

**Aquisição e instalação de dispositivos de
prevenção de ameaças de última geração com
segurança de terminal integrada**



CONCURSO PÚBLICO

Caderno de Encargos

PRC I30/2022

CAPÍTULO I

DISPOSIÇÕES GERAIS

Cláusula 1.^a

Objeto

1. O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto principal a aquisição e instalação de dispositivos de prevenção de ameaças de última geração com segurança de terminal integrada.
2. O objeto do contrato abrange ainda serviços de manutenção da solução.

Cláusula 2.^a

Contrato

1. O contrato integra os seguintes elementos:
 - a) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelo(s) concorrente(s) 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 adjudicada;
 - e) Os esclarecimentos sobre a proposta prestados pelo adjudicatário.
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 entidade adjudicante nos termos previstos no artigo 99.º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos previstos no artigo 101.º do mesmo diploma legal prevalecem sobre todos os documentos previstos no n.º 1 da presente cláusula.

Cláusula 3.^a

Prazo contratual

O contrato inicia-se em 01/01/2023, mantendo-se em vigor pelo prazo de 36 (trinta e seis) meses, sem prejuízo das obrigações acessórias que perdurem para além da cessação do contrato.

CAPÍTULO II

OBRIGAÇÕES DAS PARTES

SECÇÃO I

OBRIGAÇÕES DO COCONTRATANTE

Cláusula 4.^a

Obrigações do Cocontratante

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) Obrigação de fornecimento dos bens com as características técnicas definidas no Anexo I do Caderno de Encargos;
- b) Instalação dos bens identificados na sua proposta, nos locais identificados no Anexo II do CE;
- c) Obrigação de garantia dos bens;
- d) Obrigação de continuidade de fabrico;

Cláusula 5.^a

Conformidade e operacionalidade dos bens

- 1. O Cocontratante obriga-se a entregar à Contraente Pública os bens objeto do contrato com as características, especificações e requisitos técnicos previstos no Anexo I ao presente caderno de encargos, que dele faz parte integrante.
- 2. Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
- 3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas no que respeita à

conformidade dos bens a entregar.

4. O Cocontratante é responsável perante a Contraente Pública por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Cláusula 6.^a

Entrega dos bens

1. Os bens objeto do contrato devem ser entregues nos locais definidos no Anexo II.
2. O Cocontratante obriga-se a disponibilizar, simultaneamente com a entrega dos bens objeto do contrato, todos os documentos que sejam necessários para a boa e integral utilização ou funcionamento daqueles.
3. Com a entrega dos bens objeto do contrato, ocorre a transferência da sua posse e da propriedade para a Contraente Pública, bem como do risco de deterioração ou perecimento dos mesmos, sem prejuízo das obrigações de garantia que impendem sobre o Cocontratante.
4. Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local da entrega, bem como a respetiva instalação, são da responsabilidade do Cocontratante.

Cláusula 7.^a

Inoperacionalidade, defeitos ou discrepâncias

1. Caso se verifique a total ou parcial inoperacionalidade dos bens objeto do contrato, bem como a sua desconformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no Anexo I ao presente caderno de encargos, a Contraente Pública deve informar, por escrito, o Cocontratante.
2. No caso previsto no número anterior, o Cocontratante deve proceder, à sua custa e no prazo razoável que for determinado pela Contraente Pública, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
3. Após a realização das alterações ou substituições necessárias pelo Contraente Pública no prazo respetivo, a Contraente Pública procede a nova análise.

Cláusula 8.^a

Garantia técnica

1. Nos termos da presente cláusula e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, o Cocontratante garante os bens objeto do contrato, pelo prazo de 3 anos a contar da data de entrega dos bens, contra quaisquer defeitos ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos definidos no Anexo I ao presente caderno de encargos, que se revelem a partir da respetiva aceitação do bem.
2. A garantia prevista no número anterior abrange:
 - a) O fornecimento, a montagem ou a integração de quaisquer peças ou componentes em falta;
 - b) A desmontagem de peças, componentes ou bens defeituosos ou discrepantes;
 - c) A reparação ou substituição das peças, componentes ou bens defeituosos ou discrepantes;
 - d) O fornecimento, a montagem ou instalação das peças, componentes ou bens reparados ou substituídos;
 - e) O transporte do bem ou das peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens ou a entrega das peças ou componentes em falta, reparados ou substituídos;
 - f) A deslocação ao local da instalação ou de entrega;
 - g) A mão-de-obra.
3. No prazo máximo de dois meses a contar da data em que a Contraente Pública tenha detetado qualquer defeito ou discrepância, esta deve notificar o Cocontratante, para efeitos da respetiva reparação.
4. A reparação ou substituição previstas na presente cláusula devem ser realizadas dentro de um prazo razoável fixado pela Contraente Pública e sem grave inconveniente para esta, tendo em conta a natureza do bem e o fim a que o mesmo se destina.

Cláusula 9.^a

Garantia de continuidade de fabrico

O Cocontratante deve assegurar a continuidade do fabrico e do fornecimento de todas as peças, componentes e equipamentos que integram os bens objeto do contrato até 31 dezembro de 2025.

Cláusula 10.^a

Serviços

1. O Cocontratante é obrigado a prestar os serviços de instalação dos equipamentos.
2. O Cocontratante é ainda obrigado a prestar os serviços de suporte presencial em qualquer um dos locais previstos no Anexo II no decurso do prazo de execução do contrato.
3. Os serviços referidos no número anterior compreendem, designadamente:
 - a) Reunir condições técnicas e operacionais que lhe permitam operar as soluções Checkpoint atualmente existentes e assegurar o respetivo suporte por parte do fabricante;
 - b) Efetuar a reconfiguração da rede referente ao centro de dados migrando todas as configurações do cluster atualmente existente e em produção para o novo;
 - c) Implementar todas as regras de segmentação necessárias no sentido de garantir a sua adequação ao modelo atual de funcionamento;
 - d) Prestar o devido apoio aos diferentes integradores que estejam envolvidos no processo de implementação das soluções atualmente existentes;
 - e) Articular junto dos operadores de telecomunicações a integração das redes oT e implementar as alterações necessárias assim como os devidos mecanismos de segurança;
 - f) Implementar todas as configurações de rede necessárias à implementação do centro de dados de recuperação de desastre e em articulação com todas as entidades envolvidas neste processo (operadores, integradores de sistemas e entidade gestoras das infraestruturas e instalações DR);
 - g) No decorrer dos processos de implementação o Cocontratante deverá garantir suporte 24 horas por dia/7 dias por semana, bem como assegurar a reconfiguração de todos os equipamentos de rede e segurança em horário pós-laboral (17h00 às 8h30);
 - h) Proceder à instalação física dos equipamentos segundo especificações técnica facultadas

no momento de instalação pelos serviços técnicos da Contraente Pública;

- i) Configurar a monitorização nativa para todos os elementos de hardware e software que suportam a solução;
- j) Definir, em conjunto com a Contraente Pública, a execução de testes funcionais de resiliência a toda solução implementada;
- k) Redigir toda a documentação de instalação, configuração e manutenção dos ambientes;
- l) Assegurar a formação da equipa Contraente Pública no conjunto de tecnologias implementadas (incluindo, definição de políticas, reporting, upgrade, etc.);
- m) Complementarmente aos serviços de suporte garantidos pelo fabricante, o Cocontratante deverá assegurar os serviços de manutenção e atualização de todas as soluções instaladas no âmbito do presente contrato, sem limite de intervenções/horas de suporte em horário pós-laboral.
- n) É também da sua responsabilidade a manutenção física dos equipamentos e instalação das respetivas atualizações de software em horário pós-laboral, articulando as suas intervenções com as equipas técnicas da Contraente Pública.

Cláusula 11.ª

Dever de sigilo

- 1. O Cocontratante obriga-se a não divulgar quaisquer informações e documentação, técnica e não técnica, comercial ou outra, relativa à Contraente Pública, de que venha a ter conhecimento ao abrigo ou em relação com a execução do contrato.
- 2. O Cocontratante obriga-se também a não utilizar as informações obtidas para fins alheios à execução do contrato.
- 3. 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 Contraente Pública lhe indique para esse efeito.
- 4. O dever de sigilo mantém-se em vigor até ao termo do prazo de 10 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.

Cláusula 12.^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 Contraente Pública, 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 Contraente Pública 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 Contraente Pública, ou por quem atue em representação desta.
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 Contraente Pública, 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 Contraente Pública quaisquer reclamações ou questões colocadas pelos titulares dos dados pessoais.
10. O Cocontratante encontra-se adstrito a notificar de imediato a Contraente Pública 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 a Contraentes Pública, por escrito, disponibilizando-lhe uma descrição da violação de dados ocorrida, informando-a das categorias e número de titulares de dados afetados, das prováveis consequências da violação, assim como fornecendo-lhes qualquer outra informação que possam 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 para a Contraente Pública:
 - 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 Contraente Pública por todos os prejuízos em que venham a incorrer em virtude da utilização ilegal e/ou ilícita de dados pessoais, nomeadamente por indemnizações e despesas em que tenham 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 mesmo é fundamento de resolução do presente contrato com justa causa pela Contraente Pública, podendo implicar o dever de indemnização por eventuais violações que lhe sejam imputadas.

Cláusula 13.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 Contraente Pública.
2. Dependendo da opção da Contraente Pública, 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 14.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 Contraente Pública, exceto se for obrigado a fazê-lo pela legislação aplicável, ficando obrigado a informar, nesse caso, a Contraente Pública antes de proceder a essa transferência.

Cláusula 15.ª

Dever de cooperação

O Cocontratante deve cooperar com a Contraente Pública 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 Contraente Pública;

- 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 CONTRAENTE PÚBLICA

Cláusula 16.^a

Preço base e preço contratual

1. O preço contratual não pode ser superior a 199.850,00 EUR (cento e noventa e nove mil oitocentos e cinquenta euros).
2. Pelo fornecimento dos bens objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a Contraente Pública 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 total é estimado, por ser variável em função do número de equipamentos que venham efetivamente a ser fornecidos e/ou instalados, razão pela qual a Contraente Pública apenas pagará os bens que venham a ser real e efetivamente fornecidos/instalados, por aplicação dos preços unitários propostos.
4. As quantidades apresentadas no presente de Caderno de Encargos são meramente indicativas, destinando-se, essencialmente, à determinação do preço total estimado.
5. A Contraente Pública reserva-se o direito de não adquirir bens na totalidade do valor contratual.
6. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à Contraente Pública, nomeadamente os relativos ao transporte dos bens objeto do contrato para o respetivo local de entrega, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 17.^a

Remuneração dos serviços

Os serviços previstos no Anexo I do presente Caderno de Encargos são remunerados de acordo com os preços unitários correspondentes, nos termos da proposta apresentada.

Cláusula 18.^a

Condições de pagamento

1. A(s) quantia(s) devida(s) pela Contraente Pública, nos termos da(s) cláusula(s) anterior(es), deve(m) ser paga(s) no prazo de 60 (sessenta) dias após a receção pelo mesmo das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. Para os efeitos do número anterior, a obrigação considera-se vencida com a entrega e instalação dos bens objeto do contrato.
3. Em caso de discordância por parte da Contraente Pública quanto aos valores indicados nas faturas, deve esta comunicar, por escrito, ao Cocontratante, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.
4. A falta de pagamento dos valores contestados pela Contraente Pública não vence juros de mora nem justifica a suspensão das obrigações contratuais do Cocontratante, devendo, no entanto, a Contraente Pública proceder ao pagamento da importância não contestada.
5. Desde que devidamente emitidas e observado o disposto no n.ºs 1 e 2, as faturas são pagas através de transferência bancária para a instituição de crédito indicada pelo Cocontratante.
6. No caso de suspensão da execução do contrato e independentemente da causa da suspensão, os pagamentos ao Cocontratante serão automaticamente suspensos por igual período.

SECÇÃO III

ACOMPANHAMENTO E FISCALIZAÇÃO DA EXECUÇÃO DO CONTRATO

Cláusula 19.^a

Acompanhamento e fiscalização do modo de execução do contrato

1. A execução do contrato é permanentemente acompanhada pelo gestor do contrato designado pela Contraente Pública, a identificar no contrato.

2. No exercício das suas funções, o gestor pode acompanhar, examinar e verificar, presencialmente, a execução do contrato pelo Cocontratante.
3. Caso o gestor do contrato detete quaisquer desvios, defeitos ou outras anomalias na execução do contrato, encontra-se habilitado a determinar ao Cocontratante que adote as medidas que, em cada caso, se revelem adequadas à correção dos mesmos.
4. 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 20.^a

Modificação objetiva do contrato

Além dos fundamentos de modificação objetiva previstos no artigo 312.º do Código dos Contratos Públicos, o contrato pode ainda ser modificado nas seguintes condições:

- a) Alteração dos locais previstos no Anexo II em caso de mudança de instalações por parte da Contraente Pública, dentro do âmbito territorial de atividade da Contraente Pública;
- b) Prazo de entrega dos materiais, caso se verifique constrangimentos no aprovisionamento em virtude da escassez de matérias-primas, por circunstâncias imprevisíveis que venham a ocorrer após a assinatura do contrato.

Cláusula 21.^a

Subcontratação e cessão da posição contratual do adjudicatário

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 Contraente pública.
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 Contraente Pública 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. Em caso de incumprimento, pelo Cocontratante, das suas obrigações, que reúna os pressupostos para a resolução do contrato, a Contraente Pública pode determinar que o Cocontratante ceda a sua posição contratual ao concorrente do procedimento pré-contratual na sequência do qual foi celebrado o contrato em execução, que venha a ser indicado pela Contraente Pública, pela ordem sequencial daquele procedimento.
5. A subcontratação pelo Cocontratante depende de autorização da Contraente Pública, nos termos do Código dos Contratos Públicos.

Cláusula 22.^a

Sanções contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a Contraente Pública pode exigir do Cocontratante o pagamento de sanções contratuais, de montante a fixar em função da gravidade do incumprimento.
2. A Contraente Pública pode, designadamente, exigir do Cocontratante o pagamento de sanções contratuais nos seguintes termos:
 - a) Pelo incumprimento das datas e prazos de entrega dos bens definidos no Anexo I, no valor de 1% do valor do equipamento a instalar;
 - b) Pelo incumprimento da obrigação de garantia técnica, até 5% do valor da solução;
 - c) Pelo incumprimento da obrigação de continuidade de fabrico e de fornecimento dos bens, até 10% do valor do equipamento.
3. O valor acumulado das sanções contratuais a aplicar não pode exceder o limite máximo de 20% do preço contratual.
4. Nos casos em que seja atingido o limite de 20% e a Contraente Pública decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.
5. A Contraente Pública pode descontar o valor das sanções contratuais devidas nos termos da presente cláusula nos pagamentos devidos ao Cocontratante.
6. As sanções contratuais previstas na presente cláusula não obstam a que a Contraente Pública exija uma indemnização pelo dano excedente.

Cláusula 23.^a

Força maior

1. Não podem ser impostas sanções contratuais 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; e
 - d) Não lhe seja razoavelmente exigível contornar ou evitar os efeitos produzidos por aquelas circunstâncias.
3. Não constituem força maior, designadamente, quando aplicáveis:
 - 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 Contraente Pública a resolver o contrato ao abrigo do n.º I do artigo 335.º do Código dos Contratos Públicos, não tendo o adjudicatário direito a qualquer indemnização

Cláusula 24.^a

Resolução do contrato por parte da Contraente Pública

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a Contraente Pública 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. A Contraente Pública pode resolver o contrato designadamente nos seguintes casos:
 - a) Atraso, total ou parcial, na entrega e/ou instalação dos bens por um prazo superior a 60 (sessenta) dias ou declaração escrita do Cocontratante de que o atraso em determinada entrega excederá esse prazo;
 - b) Deterioração do sistema existentes em virtude de algum defeito causado por quaisquer bens fornecidos ou de deficiente instalação dos mesmos;
3. 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 Contraente Pública.
4. Em caso de resolução do contrato por incumprimento do Cocontratante pode ser-lhe exigida uma pena pecuniária de até 20% (vinte por cento) do preço contratual.
5. Ao valor da pena referida no número anterior são deduzidas as importâncias pagas pelo Cocontratante ao abrigo da cláusula 18.^a relativamente às prestações objeto do contrato cujo incumprimento tenha determinado a respetiva resolução sancionatória.
6. O disposto no n.º 4 não prejudica o direito de indemnização nos termos gerais, não obstante a que a Contraente Pública exija uma indemnização pelos danos excedentes.

Cláusula 25.^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 I 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, com exceção daquelas a que se refere o artigo 444.º do Código dos Contratos Públicos.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Cláusula 26.^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 27.^a

Comunicações

1. Salvo quando o contrário resulte do contrato, quaisquer comunicações entre a Contraente Pública e o Cocontratante relativas ao contrato devem ser efetuadas através de carta registada com aviso de receção ou por correio eletrónico, para os contatos identificados no contrato.
2. Qualquer comunicação feita por carta registada é considerada recebida na data indicada

pelos serviços postais.

3. Qualquer comunicação realizada por correio eletrónico é considerada recebida na data constante do respetivo recibo de receção e leitura remetido pelo recetor ao emissor.

Cláusula 28.^a

Foro competente

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

Cláusula 29.^a

Direito aplicável e natureza do contrato

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

Cláusula 30.^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.

Anexos:

ANEXO I – Características Técnicas

ANEXO II – Locais de entrega e instalação

ANEXO III – Mapa de Quantidade de Equipamentos e SLA - Nível Contratual

ANEXO I – Características Técnicas

I. Requisitos Genéricos

A Águas do Alto Minho, S.A. pretendem renovar o suporte da solução de segurança que detém atualmente, composta por um Cluster de firewall Checkpoint 5400, antivírus destinados a todos os equipamentos da organização, sendo a gestão destas componentes efetuada centralmente numa única consola de administração deste fabricante.

É objetivo da Águas do Alto Minho, S.A. adquirir um novo cluster de firewall destinada ao edifício da sede, assim como a substituição dos equipamentos atualmente existentes em todas as lojas e centros operacionais.

Fruto dos desenvolvimentos efetuados sobre a solução de segurança existente e respetiva integração com sistemas de terceiros e tendo em conta a otimização financeira deste projeto é nosso objetivo renovar o suporte para a solução de segurança que detemos atualmente, composta por um Cluster de firewall Checkpoint 5400 e 200 antivírus instalados nos computadores da organização, sendo a gestão destas duas componentes obrigatoriamente efetuada centralmente numa consola de administração unificada deste fabricante.

É objetivo da Águas do Alto Minho, S.A. adquirir uma nova solução de firewall que funcione de forma integrada na consola de administração existente, numa arquitetura de alta disponibilidade que irá ocupar o lugar do atual cluster Checkpoint 5400, sendo esta migrada posteriormente para o centro de dados secundário, responsável pela infraestrutura de recuperação de desastre.

O Cluster de firewall a adquirir irá ocupar o lugar da atual Checkpoint 5400, sendo esta migrada posteriormente para o centro de dados secundário, responsável pela infraestrutura de recuperação de desastre.

No que diz respeito à solução destinada à substituição do cluster 5400 o mesmo deve respeitar os seguintes critérios:

- a) Todos os equipamentos deverão ser fornecidos através de canais autorizados, em estado novo, e nas suas embalagens originais;
- b) O fabricante deverá ter tem conhecimento deste projeto e que o integrador em causa tem autonomia e capacidade para a sua implementação, ainda que poderá contar com o seu total apoio;
- c) O fabricante deverá comprovar a sua liderança em soluções de segurança (UTM, Firewall e prevenção de intrusões), ano após ano, em análises/relatórios de entidades independentes;
- d) O fabricante deverá endereçar todos os requisitos de um equipamento de segurança

(Firewall), tais como processamento de largura de banda, número de ligações, capacidade de securitização de aplicações de nova geração em todas as vertentes da rede (escritório, centro de dados) num único equipamento;

- e) O fabricante deverá disponibilizar as mesmas funcionalidades de inspeção avançada (Firewall, intrusion prevention, application control, URL filtering, Anti-Bot, Anti-Virus, Sandboxing) em modelo físico e virtual, quaisquer destas geridas por uma única consola central e dedicada.

A solução proposta deverá endereçar todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante:

- Statefull Inspection Firewall - A gateway deverá inspecionar end-to-end (não apenas “half-way” ou “header”) todos os fluxos de comunicação desde o estabelecimento da sessão (3-way handshake TCP), durante a transferência de informação (payload), até que esta seja terminada;
- Intrusion Prevention System;
- User Identity Acquisition;
- Application Control and URL filtering;
- Anti – Bot / Anti – Virus;
- Anti – Spam and Email Security;
- IPSec VPN;
- Remote Access VPN (Mobile Access);
- Logging and Status;
- Event Correlation and Reporting.

A solução proposta não poderá em momento algum “sacrificar” a segurança em detrimento da performance (desabilitar inspeção end-to-end em cenários de “carga” na plataforma).

A solução proposta deverá conter uma plataforma de gestão dedicada com:

- Centralização de políticas, logs, reports;
- Sem limite de storage com base em requisitos de licenciamento;
- O servidor de gestão deverá ter a capacidade de obter detalhes de configuração diretamente das gateways de firewall de forma automática.

2 - Sistema de prevenção de intrusões (IPS)

- O IPS e/ou o Application Control deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (Anonymizers);
- O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou hosts;
- A solução deve proteger DNS Cache Poisoning e impedir o acesso dos utilizadores a endereços de domínio bloqueados;
- Solução deve fornecer proteções para protocolos VOIP;
- O IPS e/ou o Application Control devem detetar e bloquear aplicações que permitam controlo remotos, incluindo as que são capazes de realizar tunneling sobre o tráfego HTTP;
- IPS deve ter proteções SCADA;
- A solução deve permitir ao administrador bloquear de forma fácil o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os intervalos de IP correspondentes ao país.

3 - Aquisição de identidade de utilizadores (User ID Acquisition)

- Deve ser capaz de adquirir a identidade dos utilizadores, com base na consulta dos eventos de segurança da Microsoft Active Directory;
- Deve ser possível a autenticação através de uma browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio;
- Deve ter um agente que possa ser instalado nos endpoints, para reportar à firewall as identidades dos utilizadores;
- Deve ser capaz de partilhar identidades de utilizadores entre vários gateways de segurança;
- Deve ser capaz de criar identity roles (grupos de identidades) para serem invocados em diferentes aplicações da solução.

4 - Filtragem de URL e Controlo de Aplicações

- A solução deve reconhecer e controlar pelo menos 6.000 aplicações populares no mercado;
- A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL;
- A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias;
- A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores;
- A solução deve categorizar aplicações e URL's por fator de risco;

- A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda;
- A solução deve permitir exceções com base em objetos de rede previamente definidos;
- A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria.

5 - Security Management, Logging, Correlação de eventos e Reporting

- A solução deverá possibilitar a segmentação da política de segurança numa estrutura de subpolíticas e de layers;
- A solução deverá possibilitar a integração de logs e audit logs numa única consola, para contextualizar o administrador ao efetuar alterações sobre a política de segurança;
- A solução deverá disponibilizar métricas de “hit count” nas regras presentes na política de segurança;
- A solução deverá possibilitar a utilização de etiquetas (labels) ou secções (tabs) para melhor organização da política de segurança;
- A solução deverá disponibilizar um mecanismo de validação da política de segurança, antes da sua instalação nas gateways de firewall;
- A solução deverá disponibilizar um mecanismo de backup e revisão da política de segurança, possibilitando comparar versões da política e reverter para versões anteriores, se necessário;
- A solução de logging deverá estar integrada na componente de gestão centralizada, e possibilitar a visualização de logs afetos a políticas específicas, sem ser necessário recorrer a uma nova janela, ou aplicação;
- A solução deverá ter a capacidade de correlacionar eventos de todas as funcionalidades ativas nas demais gateways (FW, IPS, URL-F, etc.);
- A solução deverá possibilitar a criação de filtros de logging, com base em qualquer característica, tal como: aplicação, IP de origem e destino, serviço, tipo de evento, severidade do ataque, país de origem e destino, etc.;
- A solução deverá detetar ataques de “credential guessing / brute force”;
- A solução deverá incluir relatórios horários, diários, semanais e mensais predefinidos, incluindo pelo menos: Top Events, Top Sources, Top Destinations, Top Services, etc.;
- A solução de reporting deverá disponibilizar informação consolidada sobre:
 - Volume de ligações bloqueadas por uma regra de segurança em particular;
 - Top de origens bloqueadas, e os destinos e serviços respetivos;
 - Top de regras mais utilizadas na política de segurança;
 - Top de ataques detetados no perímetro, com informação das origens e destinos associados;
 - Atividade web por user, com top de web users e websites mais utilizados.

6 - Hardware

6.1 - Requisitos de Performance Cluster Firewall para a Sede em cenário real:

Parâmetro	Métrica
Threat Prevention/Extraction	>= 3.7 Gbps
NextGen Firewall	>= 6.2 Gbps
Intrusion Prevention System	>= 10.14 Gbps
VPN Throughput	>= 4.9 Gbps
Firewall Throughput	>= 18 Gbps
Connections per second	116,000
Concurrent Connections	2/4/8M

6.2. - Requisitos físicos para a Sede

- Possibilidade de ter Wi-Fi:
 - 802.11 b/g/n/ac MIMO 3x3;
 - 6xPoE 1GE UTP.
- Características das interfaces:
 - 6x1GE UTP.
- Fonte de alimentação 12V/3.3A 40W.

6.3. - Requisitos de Performance para as Lojas

Parâmetro	Métrica
Threat Prevention with Smart Accel	>= 440 Mbps
NextGen Firewall	>= 600 Mbps
Intrusion Prevention System	>= 670 Mbps
VPN Throughput	>= 970 Mbps
Firewall Throughput	>= 1000 Mbps
Connections per second	10.500
Concurrent Connections	500.000

6.4. - Requisitos físicos para firewall das lojas

- Possibilidade de ter Wi-Fi:
 - 802.11 b/g/n/ac MIMO 3x3;
 - 6xPoE 1GE UTP.
- Características das interfaces:
 - 6x1GE UTP.
- Fonte de alimentação 12V/3.3A 40W.

7 - Proteção de Endpoints

Para proteção dos endpoints será necessário considerar o licenciamento de uma solução de Endpoint, com licenciamento para 200 dispositivos, com gestão centralizada, com os seguintes requisitos mínimos:

- Deve emular ameaças simulando a execução de ficheiros desconhecidos num ambiente isolado para detetar comportamentos maliciosos e prevenir violações, bem como extrair ameaças como conteúdos ativos dos documentos acedidos pelos utilizadores, entregando ficheiros limpos sem qualquer perigo.

- Deve incorporar uma proteção Anti-Ransomware que interrompa o malware desde o primeiro momento e repare automaticamente o dano (restaurando cópias criptografadas pelo ransomware).
- Deve utilizar uma tecnologia que funcione sem assinaturas e não seja baseada em atualizações constantes, funcionando tanto online quanto offline, colocando infeções em quarentena automaticamente com base na sua análise forense, bem como restaurando automaticamente ficheiros criptografados por ransomware ao seu estado antes do ataque.
- Deve ser capaz de prevenir erros humanos e detetar phishing de Zero-Day, bloqueando proactivamente o acesso a sites novos e desconhecidos, bem como salvaguardar as credenciais dos utilizadores e impedir o uso de senhas corporativas em sites externos.
- Deve fornecer relatórios forenses de ameaças, coletando continuamente todos os eventos relevantes do sistema, e fornecer pesquisa proativa de incidentes e análises para entender rapidamente o ciclo de vida completo do ataque, fornecer maior visibilidade do ataque e vetores de danos do ataque para maximizar a produtividade da equipa de resposta e minimizar a exposição organizacional.
- Os relatórios forenses devem oferecer uma visão do ataque representando os dados de acordo com um padrão de segurança de acordo com a Matriz MITER ATT & CK.
- A solução deve fornecer visibilidade total com recursos forenses, monitorizando e registando todos os eventos que ocorrem nos terminais: ficheiros afetados, processos iniciados, alterações no registo do sistema e atividade de rede. Esta monitorização deve garantir que os dados estejam disponíveis, mesmo se o ataque for bem-sucedido, mesmo se ele remover ficheiros ou outros indicadores de comprometimento que foram deixados no sistema.
- A solução deve incorporar mecanismos de análise comportamental que usem análise forense para identificar de forma eficaz e exclusiva comportamentos de malware desconhecidos e classificar com precisão o malware na categoria apropriada.
- Deve ter mecanismos de segurança de navegação incorporados aos principais navegadores da web que sejam capazes de extrair ameaças e reconstruir ficheiros acedidos pelos usuários em poucos segundos, eliminando possíveis ameaças e entregando rapidamente uma versão segura ao utilizador. Além disso, deve incorporar mecanismos de emulação de ameaças que detetam comportamento malicioso e evitam infeções por malware de dia zero e ataques direcionados, inspecionando ficheiros em um ambiente de sandbox virtual. A filtragem de navegação é necessária usando a Filtragem de URL para garantir uma navegação segura.
- A solução deve proteger os utilizadores de ameaças que chegam por meio de downloads da Internet usando técnicas como phishing, conteúdo malicioso copiado para dispositivos de armazenamento removíveis, infeções causadas por movimento lateral de dados e malware entre sistemas em segmentos específicos da rede, bem como infeções por meio de conteúdo criptografado.
- A solução deve incluir proteção Anti-Bot, continuamente atualizada com os dados de inteligência de ameaças mais recentes, identificando e bloqueando as comunicações de botnet com servidores de comando e controlo (C&C), contendo e colocando em quarentena os dispositivos infetados.
- O instalador da solução deve ser capaz de desinstalar agentes antivírus de terceiros e a solução deve ser capaz de ser implementada de forma fácil com administração local ou na Cloud.

- A solução deve ter uma consola central para definir políticas, criar grupos de sistema/utilizadores, registar, implementar atualizações, gerar relatórios com acesso baseado em funções e oferecer suporte ao uso de autenticação de sistemas de terceiros.
- A solução forçará as estações de trabalho a cumprir as regras de segurança definidas pela organização. Aqueles que não cumprirem serão mostrados como não conformes e políticas restritivas devem ser aplicadas.
- Deve ter um cliente de VPN integrado no próprio Endpoint, e permitir a ligação nativamente com a firewall.
- A solução deve incluir módulos de análise forense, criando automaticamente uma análise de incidentes para cada deteção/prevenção que ocorrer.
- A solução deve incluir módulos Threat Hunting que permitem a pesquisa de vários tipos de dados de sensor não detetados, incluindo ficheiros, processos, rede, registo, injeção e dados do utilizador.
- A solução deve permitir a correção de qualquer ficheiro ou processo encontrado através do Threat Hunting.
- A solução deve permitir análises forenses e relatórios de qualquer indicador encontrado por meio do Threat Hunting. A solução enriquecerá automaticamente os seus resultados de pesquisa confiáveis.
- Logs e relatórios:
 - A solução deve gerar relatórios periódicos sobre tipos de malware, tipos de vulnerabilidades exploradas, etc.;
 - A solução deve ter a capacidade de gerar relatórios visuais;
 - A solução deve mostrar o processo afetado, as chaves de registo afetadas e os ficheiros afetados no ambiente do sistema operativo;
 - A solução deve mostrar capturas de ecrã e vídeo da emulação de ficheiros maliciosos no ambiente de Sandbox;
 - A solução deve ser capaz de registar a comunicação C&C do ficheiro BOT emulado.

8 - Renovação de Suporte para Solução de Cluster CheckPoint 5400 Existente

A Águas do Alto Minho, S.A. atualmente detém uma solução de segurança informática do fabricante Checkpoint para a qual pretende renovar o respetivo suporte de software e hardware até 31 dezembro de 2025.

Neste sentido passamos a listar todos os produtos e serviços para os quais a Águas do Alto Minho, S.A. pretende renovar os respetivos suportes:

Produto	Tipo de Suporte
CPAP-SG5400-NGTX-SSD	CPCES-CO-STANDARD-ADD
CPAP-SG5400-NGTX-SSD-HA	CPCES-CO-STANDARD-ADD
CPSM-NGSM25	

SKU	Descrição	Qtd.
CPCES-CO-STANDARD	Collaborative Enterprise Support Standard SW	1
CPCES-CO-STANDARD-ADD	Collaborative Enterprise Support Standard HW	1
CPSB-NGTX-5400-3Y	Next Generation Threat Prevention & SandBlast (NGTX) for 5400 Appliance	1
CPSB-NGTX-5400-3Y-HA	Next Generation Threat Prevention & SandBlast (NGTX) for 5400 Appliance HA	1
CPSB-EVS-COMP-25-3Y	SmartEvent, SmartReporter and Compliance blades for 25 gateways (Smart-1 & open server) 3 year subscription	1
CPSB-MOB-200	Mobile Access Blade for 200 concurrent connections	2
CPCES-CO-STANDARD	Collaborative Enterprise Support Standard	1
CP-HAR-EP-ADVANCED-3Y	Advanced threat protection for Endpoint devices, includes Web Protection, forensics Access protection, Sandbox emulation and extraction, for 3 years	50
CP-HAR-EP-BASIC-3Y	Basic threat protection for Endpoint devices, includes Web Protection, forensics Access and Data protection, for 3 years	150
CPCES-CO-Premium	Collaborative Enterprise Support - Premium	1

9 - Serviços de Instalação

No que compete aos requisitos de segurança e tendo em conta a necessidade de segmentação das redes em zonas operacionais é relevante que a rede existente e em pleno funcionamento seja devidamente reestruturada e adaptada as novas necessidades e instalação de novos equipamentos.

No patamar da segurança é pretendido que a segmentação e controlo do tráfego de rede seja assegurada pelo novo cluster firewall a instalar no edifício da sede e que o cluster Checkpoint 5400 atualmente existente seja instalado no centro de dados de recuperação de desastre.

É também necessário instalar e configurar todas as firewalls das lojas e centros operacionais com o intuito de estabelecer tuneis VPN entre os edifícios remotos e a sede da Águas do Alto Minho, S.A..

No que diz respeito à implementação de todos os sistemas previstos no presente caderno de encargos o integrador deve garantir que:

- Reúne condições técnicas e operacionais que lhe permitam operar as soluções Checkpoint atualmente existente e que tem o respetivo suporte por parte do fabricante;
- Efetuar a reconfiguração da rede referente ao centro de dados migrando todas as configurações do cluster atualmente existente e em produção para o novo;
- Implementar toda as regras de segmentação necessárias no sentido de garantir a sua adequação ao modelo atual de funcionamento;
- Prestar o devido apoio aos diferentes integradores que estejam envolvidos no processo de implementação das soluções atualmente existentes;
- Articular junto dos operadores de telecomunicações a integração das redes oT e implementar as alterações necessárias assim como os devidos mecanismos de segurança;
- Implementar todas as configurações de rede necessárias à implementação do centro de dados de recuperação de desastre e em articulação com todas as entidades envolvidas neste processo (Operadores, integradores de sistemas e entidade gestoras das infraestruturas e instalações DR);
- No decorrer dos processos de implementação o integrador deverá garantir suporte 24/7 assim como a reconfiguração de todos os equipamentos de rede e segurança em horário pós-laboral;
- Proceder à Instalação física dos equipamentos segundo especificações técnica facultadas no momento de instalação pelos nossos serviços técnicos;
- Configurar a monitorização nativa para todos os elementos de hardware e software que suportam a solução;
- Definição, em conjunto com a ADAM, e execução de testes funcionais de resiliência a toda solução implementada;
- Redação de documentação de instalação, configuração e manutenção dos ambientes;
- Formação da equipa no conjunto de tecnologias implementadas (incluindo, definição de políticas, reporting, upgrade, etc.);
- Complementarmente aos serviços de suporte garantidos pelo fabricante, o revendedor deverá assegurar os serviços de manutenção e atualização de todas as soluções instaladas no âmbito deste projeto durante 36 (trinta e seis) meses sem limite de intervenções/horas de suporte em horário pós-laboral;
- É também da sua responsabilidade a manutenção física dos equipamentos e instalação das respetivas atualizações de software em horário pós-laboral, articulando as suas intervenções com as equipas técnicas internas.

Sem compromisso para a implementação deste projeto na sua totalidade o integrador deverá considerar o mínimo 320 (trezentas e vinte) horas de serviços presenciais em horário pós-laboral. Cada intervenção poderá ocorrer presencialmente numa das nossas instalações dispersas por todo o Alto Minho com duração nunca superior a 3 (três) horas.

ANEXO II – Locais de entrega e instalação

LOCAL	Cluster Data center	Cluster Data center DR Renovação	Firewall Lojas e cop	Solução de Gestão	Serviços
CNP Município Paredes de Coura Núcleo de Proximidade			x		
CNP Município Ponte de Lima Núcleo de Proximidade			x		
COP Município Arcos de Valdevez Centro Operacional			x		
COP Município Vila Nova de Cerveira Centro Operacional			x		
Datacenter DR Município Barcelos		x		x	
Datacenter Município Viana do Castelo	x			x	x
Loja Município Arcos de Valdevez			x		
Loja Município Caminha			x		
Loja Município Caminha Vila Praia de Âncora			x		
Loja Município Paredes de Coura			x		
Loja Município Ponte de Lima			x		
Loja Município Valença			x		
Loja Município Vila Nova de Cerveira			x		

