IPS) que combine proteção com uma performance avançada, disponibilizando uma completa e proactiva proteção contra intrusões integrada na solução de *firewall* implementada. O IPS deve complementar a proteção de *firewall*, acrescentando mais um nível de securitização da rede, sem comprometer o desempenho da *gateway*.

Esta proteção contra tráfego malicioso e indesejado, deve prevenir um vasto leque de ameaças como ataques *malware*; ataques Dos e DDoS; vulnerabilidades de aplicações e servidores; ameaças internas e tráfego de aplicações indesejadas como o IM e o P2P.

Para atingir este objetivo de uma tão vasta e profunda prevenção de ameaças, o IPS deve ser constantemente atualizado, a partir dos laboratórios do fabricante, com informação sobre milhares de proteções e com análise profunda de dezenas de protocolos, permitindo a deteção e prevenção constante das principais ameaças de segurança do momento e, muitas vezes, de ameaças futuras.

A solução deve ter a possibilidade de definição de perfis de proteção por âmbito (protection profiles per scope) que na prática permitirá a conjugação livre de qualquer uma das componentes de proteção (IPS + Anti-Bot + Anti-Virus + Threat Emulation + Threat Extraction) e que deve permitir traduzir numa otimização das proteções ativas contra ameaças e da performance de análise, para cada perfil de tráfego definido.

O processo de atualização das assinaturas de IPS, deve ser um processo interativo que requer alguma disponibilidade para validação e aprovação dos logs do tráfego inspecionado.

O motor de IPS deve implementar uma solução de multicamada de defesas, protegendo a Águas do Norte e o servidor, através de uma análise continua ao tráfego com as seguintes verificações:

- Deteção e prevenção específica de exploits conhecidos;
- Deteção e prevenção de vulnerabilidades, como por exemplo CVEs específicos;
- Deteção e prevenção de utilização indevida de protocolos, como por exemplo o HTTP, SMTP, POP e IMAP que muitas vezes indiciam uma atividade maliciosa ou uma potencial ameaça;
- Deteção e prevenção de comunicações externas de malware;
- Deteção e prevenção de estabelecimento de túneis não identificados, que indiciam fugas de dados ou tentativas de contornar mecanismos de proteção;
- Deteção, prevenção ou restrição de certas aplicações que, muitas vezes, representam ameaças para a rede ou consomem grande parte da largura de banda disponível;
- Deteção e prevenção de ataques genéricos e sem assinaturas pré-definidas, como por exemplo o Malicious Code Protector.

O sistema IPS deve inspecionar detalhadamente o tráfego para determinar as ameaças que nele possam estar inseridas, deverá ser feita a inspeção do tráfego encriptado em SSL. Sempre que possível, deverá ser habilitada a inspeção SSL em conjugação com o IPS, maximizando a deteção e prevenção de ameaças na globalidade do tráfego inspecionado. Para habilitar esta funcionalidade, e muito especificamente para o tráfego que vem do exterior com destino a aplicações internas das Águas do Norte, serão disponibilizados os certificados e chaves privadas dessas aplicações, para que sejam aprovisionadas na gateway Check Point e dessa forma evitar que sejam mostrados erros de certificados aos clientes que utilizam essas aplicações.

2.1.1. Identity Awareness

A funcionalidade de Identity Awareness deve ser incluída permitindo definir e criar políticas de acesso baseadas em identidades, com granularidade de identificação por utilizadores, grupos ou máquinas. Com base na ativação desta funcionalidade é possível criar políticas que controlam o seguinte tipo de atividades:

- Definir utilizadores/grupos com permissões de acesso à Internet ou a determinadas aplicações;
- Controlo granular de acessos a aplicações ou redes por utilizador, grupo ou máquina;

- Limitar acessos a determinadas aplicações para utilizadores ligados remotamente;
- Diferenciar utilizadores entre colaboradores internos, externos (outsourcers) e convidados;
- Prevenir ameaças e fuga de dados com a limitação de acessos por tipo utilizador e máquina.

O módulo de Identity Awareness deve integrar de forma transparente com a Active Directory (AD) bastando garantir a sua conectividade com a consola de gestão Check Point e ficando deste modo capacitado para identificar utilizadores, grupos ou máquinas existentes. Sendo esta a forma mais simples e rápida de ativar esta funcionalidade, iniciando a definição de políticas com base nas identidades existentes na AD, existem, contudo, outras possibilidades de integração através de:

- Captive Portal - os utilizadores que tentem aceder a um recurso para o qual não têm uma política de permissão, são encaminhados para um portal de autenticação onde têm de colocar as suas credenciais de identificação;
- Endpoint Identity Agents - agentes aplicativos que se instalam nas máquinas dos utilizadores, adquirindo conhecimento da identidade e reportando para a consola de gestão;
- Remote Access (VPN SSO) - utilizadores que acessem por VPN Check Point ficam com a sua identidade registada na consola de gestão para efeitos de validação de acessos através das políticas do Identity Awareness.

2.12. Bundle NGTX (SandBlast)

O SandBlast deve implementar uma arquitetura de defesa multicamada que filtre possíveis ameaças usando análises sofisticadas, para otimizar a eficiência e garantir uma resposta a qualquer tipo de ataque (incluindo worms, ransomware, malware sem ficheiro, spyware, etc) sem comprometer o desempenho ou a segurança da rede.

O SandBlast Zero Day Threat Detection deve integrar análise estática, análise dinâmica, Algoritmos de *Machine Learning* baseados em IA e comportamental, implementados em mais de 40 motores de deteção para garantir a máxima deteção e taxas de captura.

Além disso, a SandBlast deve utilizar mecanismos de deteção de nível de CPU para detetar explorar tentativas durante a fase de pré-infeção e parar os ataques antes de eles terem a oportunidade de evitar a deteção pela sandbox.

Mais de 70 tipos de ficheiros, incluindo: documentos e modelos do Microsoft Office, EXE, DLL, arquivos (ISO, ZIP, 7Z, RAR, etc.), PDF, Flash, Java, scripts e muito mais.

2.13. Sandblast - Protecção de ataques Zero-Day

Com a solução deveremos conseguir ter:

- a capacidade de protecção contra ataques de "Zero-Day" antes das proteções serem criados;
- a capacidade de análise e deteção de malware em documentos comerciais, tais como Adobe PDFs e ficheiros de MS Office, bem como EXE e ficheiros Zip;
- a capacidade de executar dentro do equipamento local ou num sistema na cloud do fabricante;
- a capacidade de ter zero falsos positivos (não existência de falsos positivos);
- a capacidade de emular ataques contra vários ambientes do sistema operativos Windows, pelo menos: Windows XP, Windows 7, Windows 8;

- a capacidade de ser gerida centralmente;
- a capacidade de aumentar a segurança através da partilha automática de informações novos ataques detetados com outras gateways gerando automaticamente as assinaturas para as bloquear noutros equipamentos;
- uma solução de sandboxing com a capacidade de inspecionar e bloquear ataques que passam via HTTPS sem o uso de dispositivos adicionais.
- uma solução de sandboxing capaz de poder ser implementado inline, na nuvem, num equipamento out of band ou com um MTA - Mail Transfer Agent;

A solução:

- de sandboxing deve combinar a validação/análise de ficheiros com Threat Extraction;
- de threat emulation deve ter como opção "Restrição Geo", restringindo a emulação a um país específico;
- deve ser flexível ao ponto de permitir manter o formato do ficheiro original e especificar o tipo de conteúdo a ser removido;
- de Threat Extraction deve disponibilizar, imediatamente, uma versão limpa do documento ao utilizador, dando acesso ao documento original apenas após análise e confirmação de que o documento não é malicioso.

3. Requisitos mínimos do perfil dos recursos a disponibilizar

3.1. Perfil I - Administrador de redes e comunicações:

- Licenciatura nas áreas de Engenharia Informática, Engenharia Eletrotécnica ou na área de Sistemas e Tecnologias de Informação;
- Experiência comprovada no mínimo de 7 (sete) anos;
- Certificação HPE Switches and Routers Service Qualification;
- Certificação HP ATP - FlexNetwork Solutions V3 ATP-FlexNetV3;
- Certificações CCDA (Design) ou equivalente;
- Experiência comprovada em pelo menos dois fabricantes de networking (Cisco, Nortel, HP, Awaysa);
- Experiência comprovada em pelo menos duas implementações de soluções de networking de âmbito Nacional;
- Experiência comprovada na gestão e configuração em soluções de switching (core e distribuição), Routing e Wireless em cenários empresariais e distribuídos geograficamente;
- Experiência comprovada na implementação de QoS (Quality of Service) em redes locais (wired e wireless) e redes alargadas;
- Experiência comprovada na implementação de protocolos BGP (redes privadas e redes públicas);
- Experiência comprovada em pelo menos duas implementações de soluções de networking de âmbito Nacional;
- Experiência comprovada na gestão e configuração em soluções de switching (core e distribuição), Routing e Wireless em cenários empresariais e distribuídos geograficamente.

3.2. Perfil II - Administrador de redes e comunicações:

- Experiência comprovada no mínimo de 7 (sete) anos;

- Certificação Cisco IP NGN System Engineer Representative;
- Experiência comprovada na implementação de QoS (Quality of Service) em redes locais (wired e wireless) e redes alargadas;
- Experiência comprovada na implementação de protocolos BGP (redes privadas e redes públicas);
- Experiência comprovada em pelo menos duas implementações de soluções de networking de âmbito Nacional;
- Experiência comprovada na gestão e configuração em soluções de switching (core e distribuição), Routing e Wireless em cenários empresariais e distribuídos geograficamente.

3.3. Perfil III - Administrador de plataformas Check Point:

- Licenciatura nas áreas de Engenharia Informática, Engenharia Eletrotécnica ou na Área de Sistemas e Tecnologias de Informação;
 - Experiência profissional mínima de 7 (sete) anos em administração de soluções de segurança;
 - Certificação Check Point Certified Expert (CCSE ou superior) válida comprovada;
 - Este técnico deverá ser responsável técnico pela conta da Águas do Norte, S.A.
- A ÁGUAS DO NORTE, S.A. reserva-se o direito de interditar provisória ou definitivamente o acesso às instalações, do pessoal do Adjudicatário que não tenha respeitado qualquer regulamento ou norma de segurança, sem que isso implique qualquer indemnização.
- Toda e qualquer alteração à equipa técnica terá de ser comunicada, juntamente com o respetivo curriculum vitae, certificados de habilitação e de formação na área, e sujeita à prévia aprovação da ÁGUAS DO NORTE, S.A.
- A ÁGUAS DO NORTE, S.A. pode impor formalmente a substituição dos trabalhadores que não ofereçam garantia de aptidão técnica, ou vierem a revelar-se indisciplinados, conflituosos ou desrespeitadores dos regulamentos internos da ÁGUAS DO NORTE, S.A.