Joana do Ó

Assinado de forma digital por Joana do Ó
Dados: 2021.10.13 15:25:38 +01'00'

AD&C
Agência para o Desenvolvimento e Coesão, I.P.

PROCEDIMENTO DE CONCURSO PÚBLICO COM PUBLICIDADE INTERNACIONAL PARA AQUISIÇÃO DE HARDWARE, LICENCIAMENTO DE SOFTWARE, ASSISTÊNCIA TÉCNICA, SOLUÇÕES DE LAN, WAN, WIFI, SEC E END POINTS DE VÍDEOCONFERÊNCIA

CADERNO DE ENCARGOS

EFQM Committed to Excellence 2019

EFFECTIVE CAF USER

Cohesion and Development Agency
Avenida 5 de outubro, n.º 153
1050-053 Lisboa PORTUGAL
Telf: 218 814 000 Fax: 218 881 111
agencia@adcoesao.pt
www.adcoesao.pt

PARTE I

CLÁUSULAS JURÍDICAS

SECÇÃO I

Definições

Cláusula 1ª

Definições

1. Para efeitos do presente Caderno de Encargos e respetivos anexos, os termos referidos nas alíneas seguintes têm o sentido que aí lhes é atribuído, quando utilizados no texto com a formatação de "Maiúsculas Pequenas":

CADERNO DE ENCARGOS	O presente documento;
CONTRAENTE PÚBLICO	A Agência para o Desenvolvimento e Coesão, I.P. (Agência), instituto público com o qual será celebrado o CONTRATO para fornecimento dos equipamentos e a prestação dos serviços no âmbito do presente procedimento;
COCONTRATANTE	Contraparte da Agência no Contrato. O adjudicatário com o qual será celebrado o Contrato.
CONTRATO	O acordo escrito celebrado entre a CONTRAENTE PÚBLICO e o COCONTRATANTE na sequência do procedimento pré-contratual;
PROPOSTA	A proposta adjudicada

2. Para efeitos do Caderno de Encargos, os acrónimos referidos nas alíneas seguintes têm o sentido que aí lhes é atribuído na seguinte tabela:

CCP	Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de Janeiro, com a redação em vigor introduzida pela Lei nº 30/2021, de 21 de maio
CE	Caderno de Encargos

EMRP	Estrutura de Missão Recuperar Portugal

SECÇÃO II

Cláusula 2.ª

Objeto

1. O presente CE compreende as cláusulas que integram o CONTRATO a celebrar na sequência do procedimento pré-contratual que tem por objeto principal a aquisição de hardware, licenciamento de software, serviços de assistência Técnica, soluções de LAN, WAN, WIFI, SEC e End Points de videoconferência para a Estrutura de Missão Recuperar Portugal (EMRP), de acordo com as especificações técnicas constantes da Parte II.

2. Os lotes a concurso têm o seguinte objeto, nos termos melhor definidos na Parte II do presente CE, que dele faz parte integrante:

   Lote 1 – Hardware, licenciamento e suporte;
   Lote2 – Serviços Cloud e Apoio;
   Lote 3 – Licenciamento Microsoft;
   Lote 4 – Outros Software;
   Lote 5 – Infraestrutura de LAN, Wifi, Segurança, Endpoints de Vídeo e Serviços Associados.

Cláusula 3.ª

Prevalência

1. O CONTRATO é composto pelo respetivo clausulado contratual.
2. O CONTRATO a celebrar integra ainda os seguintes elementos:
   a) Os suprimentos dos erros e das omissões do CE identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
   b) Os esclarecimentos e as retificações relativos ao CE;
   c) O presente CE;

d) A PROPOSTA adjudicada;

e) Os esclarecimentos sobre a PROPOSTA adjudicada prestados pelo COCONTRATANTE.

3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do CONTRATO e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do CCP e aceites pelo COCONTRATANTE nos termos do disposto no artigo 101.º do mesmo diploma legal.

Cláusula 4.ª

Prazo de vigência do CONTRATO

1. O(s) CONTRATO(s) entra(m) em vigor no dia seguinte ao da sua assinatura e vigora(m), em qualquer dos lotes, pelo prazo de 36 (trinta e seis) meses, sem prejuízo das obrigações acessórias, designadamente de garantia dos bens e serviços, que devam perdurar para além da cessação do mesmo.

Cláusula 5.ª

Local da execução do CONTRATO

1. O fornecimento dos equipamentos terá lugar nas instalações da Estrutura de Missão "Recuperar Portugal", sitas no concelho de Lisboa.
2. Os bens e serviços a fornecer pelo COCONTRATANTE serão entregues e instalados por este diretamente na EMRP, nos termos da PROPOSTA adjudicada e, em qualquer caso, sempre de acordo com as indicações que, para o efeito, lhe sejam dadas pelo contraente público, de acordo com o estabelecido nas Especificações Técnicas do CE.
3. Sempre que seja necessária a presença de colaboradores do CONTRAENTE PÚBLICO para a execução do CONTRATO, a mesma deverá ocorrer em dias úteis, e, em regra, entre as 9h00 e as 17h00.

OBRIGAÇÕES DAS PARTES

SECÇÃO III

OBRIGAÇÕES DO COCONTRATANTE

Cláusula 6ª

Principais obrigações do COCONTRATANTE

1. Nos termos do CONTRATO a celebrar, o COCONTRATANTE obriga-se, durante o período da sua execução, à realização de todas as operações necessárias ao integral, adequado e pontual cumprimento do objeto do CONTRATO, considerando as finalidades a que o mesmo se destina.
2. Sem prejuízo de outras obrigações previstas na legislação aplicável ou nas cláusulas contratuais, da celebração do CONTRATO decorrem para o COCONTRATANTE as seguintes obrigações principais:
   a) Fornecer e instalar os equipamentos identificados nas Especificações técnicas do CE, dentro dos prazos dele constantes, bem como da PROPOSTA adjudicada, e nos locais indicados pelo CONTRAENTE PÚBLICO;
   b) Prestar os serviços conforme os requisitos e características técnicas definidas no CE e demais documentos contratuais;
   c) Garantir ao CONTRAENTE PÚBLICO o acesso, a todo o momento, de forma presencial ou remota, aos ambientes de instalação ou desenvolvimento dos serviços objeto do CONTRATO, para efeitos de monitorização e fiscalização do mesmo;
   d) Comunicar, de imediato, após o respetivo conhecimento, os factos que tornem total ou parcialmente impossível o cumprimento atempado de qualquer das suas obrigações;
   e) Desenvolver todas as diligências e praticar todos os atos junto do CONTRAENTE PÚBLICO, de forma a garantir a correta e adequada implementação dos serviços contratados;
   f) Prestar de forma completa e integrada as informações em cada momento relativas às condições dos serviços objeto do presente CE e prestar todos os esclarecimentos que sejam relevantes ou requeridos pelo CONTRAENTE PÚBLICO;
   g) Proceder à cobertura, através de contratos de seguro, de quaisquer riscos de acidentes pessoais relativos aos seus colaboradores, independentemente do vínculo jurídico que com eles tenha, nos termos da lei em vigor, bem como assegurar a cobertura dos riscos associados ao transporte e à instalação dos equipamentos objeto do CONTRATO.

Cláusula 7ª

Poder de conformação da prestação pelo Contraente Público

Sem prejuízo da autonomia do COCONTRATANTE, dentro dos limites do CE e da PROPOSTA adjudicada, o COCONTRATANTE aceita expressamente os poderes do CONTRAENTE PÚBLICO, nos termos dos artigos 302.º e seguintes do CCP e demais legislação em vigor, de definição e conformação dos serviços a prestar, com vista a atingir os objetivos globais do projeto a implementar.

Cláusula 8ª

Relatório Final

1. Sem prejuízo do disposto na Parte II relativamente aos serviços objeto do CONTRATO, e para além de outros documentos e materiais previstos noutras disposições do CE, o COCONTRATANTE deverá entregar ao CONTRAENTE PÚBLICO um Relatório final de execução, bem como os manuais técnicos dos serviços implementados.
2. Todos os documentos deverão ser redigidos em língua portuguesa e/ou inglesa, e serão entregues em suporte digital, no formato PDF, com texto selecionável e pesquisável.
3. As datas de entrega dos documentos previstos no número 1 serão acordadas entre as partes, não podendo em caso algum o CONTRAENTE PÚBLICO proceder ao pagamento dos últimos 5% (cinco por cento) do valor do CONTRATO, sem que todos eles sejam recebidos e validados pelo CONTRAENTE PÚBLICO.
4. O Contraente Público, quer antes da receção desses documentos, quer depois da sua receção, mas antes da sua validação formal, poderá discutir com o COCONTRATANTE o respetivo conteúdo, acordando nos conteúdos, alterações ou aditamentos que forem convenientes.

Cláusula 9ª

Sigilo e confidencialidade

1. O COCONTRATANTE garante o sigilo relativamente a todas as informações ou documentos relativos ao objeto do presente procedimento ou relacionados com a atividade do CONTRAENTE PÚBLICO, que sejam fornecidos ao COCONTRATANTE ou a quaisquer dos seus técnicos, independentemente da natureza da relação contratual, não podendo ser divulgados e/ou usados para fins diferentes daqueles a que se destinam ou cedidos a terceiros, ainda que para fins meramente estatísticos ou de estudo.

2. Sem prejuízo do disposto no número seguinte, o COCONTRATANTE compromete-se a não divulgar, durante e após a execução do CONTRATO, quaisquer informações que obtenha no seu âmbito, competindo-lhe assegurar o cumprimento desse dever relativamente a todos os colaboradores, independentemente da natureza do vínculo contratual que com eles tenha.
3. O COCONTRATANTE só pode divulgar informações referidas no número anterior na medida em que tal seja estritamente necessário à execução do CONTRATO, mediante autorização do CONTRAENTE PÚBLICO, ou do estritamente necessário ao exercício do direito de defesa em processo judicial.
4. O COCONTRATANTE deve ainda limitar o acesso às informações confidenciais aos seus técnicos que a elas tenham de recorrer para a correta execução do CONTRATO, assegurando que os mesmos são obrigados a manter essa confidencialidade.
5. São suscetíveis de serem consideradas informações confidenciais, sem prejuízo de outras que venham contratualmente a ser qualificadas como tal, as que, a serem divulgadas, possam causar danos, de qualquer natureza, a qualquer das partes ou a terceiros, ou perturbar o normal desenvolvimento da prestação de serviços objeto deste CE.
6. O COCONTRATANTE e os seus colaboradores obrigam-se a respeitar a total confidencialidade, neutralidade e descrição relativamente aos trabalhadores do CONTRAENTE PÚBLICO com quem contactem.
7. Nenhum documento ou dado a que o COCONTRATANTE tenha acesso, direto ou indiretamente, no âmbito do CONTRATO poderá ser reproduzido sem autorização expressa do CONTRAENTE PÚBLICO.
8. O dever de sigilo mantem-se em vigor indefinidamente, até autorização expressa em contrário pelo CONTRAENTE PÚBLICO, a contar do cumprimento ou cessação, por qualquer causa, do CONTRATO, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, a proteção de segredos comerciais ou da credibilidade, do prestigio ou da confiança devidos às pessoas coletivas.
9. Os deveres referidos nos números anteriores abrangem igualmente as entidades subcontratadas pelo COCONTRATANTE, devendo, em qualquer caso, o COCONTRATANTE credenciar os colaboradores da equipa sempre que em causa esteja ou possa estar o tratamento de dados pessoais.

Cláusula 10ª

Conformidade e operacionalidade

1 O COCONTRATANTE obriga-se a disponibilizar ao CONTRAENTE PÚBLICO os bens e serviços com as características, especificações e requisitos técnicos previstos na parte II do presente CE, que dele faz parte integrante.

2 É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de software e das garantias a este relativo no que respeita à conformidade das licenças a disponibilizar.

3 O COCONTRATANTE é responsável perante o CONTRAENTE PÚBLICO por qualquer defeito ou discrepância das licenças objeto do CONTRATO que existam no momento em que lhe forem disponibilizadas.

4 Sempre que aplicável, o COCONTRATANTE obriga-se a executar o objeto do CONTRATO de acordo com o princípio do *Privacy by Design* e/ou do *Privacy by Default* (se aplicável), fazendo constar esta obrigação e a metodologia e processos definidos no Relatório final de execução.

Cláusula 11ª

Proteção de dados pessoais

1. A atividade desenvolvida pelo COCONTRATANTE e respetivos técnicos, independentemente da natureza da relação contratual, encontra-se sujeita à aplicação do Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, (Regulamento Geral sobre a Proteção de Dados), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
2. Com a celebração do CONTRATO, o COCONTRATANTE assume a qualidade de subcontratante no que diz respeito ao tratamento dos dados pessoais objeto do CONTRATO, em que o CONTRAENTE PÚBLICO assuma a qualidade de entidade responsável pelo tratamento.
3. O tratamento dos dados pessoais autorizado ao abrigo do CONTRATO a celebrar será o estritamente necessário à execução do mesmo, de acordo com as instruções da EMRP e do CONTRAENTE PÚBLICO, nos termos da legislação aplicável à proteção de dados pessoais.
4. O COCONTRATANTE obriga-se, ainda, enquanto subcontratante, ao cumprimento de todos os deveres e obrigações que impendem sobre o CONTRAENTE PÚBLICO, enquanto entidade responsável pelo tratamento de dados pessoais objeto do CONTRATO, comprometendo-se designadamente a:

a) Utilizar os dados pessoais a que tenha acesso ou que lhe tenham sido transmitidos pelo CONTRAENTE PÚBLICO, única e exclusivamente para efeitos da prestação de serviços objeto do CONTRATO;

b) Não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer outra forma colocar à disposição de terceiros os dados pessoais a que tenha acesso, ou que lhe sejam transmitidos pelo CONTRAENTE PÚBLICO, sem que, tenha sido por esta, expressamente instruído por escrito;

c) Comunicar de imediato qualquer situação que possa afetar o tratamento dos dados em causa, ou que de algum modo possa dar origem ao incumprimento das disposições legais em matéria de proteção de dados pessoas;

d) Assegurar que os seus colaboradores, incluindo representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido com o COCONTRATANTE, cumprem todas as obrigações previstas na presente cláusula;

e) Assegurar a confidencialidade dos dados pessoais tratados, sem prejuízo do respeito do cumprimento de obrigações legais, nomeadamente a entidades policiais, judiciais, fiscais e reguladoras;

f) Colaborar com o DPO (*Data Protection Officer* – Encarregado de Proteção de Dados) do CONTRAENTE PÚBLICO, facultando todas as informações e esclarecimentos que este vier a solicitar no âmbito das suas funções;

g) Garantir, sem prejuízo de assegurar a utilização contínua dos dados e aplicações migradas findo o CONTRATO, que qualquer informação, cópia, reprodução ou qualquer outro modo de retenção de informação relativamente aos dados pessoais por si tratados, na qualidade de subcontratante, são integralmente destruídos, mantendo-se também o sigilo mesmo após a cessação do CONTRATO, independentemente do motivo pelo qual ocorra.

5. As partes ficam desde já autorizadas a comunicar o conteúdo do CONTRATO, bem como os elementos com ele relacionados, à Comissão Nacional de Proteção de Dados.

6. Em observância pelo Regulamento Geral sobre a Proteção de Dados, os currículos e/ou outros documentos nos quais constem dados pessoais, deverão ser acompanhados do consentimento expresso dos seus titulares para a finalidade a que se destinam, para que o CONTRAENTE PÚBLICO, no âmbito exclusivo do procedimento de contratação pública em apreço, fique habilitada para o tratamento desses dados.

7. Uma vez atingida a finalidade prevista do número anterior, incluindo monitorização do CONTRATO e auditorias decorrentes do procedimento, os dados pessoais serão eliminados, no respeito pelo Regulamento Geral sobre a Proteção de Dados.
8. Se quaisquer dados se perderem ou forem danificados no âmbito da execução do CONTRATO, por causas imputáveis ao COCONTRATANTE, este compromete-se a adotar as medidas que forem necessárias com vista à recuperação dos dados, sem quaisquer custos adicionais para o CONTRAENTE PÚBLICO.
9. O COCONTRATANTE obriga-se a ressarcir o CONTRAENTE PÚBLICO por todos os prejuízos em que este venha a incorrer em virtude da utilização ilegal e/ou ilícita dos dados referidos, nomeadamente por indemnizações e despesas em que tenha incorrido na sequência de reclamações ou processos propostos pelos titulares dos dados contra o CONTRAENTE PÚBLICO, bem como por taxas, coimas e multas que tenha de pagar.
10. O encarregado da proteção dos dados é a colaboradora Patrícia Guedes com o email protecao.dados@adcoesao.pt, para o qual deverão ser remetidas quaisquer questões, sem prejuízo do direito de as apresentar também à entidade reguladora, a Comissão Nacional de Proteção de Dados.

Cláusula 12 ª

Conflito de interesses e responsabilidade

1. O COCONTRATANTE deve prosseguir a sua atividade de acordo com a lei aplicável e com as regras de boa-fé, tomando todas as medidas necessárias para evitar a ocorrência de quaisquer situações que possam resultar em conflito com os interesses do CONTRAENTE PÚBLICO
2. O COCONTRATANTE obriga-se a não praticar qualquer ato ou omissão do qual possa resultar quaisquer ónus ou responsabilidades para o CONTRAENTE PÚBLICO, ou para os seus direitos e interesses.
3. O COCONTRATANTE obriga-se ainda a suportar quaisquer encargos resultantes, designadamente, de reclamações, custos, despesas, multas, coimas ou sanções, necessários para a libertação de quaisquer ónus ou responsabilidades que recaiam sobre a propriedade do CONTRAENTE PÚBLICO, quando tenham sido criados ou causados por si ou por qualquer dos seus subcontratados.

SECÇÃO IV

OBRIGAÇÕES DA CONTRAENTE PÚBLICO

Cláusula 13.ª

Preço-base e preço contratual

1. O preço base fixado para o presente procedimento, que constitui o encargo máximo a pagar pela execução da prestação de serviços que constitui objeto do CONTRATO a celebrar, é de 350 000,00€ (trezentos e cinquenta mil euros) euros, a que acresce o IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço base estabelecido no número anterior é decomposto do seguinte modo para cada um dos lotes:
   Lote 1 - 130 000,00 € (cento e trinta mil euros),
   Lote 2 - 105 000,00 € (cento e cinco mil euros),
   Lote 3 - 5 000,00 € (cinco mil euros),
   Lote 4 - 10 000,00 € (dez mil euros),
   Lote 5 - 100 000,00 € (cem mil euros),

3. Pelos bens e serviços objeto do CONTRATO, bem como pelo cumprimento das demais obrigações constantes do presente CE, o CONTRAENTE PÚBLICO obriga-se a pagar ao COCONTRATANTE o preço constante da PROPOSTA adjudicada.
4. O preço contratual inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao CONTRAENTE PÚBLICO pelo presente CE, nomeadamente despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 14ª

Revisão de preços

Não há lugar a revisão de preços durante o prazo de vigência do CONTRATO.

Cláusula 15.ª

Condições de pagamento

1. As quantias devidas pelo CONTRAENTE PÚBLICO devem ser pagas no prazo de 30 (trinta) dias após a receção das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação



respetiva.

2. O COCONTRATANTE obriga-se a apresentar mensalmente, ou em cada uma das datas de entrega previstas nas Especificações Técnicas do CE, uma fatura, em função dos serviços prestados até essa data, acompanhada do correspondente Relatório de Serviço.
3. Para os efeitos do número 1, a obrigação considera-se vencida com a comunicação da aceitação dos bens ou serviços contratados pelo CONTRAENTE PÚBLICO.
4. A emissão das faturas pelo COCONTRATANTE deve observar o disposto no artigo 9.º Decreto-Lei nº 111-B/2017, de 31 de agosto, com a redação conferida pelo Decreto-Lei nº 14-A/2020, de 7 de abril.
5. As faturas têm de conter obrigatoriamente a indicação do número de compromisso, para efeitos de cumprimento da Lei sobre os Compromissos e Pagamentos em Atraso, sob pena de devolução.
6. Em caso de discordância por parte do CONTRAENTE PÚBLICO quanto aos valores indicados nas faturas, deve este comunicar, por escrito, ao COCONTRATANTE, os respetivos fundamentos, ficando o COCONTRATANTE obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.
7. A comunicação ao COCONTRATANTE referida no número anterior deve ser efetuada pelo CONTRAENTE PÚBLICO no prazo máximo de 10 (dez) dias.
8. Desde que devidamente emitidas, as faturas são pagas através de transferência bancária para a instituição de crédito indicada pelo COCONTRATANTE.
9. O atraso no pagamento das faturas apresentadas fará o CONTRAENTE PÚBLICO incorrer em mora com a correspondente aplicação, do artigo 1.º da Lei nº 3/2010, de 27 de abril, sobre o montante em dívida, à taxa legalmente fixada para o efeito, desde o respetivo vencimento até ao integral e efetivo pagamento.

SECÇÃO V

ACOMPANHAMENTO E FISCALIZAÇÃO DA EXECUÇÃO DO CONTRATO

Cláusula 16.ª

Acompanhamento da execução do CONTRATO

1. Sem prejuízo das competências exercidas pelos demais membros da equipa do CONTRAENTE PÚBLICO, a execução do CONTRATO é acompanhada pelo gestor do CONTRATO designado pelo CONTRAENTE PÚBLICO e mencionado no CONTRATO a celebrar.
2. 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.

SECÇÃO VI

MODIFICAÇÕES, INCUMPRIMENTO E EXTINÇÃO DO CONTRATO

Cláusula 17.ª

Penalidades

1. Pelo incumprimento de obrigações contratuais, por razões que lhe sejam imputáveis, o CONTRAENTE PÚBLICO pode exigir ao COCONTRATANTE o pagamento de uma sanção pecuniária, de montante a fixar em função da gravidade do incumprimento, nos termos e nas condições estabelecidas nos números seguintes.
   a) No valor de 0,5 ‰ (meio por mil) do preço contratual por cada dia de atraso na entrega de cada equipamento (por equipamento), do fornecimento ou instalação de licença ou de software;
   b) No valor de 1 ‰ (um por mil) do preço contratual por cada dia de atraso na conclusão da instalação de softwares ou quaisquer serviços objeto do CONTRATO, de acordo com os cronogramas fixados;
   c) No valor de €1.000,00 (mil euros) pela falta, sem justificação atempada e por motivo ponderoso, do gestor do projeto ou responsável pelo mesmo, a qualquer reunião agendada para a qual deva estar presente;
   d) No valor de 0,5 ‰ (meio por mil) do preço contratual por cada atraso de 10 (dez) minutos de incumprimento do tempo de resposta remoto para os pedidos de prioridade 1 e 2, nos termos melhor definidos na Parte II do CE;
   e) No valor de 0,5 ‰ (meio por mil) do preço contratual por cada atraso de 60 (sessenta) minutos de incumprimento do tempo de resposta remoto para os pedidos de prioridade 3 e 4, nos termos melhor definidos na Parte II do CE;
   f) No valor de 1 ‰ (um por mil) do preço contratual por cada atraso de 30 (trinta) minutos de incumprimento do tempo de resposta presencial para os pedidos de prioridade 1, e no valor de 0,5 ‰ (meio por mil) para os de prioridade 2, nos termos melhor definidos na Parte II do CE;
   g) No valor de 0,5 ‰ (meio por mil) do preço contratual por cada atraso de 60 (sessenta) minutos de incumprimento do tempo de resposta presencial para os pedidos de prioridade 3, nos termos melhor definidos na Parte II do CE;
2. O valor acumulado das penalidades a aplicar não poderá exceder o limite máximo de 20% do preço contratual.

3. Nos casos em que seja atingido o limite máximo previsto no número anterior, e o CONTRAENTE PÚBLICO decida não proceder à resolução do CONTRATO, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30 % (trinta por cento).
4. Em caso de resolução do CONTRATO por incumprimento definitivo, nos termos do artigo 333.º do CCP, o CONTRAENTE PÚBLICO pode aplicar uma pena pecuniária de até 20% (vinte por cento).
5. O CONTRAENTE PÚBLICO pode compensar os pagamentos devidos ao abrigo do CONTRATO com as penas pecuniárias devidas nos termos da presente cláusula, obrigando-se o COCONTRATANTE a emitir os necessários documentos contabilísticos para o efeito.
6. As penas pecuniárias previstas na presente cláusula não obstam a que o CONTRAENTE PÚBLICO exija uma indemnização pelo dano excedente nos termos das disposições relativas à obrigação de indemnização por mora e incumprimento definitivo previstas na lei.
7. A aplicação das sanções previstas no presente artigo será objeto de audiência prévia, nos termos previstos no n.º 2 do artigo 308.º do CCP.

Cláusula 18.ª

Força maior

1. Não podem ser impostas penalidades ao COCONTRATANTE, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, 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. Consideram-se como motivos de força maior, designadamente, os seguintes:
   a) Epidemias, greves, conflitos laborais, insurreições ou motins, guerra, invasão e mobilização que originem a suspensão ou interrupções do trabalho;
   b) Movimentos sísmicos, incêndios, explosões, inundações e acidentes graves que suspendam ou interrompam o trabalho.
3. Não constituem casos de força maior, designadamente:
   a) Circunstâncias que não constituam força maior para os subcontratados do COCONTRATANTE, na parte em que intervenham;
   b) Greves ou conflitos laborais limitados às sociedades do COCONTRATANTE ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;

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

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

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

f) Avarias nos sistemas informáticos ou mecânicos do COCONTRATANTE não devidas a sabotagem;

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

h) Declaração de estado de emergência ou de calamidade pública, imposições administrativas ou legislativas de teletrabalho ou de circulação, por motivos sanitários, que não sejam tecnicamente impeditivas da execução do CONTRATO.

4. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para o restabelecimento da situação.
5. Quando o motivo de força maior for reconhecido como comprovado pelo CONTRAENTE PÚBLICO, consideram-se os prazos acordados prorrogados pelo tempo em que aquele os tenha afetado.

Cláusula 19.ª

Resolução por parte do CONTRAENTE PÚBLICO

1. Sem prejuízo de outros fundamentos de resolução previstos na lei e no CONTRATO, o CONTRAENTE PÚBLICO, pode resolver o CONTRATO, a título sancionatório, no caso de incumprimento definitivo do CONTRATO por facto imputável ao COCONTRATANTE.
2. Para efeitos do disposto no número anterior, a Entidade Adjudicante pode qualificar como incumprimento definitivo o incumprimento dos prazos, parciais ou final, para a execução do CONTRATO e entrega de artes finais ou documentos similares, quando este tenha ultrapassado o prazo contratual e o posterior que possa ser fixado.
3. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao COCONTRATANTE.
4. O CONTRAENTE PÚBLICO pode, caso assim o entenda, solicitar ao COCONTRATANTE a cessão da posição contratual, nos termos constantes do artigo 318º-A do CCP.

Cláusula 20.ª

Resolução por parte do COCONTRATANTE

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o COCONTRATANTE pode resolver o CONTRATO quando o montante que lhe seja devido esteja em dívida há mais de 6 (seis) meses ou o montante em dívida exceda 25% (vinte cinco por cento) do preço contratual, excluindo juros.
2. O direito de resolução é exercido por via judicial.
3. No caso previsto na parte final do n.º 1, o direito de resolução pode ser exercido mediante declaração ao CONTRAENTE PÚBLICO, que produz efeitos 30 (trinta) dias após a receção dessa declaração, salvo se esta última cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.

Cláusula 21.ª

Caução

A celebração do CONTRATO não se encontra sujeita à prestação de caução, nos termos do artigo 88º, nº 2 alínea a) do CCP.

Cláusula 22.ª

Cessão da posição contratual e subcontratação

1. A cessão da posição contratual e a subcontratação apenas são permitidas mediante autorização prévia escrita do Contraente Público e nos termos previstos pelos artigos 317º a 318º do CCP.
2. No caso de subcontratação, o COCONTRATANTE permanece integralmente responsável perante o CONTRAENTE PÚBLICO, pelo exato e pontual cumprimento de todas as obrigações contratuais.

Cláusula 23.ª

Direitos de propriedade intelectual

1. A titularidade dos direitos de propriedade intelectual sobre quaisquer obras e materiais desenvolvidos, criados, modificados ou personalizados pelo COCONTRATANTE para o CONTRAENTE PÚBLICO ou pelo CONTRAENTE PÚBLICO ao abrigo do CONTRATO, incluindo nomeadamente o software, escritos, relatórios, esquemas, desenhos, imagens, fotografias, especificações, parametrizações, dados em formato eletrónico e tabulações, inquéritos e questionários, invenções, inovações técnicas, know-how, processos, técnicas, métodos de investigação, documentos ou quaisquer outras criações, de qualquer natureza ou meio, (em conjunto “obras”) pertencem ao CONTRAENTE PÚBLICO, ao abrigo do regime da

obra por encomenda e como tal cabendo exclusivamente a este todos os direitos de propriedade intelectual a elas inerentes, considerando-se contrapartida suficiente para tal a remuneração adjudicada.

2. O COCONTRATANTE garante que todos os seus colaboradores afetos à prestação de serviços, independentemente do vínculo jurídico que possuam com o COCONTRATANTE, foram atempadamente informados e aceitaram que os direitos de propriedade intelectual sobre as obras acima indicadas pertencem exclusivamente ao CONTRAENTE PÚBLICO.
3. O COCONTRATANTE é responsável pela infração de quaisquer direitos de patente, de conceção, de licenças, de projetos, de marcas, de nomes, ou de quaisquer outros direitos de propriedade intelectual, industrial ou afins, respeitantes aos bens e aos serviços objeto do CONTRATO, nomeadamente, projetos, estudos, programas informáticos, equipamento, materiais, documentação ou trabalhos realizados.
4. O COCONTRATANTE é responsável por qualquer reclamação formulada perante o CONTRAENTE PÚBLICO, resultante de violação dos direitos referidos nos números anteriores, adotando o CONTRAENTE PÚBLICO o procedimento que se revele mais adequado para a intervenção plena do COCONTRATANTE na discussão e no esclarecimento, perante terceiros reclamantes ou quaisquer autoridades, das dúvidas que, neste âmbito, se coloquem.
5. No caso de o CONTRAENTE PÚBLICO ser demandado por violação de direitos constantes dos números anteriores, o COCONTRATANTE indemniza-o por todas as despesas que, em consequência, deva suportar e por todas as quantias que tenha de pagar, seja a que título for.

Cláusula 24.ª

Transferência da propriedade

1. Com a aceitação dos bens e dos serviços objeto do presente CONTRATO, ocorre a transferência da propriedade dos mesmos para o CONTRAENTE PÚBLICO, bem como de todos os documentos elaborados pelo COCONTRATANTE previstos neste CE, podendo o CONTRAENTE PÚBLICO utilizá-los, reproduzi-los, alterá-los e cedê-los livremente, sem quaisquer restrições e sem necessidade de autorização do COCONTRATANTE.
2. Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente CE.

SECÇÃO VII

DISPOSIÇÕES FINAIS

Cláusula 25.ª

Comunicações

1. Salvo quando o contrário resulte do contrato, quaisquer comunicações entre o CONTRAENTE PÚBLICO e o COCONTRATANTE relativas ao CONTRATO devem ser efetuadas através de carta registada com aviso de receção ou correio eletrónico, para os contactos a definir obrigatoriamente no CONTRATO.
2. Qualquer comunicação feita por carta registada é considerada recebida na data em que for assinado o aviso de receção ou, na falta dessa assinatura, na data indicada pelos serviços postais.
3. Qualquer comunicação feita por correio eletrónico é considerada recebida no 2º (segundo) dia útil após o envio.

Cláusula 26.ª

Encargos

Todos os encargos decorrentes, do visto do Tribunal de Contas e da celebração do CONTRATO, bem como todos os que não se encontrem expressamente atribuídos ao CONTRAENTE PÚBLICO, são da responsabilidade do COCONTRATANTE.

Cláusula 27.ª

Contagem dos prazos

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

Cláusula 28.ª

Idioma Oficial

Toda a documentação, incluindo manuais, deverá estar disponível em Língua Portuguesa.

Cláusula 29.ª

Foro competente

Para todas as questões emergentes do CONTRATO será competente o Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

Cláusula 30.ª

Legislação aplicável

1. O CONTRATO é regulado pela lei portuguesa, com renúncia expressa a qualquer outra.
2. Sem prejuízo de outras leis e regulamentos especialmente aplicáveis, a tudo o que não esteja expressamente previsto ou regulado no programa do procedimento e no presente CE, é aplicável o CCP.

PARTE II

ESPECIFICAÇÕES TÉCNICAS

Lote 1 - Hardware, licenciamento e suporte

1. HARDWARE

a) **Surface Laptop 4 i5/8/256 GB Disco - Linha Empresarial, com teclado Português ou equivalente – Quantidade 40 (quarenta)**

Dimensões: Surface Laptop 4 de 13,5”: 308 mm × 223 mm × 14,5 mm (12,1" × 8,8" × 0,57") (ou equivalente)

Ecrã

Surface Laptop 4 de 13,5”:
Ecrã: Ecrã PixelSense™ de 13,5”
Resolução: 2256 x 1504 (201 PPP)
Proporção: 3:2
Suporte para Caneta para Surface2
Toque: Multitoque de 10 pontos

Memória: 8 GB RAM
Processador: Processador Quad Core Intel® Core™ i5-1145G7 de 11.ª Geração ou equivalente
Peso: Surface Laptop 4 de 13,5” ou equivalente, em **Preto Mate** e Arenito (Metal): 1.288 g (2,84 lb)
Exterior: Cores do Surface Laptop 4 de 13,5”7: Preto Mate com apoio para os pulsos em metal
Garantia: Extensões de Garantia para 3 anos;

b) **Surface Dock 2 (ou equivalente) – Quantidade 40 (quarenta) -** Compatível com o equipamento da alínea a);

c) **Ratos Surface Mobile Mouse Bluetooth (ou equivalente) – Quantidade 40 (quarenta)-** Compatível com o equipamento da alínea b);

d) **Mochilas PORTLAND BLACK 15.6" (ou equivalente) – Quantidade 40 (quarenta)**

Deve garantir todas as condições de proteção para o transporte do equipamento da alínea a);

2. **PERIFÉRICOS**

   a) **Auriculares tipo Microsoft (ou equivalente) ou tipo LifeChat LX-6000 for Business – Quantidade 65 (sessenta e cinco) –** Compatível com o equipamento, do ponto 1, alínea a);

   b) **Monitores tipo LG (ou equivalente) de 24 polegadas FullHD (VGA/HDMI) PN: 24MK400H – Quantidade 65 (sessenta e cinco) –** Compatível com o equipamento, do ponto 1, alínea b);

   Caraterísticas:

   Ecrã Full HD
   Tecnologia AMD FreeSync™
   Dynamic Action Sync
   Black Stabilizer
   On Screen Control
   Modo Poupança de Energia
   Ecrã 24'' Full HD com On Screen Control

   Resolução: 1920 x 1080

   c) **Teclados PT com fio – Quantidade 65 (sessenta e cinco) –** Compatível com o equipamento, do ponto 1, alínea b);

3. **Licenciamento Office 365 E5 (24 meses) – Quantidade 40 (quarenta);**
4. **Assistência Técnica Hardware -** Banco de horas de apoio técnico à instalação e manutenção PC – Quantidade 400 (quatrocentas) horas;

O prazo máximo de entrega relativo ao presente lote é de dez semanas, sendo excluídas as propostas que apresentem prazo superior.

Lote 2 - Serviços Cloud e Apoio

1. **Azure Monetary Commitments – Quantidade 28 (vinte e oito);**
2. **ITEXT single Instance Server Instance (subscrição 3 ano) – Quantidadee 1 (um);**
3. **Banco de horas Banco de horas de apoio técnico à instalação e manutenção dos servidores Azure – Quantidade 430 (quatrocentas e trinta) horas;**

Para referência adicional, os servidores Azure terão de conseguir dar resposta a, no mínimo, os seguintes requisitos:

Servidor	Sistema Operativo	Tipo	Ref	vCPU	Memória (Gb)	Disco Sistema - SSD Premium (Gb)	Disco Dados - Disco Ultra (Gb)
Base dados SQL Server Enterprise	Windows	SQL Server Enterprise	E4ds v4	4	32	256	1024
Serviços Aplicacionais Windows	Windows	Windows	D4ds v4	4	16	256	
SGO RP	Linux Ubuntu Advantage Advanced	LAMP	D4ds v4	4	16	256	
Balcão Beneficiário	Linux Ubuntu Advantage Advanced	LAMP	D4ds v4	4	16	256	
SGO Beneficiários Finais	Linux Ubuntu Advantage Advanced	LAMP	D2ds v4	2	8	256	
Balcão Beneficiário - Beneficiários Finais	Linux Ubuntu Advantage Advanced	LAMP	D2ds v4	2	8	256	

Requisitos adicionais obrigatórios:

1. Armazenamento partilhado Ficheiros do Azure – 2Tb
2. Armazenamento para instantâneos diários de todos os discos de todos os servidores, bem como do armazenamento partilhado
3. Backup diário de todos os servidores
4. Software: Licença iText 7 (https://itextpdf.com/) – Para manipulação de PDF (incluindo processamento de assinaturas digitais)

O prazo máximo de entrega relativo ao presente lote é de três semanas, sendo excluídas as propostas que apresentem prazo superior.

Lote 3 - Licenciamento Microsoft

1. Licenciamento Microsoft - Common Area Phone (subscrição 3 anos) – Quantidade 2 (dois);
2. Licenciamento Microsoft - Microsoft Teams Rooms Standard Promo (subscrição 3 anos) – Quantidade 2 (dois).

O prazo máximo de entrega relativo ao presente lote é de três semanas, sendo excluídas as propostas que apresentem prazo superior.

Lote 4 - Outros Software

1. Acrobat Pro DC for teams Multi European Languages Team Licensing Subscription New (subscrição 3 anos) – Quantidade 10 (dez);
2. ZOOM PRO (subscrição 3 anos) – Quantidade 3 (três);
3. Certificados de CDA de Selo Eletrónico (subscrição 3 anos), para ser utilizado num servidor na Cloud. – Quantidade 1 (um)

O prazo máximo de entrega relativo ao presente lote é de três semanas, sendo excluídas as propostas que apresentem prazo superior.

Lote 5

Infraestrutura de LAN, Wifi, Segurança, Endpoints de Vídeo e Serviços Associados

Com a presente contratação, a EMRP pretende criar uma infraestrutura tecnológica que permita constituir um meio fiável, ágil e seguro para a prossecução da sua missão. Para o efeito, a EMRP pretende implementar uma solução baseada em controladores existentes na Cloud para minimizar a dependência dos ambientes *on-premises,* garantindo assim escalabilidade, flexibilidade e resiliência. A contratação em causa no presente lote tem por objeto o fornecimento de material de nova geração e com altos padrões de resiliência, garantindo uma infraestrutura "*always up"*, respondendo sempre às necessidades de cada utilizador/dispositivo.

A solução pretendida encontra-se também vocacionada para garantir um nível de segurança alto, garantindo ao máximo o impedimento das intrusões no perímetro, como também ao nível do *endpoint* (dispositivo). Encontra-se prevista a implementação de várias ferramentas que permitem incrementar o nível de segurança em várias camadas.

Constitui igualmente objeto do CONTRATO a celebrar para o presente lote, o fornecimento e configuração de terminais telefónicos e salas de vídeo conferência, assim como equipamento que permita ligação entre a solução de comunicações (MS Phone System) e a rede de operador, genericamente designado como SBC.

- Características Genéricas

1. Mapa de quantidades:

Equipamento	Quantidades
Switch tipo 1	2
Switch tipo 2	2
Ponto de acesso	5
Transceiver	4

Cabo direto (Stack)	4
Router/Firewall	1
Segurança DNS	50 dispositivos
Segurança de dispositivo	50 dispositivos
Telefone tipo 1	15
Telefone tipo 1	7
Telefone tipo 1	4
Sala video tipo 1	1
Sala video tipo 2	1
Session Border Controler	1

Toda e qualquer solução que implique subscrições, deverá ser proposta com um período de 3 anos, de acordo com o contrato de manutenção que será também celebrado pelo mesmo período de 3 anos.

2. Networking

Pontos de acesso

Requisitos WiFi

Teremos pontos de acesso WiFi. Esta é uma componente fundamental do negócio, por se tratar da interface entre a EMRP e os seus clientes. Pretende-se a aquisição de 5 (cinco) pontos de acesso com as seguintes funcionalidades:

1. Por motivos de segurança os pontos de acesso não deverão ter porto série (RS232/USB) de gestão local. A gestão local deve também ela ser limitada, sendo que toda a gestão do ponto de acesso deverá ser assegurada por uma plataforma de gestão principal.
2. A comunicação com a plataforma de gestão principal deve ser encriptada.
3. Possibilidade de upgrade de firmware automático a partir da plataforma de gestão, sem intervenção manual.

4. Funcionalidades de integração com soluções de proteção a nível de *Domain Name System* (DNS).
5. Ferramentas de estatística e troubleshooting que permita de uma forma intuitiva detetar problemas na rede de pontos de acesso, como por exemplo problemas de acesso por parte dos clientes à rede WiFi, qualidade de utilização irregular e sobre-utilização dos pontos de acesso.
6. 802.11ax com 4x4 Multiple-Input Multiple-Output (MIMO) com 4 (quatro) spatial streams, a operar em Single User ou Multiuser MIMO (MU-MIMO).
7. Beacons Bluetooth de baixa energia (BLE) e scanning radio.
8. Suporte em tempo real, 24x7, de mecanismos *Wireless Intrusion Prevention System* (WIPS) e *Wireless Intrusion Detection System* (WIDS).
9. Circuito radio dedicado para *spectrum analytics* e *location tracking*.
10. Segurança empresarial e acesso *guest* integrado.
11. Suportar visibilidade aplicacional, permitindo identificação de aplicações e definição de políticas *QoS* sobre cada tipo de tráfego.
12. Suportar os standards 802.11a, 802.11b/g, 802.11n, 802.11ac e 802.11ax.
13. Suportar canais na banda dos 2,4GHz e dos 5GHz.
14. Frame rates agregados de 3.5Gbps.
15. Suportar *Enterprise Mobility Management* (EMM) e *mobile device management* (MDM).
16. Deve suportar 802.1p e WiFi Multimedia (WMM).
17. Suportar protocolos de segurança WEP, WPA, WPA2-PSK, WPA2-Enterprise com 802.1x, WPA3 - Personal, WPA3 – Enterprise e WPA3 - Enhanced Open (OWE).
18. Suportar 802.1q e VPNs IPsec.
19. Suportar autenticação EAP-TLS, EAP-TTLS, EAP-MSCHAPv2 e EAP-SIM.
20. Suportar encriptação TKIP e AES.
21. Deve ter 1 porta 100/1000/2.5G BASE-T Ethernet (RJ45).
22. Suporte para *Maximal ratio combining* (MRC) e *beamforming*.
23. Canais de 20, 40 e 80MHz.
24. Antenas omnidirecionais integradas.
25. Suporte para *Power over Ethernet* (PoE) com entrada de alimentação DC alternativa.

Switch tipo 1

De forma a interligar os pontos de acesso, será também necessário o fornecimento de equipamentos de switching, com os seguintes requisitos:

2 (dois) switches Tipo 1 com as seguintes características:

1. Deve ter 16 portas 10/100/1000BASE-T Ethernet RJ45, 8 portas 100M/1G/2.5G/5/10G Ethernet RJ45 e 4 portas SFP+ 10G uplink.
2. Deve ter 2 portas de stacking.
3. Suporte para stacking físico até 8 switches.

4. Suporte para stacking virtual para gestão, monitorização e configuração unificada através de um único stack lógico.
5. Suporte para 802.3af/802.3at Power-over-Ethernet (PoE/PoE+/UPoE) disponível em todas as portas (máximo de 60W por porta para UPoE), com um output máximo de PoE de 740W com apenas uma fonte de alimentação instalada.
6. Capacidade de operar em temperaturas entre -5ºC até 50ºC.
7. MTBF (a 25ºC) mínimo de 321,515h.

Switch tipo 2

2 (dois) switches Tipo 2 com as seguintes características:

1. Deve ter 24 portas 10/100/1000BASE-T Ethernet RJ45 e 4 portas SFP+ 10G uplink.
2. Deve ter 2 portas de stacking.
3. Suporte para stacking físico até 8 switches.

4. Suporte para stacking virtual para gestão, monitorização e configuração unificada através de um único stack lógico.

5. Suporte para 802.3af (PoE) 15.4 W por porta e 802.3at (PoE+) 30 W por porta, disponível em todas as portas, com um output máximo de PoE de 370W com apenas uma fonte de alimentação instalada.

6. Capacidade de operar em temperaturas entre 0ºC até 45ºC.
7. MTBF (a 25ºC) mínimo de 568,000h.

Características gerais da solução de switching:

1. À semelhança dos pontos de acesso os switches não deverão ter porto série (RS232/USB) de gestão local, que deve ser limitada, e assegurada por uma plataforma de gestão principal.
2. A comunicação com a plataforma de gestão principal deve ser encriptada.
3. Suportar visibilidade aplicacional.
4. Possibilidade de upgrade de firmware calendarizado a partir da plataforma de gestão, sem intervenção manual.
5. A configuração das interfaces do switch deve poder ser feita utilizando grupos, mesmo que estes abranjam diferentes equipamentos.
6. Suporte para VLAN voz para VoIP.
7. Suporte para LLDP, Port-Mirroring, IGMP Snooping e LACP.
8. Suporte para *queues* QoS para voz, vídeo e dados.
9. Suportar 802.1x e RADIUS *server monitoring.*
10. Suportar *Access Control Lists* (ACLs) para IPv4 e IPv6.
11. Suporte para *DHCP snooping* e *Spanning Tree* (STP) e RSTP.
12. Possibilidade de aprovisionamento automático de novos switches com o uso de templates de configuração.
13. Suportar *role-based access control* (RBAC).
14. Suporte para stacking entre equipamentos switching do Tipo 1 e entre equipamentos switching do Tipo 1 e Tipo 2.

Interligação de equipamentos de switching

Transceivers

Pretende-se o fornecimento de 4 (quatro) acopladores ópticos SFP+ 10GBASE-LRM para fibra multimodo com capacidade até 220 metros.

Os adaptadores fornecidos devem ser compatíveis e do mesmo fabricante que os equipamentos de switching anteriormente descritos.

Stacking

Deverá ser fornecido um cabo de stacking juntamente com cada equipamento de switching.

Características gerais da solução:

A gestão da rede de acesso, constituída pelos pontos de acesso e switches deve ser feita através da mesma plataforma de gestão. Esta deve respeitar os seguintes requisitos:

1. A plataforma de gestão deve situar-se *off premises*, numa Cloud segura e com redundância geográfica.
2. Oferecer ao usuário a possibilidade de realizar e descarregar capturas de tráfego, através da sua consola de gestão.
3. A plataforma de gestão deve apresentar um histórico de usuários e estatísticas para um mínimo de 30 dias, sem recurso a hardware adicional.
4. Suportar *Multi-Factor Authentication*, 802.1x e RADIUS
5. Visibilidade, controlo, monitorização e alarmística através de um único dashboard, tanto para a rede de switching como de pontos de acesso.
6. Registo de atividade e eventos dos elementos da rede.
7. A comunicação com os equipamentos deverá ser assegurada através de SSL.
8. A plataforma de gestão deverá oferecer uma *Graphical User Interface* (GUI) e poder ser acedida a partir de um Web Browser.
9. Ser PCI compliant.

3. Colaboração

Constitui ainda do presente lote, o fornecimento de soluções, equipamentos voz, vídeo e Session Border controler (SBC).

Todos os equipamentos a fornecer têm de ser suportados e certificados para integração simples e completa com a solução de comunicações baseada em Microsoft Teams.

Características técnicas dos telefones a fornecer:

Telefone tipo 1 - Modelo de referência Poly CCX400 Business Media Phone

1. Recursos do interface de utilizador
    1.1. A tecnologia HD Voice oferece qualidade de voz realista para todos os canais de áudio: monofone, alta-voz e headset opcional
    1.2. proporciona conversas full duplex, cancelamento de eco acústico e redução de ruído de fundo
    1.3. Ecrã sensível ao toque com recurso multitoque e baseada em gestos
    1.4. LCD colorido de 5 polegadas (720 x 1280 pixels)
    1.5. Proporção de 9:16
    1.6. Protetor de tela
    1.7. Teclado virtual na tela
    1.8. Suporte a correio de voz
    1.9. Altura da base ajustável
    1.10. Uma porta USB tipo A (compatível com 2.0) para aplicativos de mídia e armazenamento
    1.11. Suporte a caracteres Unicode UTF-8
    1.12. Seleção de tamanho de fonte ajustável (normal, médio, grande)
2. Recursos de Áudio
    2.1. Áudio de banda larga TIA-920, compatível com tipo 1 (IEEE 1329 full duplex)
    2.2. Resposta de frequência – 150 Hz a 7 kHz para os modos monofone, headset opcional e viva-voz
    2.3. Codecs: G.711 (A-law e µ-law), G.729AB, G.722 (HD Voice), G.722.1 iLBC
    2.4. Configurações de volume individuais com feedback visual para cada canal de áudio
    2.5. Deteção de atividade de voz

2.6. Geração de ruído de conforto

2.7. Geração de tom DTMF (RFC 2833 e em banda)

2.8. Transmissão de pacotes de áudio com baixo atraso

2.9. Buffers de tremulação adaptativos

2.10. Ocultação de perda de pacotes

---

3. Segurança
   3.1. Autenticação 802.1X e criptografia de mídia EAPOL via SRTP
   3.2. Segurança da camada de transporte (TLS)
   3.3. Arquivos de configuração criptografados
   3.4. Autenticação Digest
   3.5. Senha de acesso
   3.6. Suporte para sintaxe de URL com senha para endereço do servidor de inicialização
   3.7. Provisionamento de HTTPS seguro
   3.8. Suporte para executáveis de software certificados
4. Alimentação
   4.1. Auto-detecção incorporada IEEE 802.3af Power over Ethernet 13 W (Máx)
   4.2. Adaptador Ac/DC Universal Externo (opcional) 5 VDC @ 3 A (15 W)
   4.3. Energy STAR® avaliado

Telefone tipo 2 - Modelo de referência Poly CCX500 Business Media Phone

1. Recursos do interface de utilizador
   1.1. A tecnologia HD Voice oferece qualidade de voz realista para todos os canais de áudio: monofone, viva-voz e headset opcional
   1.2. proporciona conversas full duplex, cancelamento de eco acústico e redução de ruído de fundo
   1.3. Ecrã sensível ao toque com recurso multitoque e baseada em gestos
   1.4. LCD colorido de 5 polegadas (720 x 1280 pixels)
   1.5. Protetor de tela com proporção de 9:16

1.6. Teclado virtual na tela

1.7. Suporte a correio de voz

1.8. Altura da base ajustável

1.9. Uma porta USB tipo A (compatível com 2.0) para aplicativos de mídia e armazenamento

1.10. Uma porta USB tipo C (compatível com 2.0) para aplicativos de mídia e armazenamento

1.11. Bluetooth 4.2 integrado

1.12. Suporte a caracteres Unicode UTF-8

1.13. Seleção de tamanho de fonte ajustável (normal, médio, grande)

2. Recursos de áudio

2.1. cancelamento de eco acústico e redução de ruído de fundo

2.2. Áudio de banda larga TIA-920, compatível com tipo 1 (IEEE 1329 full duplex)

2.3. Resposta de frequência - 100 Hz a 20 kHz para os modos monofone, headset opcional e viva-voz

2.4. Codecs: G.711 (A-law e μ-law), G.729AB, G.722 (HD Voice), G.722.1 iLBC

2.5. Configurações de volume individuais com feedback visual para cada canal de áudio

2.6. Deteção de atividade de voz

2.7. Geração de ruído de conforto

2.8. Geração de tom DTMF (RFC 2833 e em banda)

2.9. Transmissão de pacote de áudio de baixo atraso

2.10. Buffers de tremulação adaptativos

2.11. Ocultação de perda de pacotes

2.12. Suporte a OPUS

3. Segurança

3.1. Autenticação 802.1X e criptografia de mídia EAPOL via SRTP

3.2. Segurança da camada de transporte (TLS)

3.3. Arquivos de configuração criptografados

3.4. Autenticação Digest

3.5. Senha de acesso

3.6. Suporte para sintaxe de URL com senha para endereço do servidor de inicialização

3.7. Provisionamento de HTTPS seguro

3.8. Suporte para executáveis de software certificados

4. Alimentação

4.1. Sensor automático integrado IEEE 802.3af Power over Ethernet 13W Máx.)

4.2. Adaptador CA/CC universal externo (opcional) 48 VCC a 0,52 A (25W)

4.3. Classificação ENERGY STAR®

Telefone tipo 3 - Modelo de referência Poly CCX600 Business Media Phone

1. Recursos do interface de utilizador

1.1. Ecrã sensível ao toque com recurso multitoque e baseada em gestos

1.2. LCD colorido de 7 polegadas (resolução de 1024x600 pixels)

1.3. Protetor de tela com proporção de 16:9

1.4. Teclado virtual na tela

1.5. Suporte a correio de voz

1.6. Altura da base ajustável

1.7. Uma porta USB tipo A (compatível com 2.0) para aplicativos de mídia e armazenamento

1.8. Uma porta USB tipo C (compatível com 2.0) para aplicativos de mídia e armazenamento

1.9. Bluetooth 4.2 integrado

1.10. Wi-Fi integrado

1.11. Suporte a caracteres Unicode UTF-8

1.12. Seleção de tamanho de fonte ajustável (normal, médio, grande)

2. Recursos de Áudio

2.1. A tecnologia HD Voice oferece qualidade de voz realista para todos os canais de áudio: monofone, viva-voz e headset opcional

2.2. proporciona conversas full duplex, cancelamento de eco acústico e redução de ruído de fundo

2.3. Áudio de banda larga TIA-920, compatível com tipo 1 (IEEE 1329 full duplex)

2.4. Resposta de frequência - 100 Hz a 20 kHz para os modos monofone, headset opcional e viva-voz

2.5. Codecs: G.711 (A-law e µ-law), G.729AB, G.722 (HD Voice), G.722.1 iLBC

2.6. Configurações de volume individuais com feedback visual para cada canal de áudio

2.7. Deteção de atividade de voz

2.8. Geração de ruído de conforto

2.9. Geração de tom DTMF (RFC 2833 e em banda)

2.10. Transmissão de pacotes de áudio com baixo atraso

2.11. Buffers de tremulação adaptativos

2.12. Ocultação de perda de pacotes

2.13. Suporte a OPUS

3. Segurança

3.1. Autenticação 802.1X e criptografia de mídia EAPOL via SRTP

3.2. Segurança da camada de transporte (TLS)

3.3. Arquivos de configuração criptografados

3.4. Autenticação Digest

3.5. Senha de acesso

3.6. Suporte para sintaxe de URL com senha para endereço do servidor de inicialização

3.7. Provisionamento de HTTPS seguro

3.8. Suporte para executáveis de software certificados

3.9. Criptografia Wi-Fi: WEP, WPA-Personal, WPA2-Personal, WPA2-Enterprise com 802.1X (EAP-TLS, PEAP-MSCHAPv2)

4. Alimentação

4.1. Sensor automático integrado IEEE 802.3at Power over Ethernet 25 W (Máx.)

4.2. Adaptador universal externo CA/CC (opcional), 48 VCC a 0,52 A (25 W)

Sessio Border Controler

A solução de SBC pretendida deverá ser uma solução baseada em appliance, que que permita a comunicação entre a solução de colaboração (MS teams), e o operador de comunicações.

Este equipamento deverá estar licenciado inicialmente para suportar 20 comunicações em simultâneo podendo ser licenciado para suportar até pelo menos 250 sessões.

Seguidamente são apresentadas as características técnicas que o equipamento pretendido deverá suportar/possuir:

1. Interfaces
   1.1. 4 GE e 8 FE portas com uma única fonte de alimentação AC
2. Segurança
   2.1. Suporte DoS/DDoS line rate protection, bandwidth throttling, dynamic blacklisting (Sistema de Deteção de Intrusões)
   2.2. Suportar, RTP pinhole management, rogue RTP detection and prevention, SIP message policy, advanced RTP latching
   2.3. Suportar,TLS, DTLS, SRTP, HTTPS, SSH, cliente/servidor Autenticação SIP Digest, RADIUS Digest
   2.4. Suportar, Automatic topology hiding, user privacy
   2.5. Separação VLAN/interface física para múltiplos meios, interfaces de controlo e OAMP
   2.6. Deteção e prevenção de ataques VoIP, roubo de serviço e acesso não autorizado
3. Interoperabilidade
   3.1. SIP B2BUA - Full SIP transparency, mature and broadly deployed SIP stack, stateful proxy mode
   3.2. SIP Interworking
   3.3. Registration and Authentication - SIP Registrar, registration on behalf of users/servers, SIP Digest access authentication
   3.4. Transport Mediation - Mediation between SIP over UDP/TCP/TLS/WebSocket, IPv4/IPv6, RTP/SRTP (SDES/DTLS)
   3.5. Header Manipulation - Add/modify/delete SIP headers and message body using simple WireShark-like language with powerful capabilities such as variables and utility functions
   3.6. Number Manipulations - Ingress and egress digit manipulation
   3.7. Transcoding and Vocoders - Coder normalization including transcoding, coder enforcement and re-prioritization, extensive vocoder support: G.711, G.723.1, G.726, G.729A/B, GSM-FR, AMR-NB, AMR-WB (G.722.2), SILK-NB/WB, Opus-NB/WB, iLBC
   3.8. Signal Conversion - DTMF/RFC 2833/SIP, T.38 fax, T.38 V3, V.34, packet-time conversion, V.150.1
   3.9. WebRTC Gateway - Interworking between WebRTC endpoints and SIP networks. Supports WebSocket, Opus, VP8 video coder, lite ICE, DTLS, RTP multiplexing.



3.10. NAT - Local and far-end NAT traversal for support of remote workers

4. Voice Quality and SLA
   4.1. Call Admission Control - Limit number and rate of concurrent sessions and registers per peer for inbound and outbound directions
   4.2. Packet Marking - 802.1p/Q VLAN tagging, DiffServ, TOS
   4.3. Standalone Survivability - Maintains local calls in the event of WAN failure. Outbound calls can use PSTN fallback (including E911).
   4.4. Voice Monitoring and Enhancement - Transrating, RTCP-XR, Acoustic echo cancellation, replacing voice profile due to impairment detection, fixed and dynamic voice gain control, packet loss concealment, dynamic programmable jitter buffer, silence suppression/comfort, noise generation, RTP redundancy, broken connection detection
   4.5. Direct Media - Hair-pinning (no media anchoring) of local calls to avoid unnecessary media delays and bandwidth consumption
   4.6. High Availability - SBC high availability with two-box redundancy, active calls preserved
   4.7. Test Agent - Ability to remotely verify connectivity, voice quality and SIP message flow between SIP UAs

1. Tratamento de chamadas SIP
   a. Criterios - Incoming SIP trunk, DID ranges, host names, any SIP headers, codecs, QoE, bandwidth
   b. Consulta de bases de dados externas - Destinations based on customized queries of ENUM, LDAP, HTTP server (REST API)
   c. Destinos disponíveis - Pares SIP configurados, utilizadores registados, endereço IP, solicitar URI
   d. Advanced Features - Alternative destinations, load balancing, LCR, call forking, E911 emergency call detection and prioritization
   e. SBC Media Types - Audio\Video\Fax\Text\Message Session Relay Protocol (MSRP)\Binary Floor Control Protocol (BFCP)
   f. SIPREC - IETF standard SIP recording interface, supporting both audio and video SBC sessions

- Gestão

- OAM&P - Browser-based GUI, CLI, SNMP, INI Configuration file, REST API, One Voice Operations Center (OVOC)

- Alimentação
  - Internal AC power supply rated: 100-240 VAC ~50- 60Hz 1.5A maximum (Optional) Additional 12V 10A DC power, via an AudioCodes external AC/DC power adaptor

Salas de Video Conferência

Pretende-se equipar duas salas com meios e equipamentos, que permitam a participação em reuniões por vídeo conferência. Devem estar integradas com a solução de colaboração MS Teams e serem MS Teams Certified. Estas salas deverão ser equipadas com:

Sistema de vídeo conferência;

1. Equipamentos audiovisuais para suporte à solução de vídeo conferência;
2. Cabos e acessórios necessários ao correto funcionamento da solução;

Deverá no mínimo permitir as seguintes funcionalidades:

1. Join a scheduled meeting (Microsoft Teams Meeting)
2. Initiate an ad hoc meeting (Microsoft Teams Meeting)
3. Manage your room device with Microsoft Intune

Sala tipo 1 – Características técnicas

O sistema de videoconferência a fornecer deverá ser composto por câmara, colunas e microfones integrados numa plataforma de hardware tipo barra, e uma interface de comando, do tipo touchpad, suporte até dois monitores e a câmara deverá ter enquadramento automático de pessoas. Deverá também ser equipada com uma televisão de 65” 4K e suporte de chão com rodas.

Características do Sistema de conferência tipo barra:

1. Vídeo:

1.1. Uma porta input HDMI

1.2. Duas portas output HDMI

1.3. Compatibilidade com display touch

1.4. Protocolos H.264 AVC, H.264 High Profile, H.265, H.239

1.5. Resolução de vídeo tanto input e output até UHD (3840 x 2160)

2. Câmera:

2.1. Área de cobertura de 120°

2.2. 5x zoom digital

2.3. Resolução UHD 2160p (4K)

2.4. Possibilidade de adição de câmaras secundárias via USB ou HDMI

2.5. Suporte às tecnologias People Framing e Speaker Tracking

3. Áudio

3.1. Uma porta input HDMI

3.2. USB áudio

3.3. Output para Stereo speakers

3.4. 3x microfones MEMS, mais 2x microfones de segunda ordem

3.5. Input 3.5 mm line-in

3.6. Output 3.5 mm

3.7. Microphone pickup range 25 ft

4. Network

4.1. IPv4 e IPv6

4.2. Um porta Ethernet 10/100/1G

4.3. Auto-MDIX

4.4. Reconfigurable MTU size

4.5. Web proxy support—Basic, Digest, and NTLM

4.6. H.323 e/ou SIP até 6 Mbps

4.7. Simple Certificate Enrollment Protocol (SCEP)

4.8. Dynamic bandwidth allocation

4.9. Tecnologia Polycom Lost Packet Recovery (LPR) ou equivalente

5. Interoperabilidade

5.1. USB device mode

5.2. Certificação Zoom e Microsoft Teams

5.3. Suporte nativo para aplicações de terceiros como Zoom, Microsoft Teams, GoToRoom, RingCentral, 8x8 e StarLeaf

6. Segurança

6.1. BFCP

6.2. Security profiles

6.3. Media encryption (H.323, SIP): AES-128, AES-256

6.4. Remote logging with support for TLS

6.5. Active directory external authentication

6.6. H.235.6 support

6.7. Authenticated access to admin menus, web interface, and API

6.8. Security profiles

6.9. Local account and login port lockout

6.10. Local account password policy configuration

6.11. Secure defaults

7. Outras interfaces

7.1. Duas portas USB-A (3.0)

7.2. Uma porta UDB-C

7.3. Bluetooth 5.0

7.4. WiFi 802.11a/b/g/n/ac (MIMO) Multi-channel Concurrency

Características da interface de comando:

1. Ecrã

1.1. 8 polegadas

1.2. Resolução WXGA (1280 x 800)

1.3. Ângulo de visão de 75°

2. Tecnologia

2.1. IPC (In-Plane Switching)

2.2. Painel LCD com iluminação de fundo LED

2.3. Capacidade multi-touch

2.4. Comando directo de API pela rede

3. Outras características

3.1. Suporte integrado

3.2. Calendário integrado

3.3. Compartilhamento de conteúdo, ajuste da câmera e alteração dos layouts dos participantes

3.4. Alimentação por meio da ethernet (PoE) compatível com IEE 802.3af classe 3

3.5. Mode de suspensão de baixo consumo de energia

Sala tipo 2 – Características técnicas

O sistema de videoconferência a fornecer deverá ser um sistema modular composto por duas câmaras, com enquadramento automático, uma interface de comando, do tipo touchpad e um PC incorporado. Deverá também ser equipada com um microfone de conferência, uma televisão de 75" 4K e suporte de parede.

Características da interface de comando:

1. Ecrã

1.1. 8 polegadas

1.2. Resolução 1280 x 800

1.3. Ângulo de visão de 170°

1.4. Sensor de movimento PIR

2. Interface

2.1. USB 3.1 Tipo C

2.2. USB 3.1 Tipo A

2.3. HDMI Mini

2.4. Jack 3,5mm

2.5. Power Jack

2.6. Sensor de movimento PIR

3. Outras características
    3.1. Bloqueio Kensignton

Características da câmera

1. Características gerais
    1.1. 2x câmeras
    1.2. 1080p @ 60 FPS
    1.3. Enquadramento automático do grupo e rastreio de alto-falante ativo
    1.4. 12x Zoom (cada câmera)
    1.5. Matriz de microfone incorporado para rastreio de altifalantes
    1.6. Ângulo de visão120°
    1.7.
2. Compatibilidade
    2.1. Certificada para Microsoft Teams Rooms
    2.2. Microsoft Surface Hub e Hub 2
    2.3. Certificada para Skype for Business
3. Interfaces
    3.1. 2x USB 2.0
    3.2. 1x HDMI in
    3.3. 1x HDMI out
    3.4. 1x mini-HDCI
    3.5. 1x 3.5 mm stereo line-in

Características do microfone de conferência:

1. Áudio
    1.1. 3 Microfones 360º
    1.2. Alta qualidade de som e conversas Full Duplex
    1.3. Cancelamento de ruído externo
    1.4. Codecs suportados:
        1.4.1. G.711 (A-law and µ-law)



1.4.2. G.719 - G.722

1.4.3. G722.1

1.4.4. G722.1C

1.4.5. G.729AB

1.4.6. Siren 14

1.4.7. iLBC (3.33 Kbps and 15.2 Kbps)

1.4.8. Opus (8 Kbps–24 Kbps)

1.4.9. SILK

1.5. Emparelhamento de dispositivo Bluetooth

2. Network

2.1. Open SIP

2.2. Microsoft Teams

2.3. SDP

2.4. IETF SIP (RFC 3261 and companion RFCs)

3. Segurança

3.1. Autenticação 802.1X e EAPOL

3.2. Transport layer security (TLS) v1.2

3.3. Media encryption via SRTP

3.4. Encrypted configuration files

3.5. Wi-Fi encryption1 : WEP, WPA-Personal, WPA2-Personal, WPA2-Enterprise with 802.1X (EAP-TLS, PEAP-MSCHAPv2)

3.6. QoS- IEEE 802.1p/Q tagging (VLAN), layer 3 TOS, and DSCP

3.7. WMM (Wi-Fi multimedia)

3.8. Suporte para executáveis de software assinados

3.9. Password login

3.10. Autenticação Digest

3.11. Provisionamento seguro HTTPS

3.12. Suporte para sintaxe de URL com senha para endereço do servidor de inicialização



Características do PC:

1. Especificações
    1.1. Processador Intel Core i5-9600T CPU 2.30GHz/3.9 GHz (base/max)
    1.2. Sistema operativo Microsoft Windows 10 Enterprise IoT
    1.3. Memória interna de 32 GB
    1.4. Disco SSD de 120 GB
    1.5. WiFi e Bluetooth
2. Interface (frente)
    2.1. USB 3.1 Gen 2
    2.2. USB 3.1 Gen 1 Tipo-C
    2.3. Microfone jack
    2.4. Fones de ouvido/Microfone combo jack
3. Interface (trás)
    3.1. USB 3.1 Gen 2 (2x)
    3.2. USB 3.1 Gen 1 (2x)
    3.3. Gigabit Ethernet (RJ45)
    3.4. Display port/HDMI
    3.5. HDMI

4. Monitores

a) Monitores semi profissionais de 65” e 75”
b) Resolução 4K
c) Brilho mínimo 500 cd/m2
d) IPS
e) Funcionamento 18x7
f) Relação de contraste dinâmico 450000:1
g) Áudio 10W + 10W
h) Google Chromecast built-in and Apple Airplay
i) Garantia de 3 anos



5. Segurança

5.1. Router/Firewall

A solução de router/firewall pretendida deverá ser uma solução gerida por uma plataforma assente em cloud e totalmente integrável com a solução de switching e DNS Security a implementar.

Desta forma pretende-se que através da solução de gestão centralizada cloud-based seja possível ter visibilidade e gestão de:

a) Network security
b) WAN connectivity
c) Content and web security
d) Policy application
e) Unified access
f) Application management
g) Software-defined WAN (SD-WAN)

5.2.O equipamento a adquirir deverá cumprir as seguintes características técnicas:

a) Stateful firewall throughput: 1 Gbps
b) Advanced security troughput: 750 Mbps
c) Maximum site-to-site VPN throughput: 500 Mbps
d) Maximum site-to-sote VPN tunnels: 75
e) Interfaces WAN (dedicadas): 1x GbE SFP, 2x GbE RJ45
f) Interfaces LAN (fixas): 10x GbE RJ45 (2x PoE)
g) Mounting: Desktop ou wall mount
h) Dimensões: 283 mm x 148 mm x 27 mm
i) Peso: 0.85 kg
j) Power Supply: 100W DC
k) Power load (idle/max): 12W/96W
l) Temperatura de operação: 0°C a 45°C

A solução a propor deve contemplar os serviços de subscrição por um período de duração de 3 anos.

5.3.Os serviços de subscrição deverão permitir à solução ter as funcionalidades de:

a) Gestão centralizada Cloud-based com open APIs e 24×7 enterprise support
b) Verdadeiro zero-touch provisioning e firmware updates
c) Site-to-site Auto VPN
d) Client VPN
e) Traffic shaping e prioritização
f) WAN failover automático
g) Sub-second site-to-site VPN failover e dynamic path selection
h) Source based routing e IP-based local breakout
i) Content filtering
j) Intrusion Detection & Prevention

5.4.Funcionalidades de Content filtering

a) Capacidade de aplicar Blocked e whitelisted URL patterns com base em group policies
b) Capacidade de aplicar Blocked categories via group policy (integrando com a AD)
c) Capacidade de aplicar Blocked e whitelisted URL patterns via network-wide content-filtering rules
d) Capacidade de aplicar Blocked categories via network-wide content-filtering rules

6. Solução de DNS Security

A solução de DNS Security pretendida deverá ser uma solução baseada na Cloud, que forneça a primeira linha de defesa onde quer que os utilizadores estejam, dentro ou fora da organização mesmo quando estes têm a VPN para a empresa desativada.
A solução deve comtemplar um universo de 50 utilizadores e um período de duração de 3 anos.

6.1.Características técnicas para a solução pretendida:

a) Solução 100% baseada na Cloud.
b) Interface de gestão Web-based com suporte para APIs para integrações futuras.
c) Solução baseada em DNS com capacidade de proteção de qualquer porto ou protocolo.

d) Suporte para Anycast Routing, no qual todos os Datacenter da solução Cloud anunciam o mesmo endereço IP.
e) Possuir capacidade de aprendizagem estatística e Machine Learning por forma a detetar ameaças existentes e emergentes.
f) Capacidade de funcionar sem recorrer a mecanismos de VPN (SSL & IPSEC, etc)

6.2.Funcionalidades de proteção:

a) Capacidade de proteger qualquer tipo de dispositivo independentemente da sua localização.
b) Proteção dos utilizadores dentro e fora do perímetro da rede e organização.
c) Prevenção de ataques de Malware, Phishing e Command & control (C2) Callbacks em qualquer porta ou protocolo.
d) Parar conexões para domínios maliciosos logo ao nível do DNS
e) Deve ser possível adicionar um layer de segurança sobre o DNS apenas apontando os servidores de DNS para esta solução.
f) Funcionalidade de URL Filtering/Content Filtering com uma base de dados de domínios categorizada com 60 ou mais categorias.

6.3. Funcionalidades de controlo:

a) Capacidade de definir políticas baseadas em utilizadores de Active Directory.
b) Capacidade de definir políticas diferenciadas para redes internas distintas.
c) Capacidade de definir políticas diferenciadas para os utilizadores fora da rede e com VPN desligada.
d) Capacidade de bloqueio de pedidos maliciosos, de domínio e respostas de IP ao nível do DNS.
e) Por forma a bloquear malware que tente a ligação IP direta (sem recorrer ao pedido de DNS) a solução deve ter a capacidade de bloqueio caminhos de URL (URL Paths) & conexões diretas na camada IP.
f) Capacidade de funcionamento sem recorrer a mecanismos de proxy.

g) Capacidade de funcionar como proxy para domínios que apresentem risco(domínios com conteúdo legitimo e malicioso) para realização de inspeção ao nível do URL e ficheiros, através de motores de antivírus e anti-malware com capacidade retrospetiva.

6.4.Funcionalidades de visibilidade:

a) Visualização das atividades através de relatórios agendados e em modo real-time de forma a poder ver instantaneamente ou quase, as atividades realizadas.
b) Capacidade de comparação entre atividade local e atividade global por forma a ajudar a identificar ataques direcionados “Target Attacks”
c) Capacidade de Identificação de riscos associados com o uso de ambientes de Cloud e IoT.
d) Visibilidade sobre as aplicações cloud utilizadas(Shadow IT)
e) Visibilidade granular sobre os pedidos de qualquer IP, utilizadores ou máquina.

6.5.Funcionalidades de gestão:

a) Suporte para listas de bloqueio e permissão (Black & white lists) customizáveis;
b) Integração com Active Directory para controlo e visibilidade;
c) Definição de políticas baseadas em grupos de utilizadores;
d) Possibilidade de testar/simular a aplicação de politicas antes destas serem aplicadas.
e) Capacidade de reter logs
f) Capacidade de integração com Amazon S3 para retenção de logs
g) Relatório avançados.

6.6.Funcionalidades de autenticação:

a) Capacidade de Integração com o Active Directory, através de software adicional;
b) Suporte para single sign-on (SSO), através de SAML (Security Assertion Markup Language).

6.7.Integração com soluções de terceiros:

1. A solução deve disponibilizar um API para integração com terceiros.
2. As integrações com API devem ter a capacidade de utilizar e gerir listas de bloqueio de terceiros (3rd-party block lists)

3. Integrações já pré-definidas para as seguintes soluções/fabricantes:

3.1. FireEye, Check Point, ZeroFox, ThreatConnect, ThreatQuotient, Cisco AMP Threat Grid.

6.8.Funcionalidades de investigação:

1. A solução deve conter uma consola de investigação que simplifique a resposta a incidentes. Esta consola deve dar acesso à informação que a solução dispõe sobre domínios, IPs, ASNs, hashes de ficheiros e à forma como estes se relacionam entre si.
2. Para qualquer domínio deve ser possivel visualizar informação global sobre:
   2.1. Histórico de DNS queries
   2.2. WHOIS records
   2.3. Name Servers
   2.4. Hashes de ficheiros maliciosos associados a este domínio
   2.5. Classificação do domínio
   2.6. TTLs
   2.7. Distribuição geográfica dos pedidos
   2.8. Classificação DGA
   2.9. IPs associados
   2.10. Co-occurrances
3. API de investigação com possibilidade de enriquecimento dos eventos da plataforma de SIEM.
4. Utilizar expressões RegEx para pesquisa de domínios.

7.Segurança de Dispositivo

Pretende-se adquirir uma ferramenta de monitorização e deteção de ameaças, vulnerabilidades e malware para ser utilizada na nossa infraestrutura para um total de 50 endpoints e/ou servidores.

A solução a instalar tem de analisar e monitorizar continuamente a atividade dos ficheiros, processos e comunicações nos servidores e endpoints de forma a poder encontrar qualquer atividade suspeita.

Esta solução deve ter como base uma rede de inteligência global que possua informação sobre os mais recentes ataques e malwares.



Deve também oferecer total visibilidade e controlo para rapidamente detetar, conter e remediar ameaças/malware que possam existir na rede e não tenham sido detetadas pelas soluções atualmente existentes. Nestes casos, deve ser possível identificar:

a) Como o malware entrou
b) Que sistemas foram afetados
c) O que é que o malware fez e o que está a fazer
d) O problema e a origem dele

7.1 A solução deve oferecer ainda as seguintes funcionalidades:

1. Reputação de ficheiros
   1.1. A solução deve utilizar mecanismos tradicionais para verificar a reputação de um ficheiro como por exemplo 1to1 signatures. Deve também utilizar mecanismos baseados em inteligência artificial e ser capaz de identificar malware que usa polimorfismo.
2. Motor Antivirus
   2.1. A solução deve conter um motor Antivirus de forma a permitir ter um único agente para Antivirus e funcionalidades avançadas de deteção, proteção e investigação forense.
3. Outbreak Control
   3.1. A solução deve permitir definir listas para:
      3.1.1. Bloqueio de aplicações
         3.1.1.1. Deve ser possível para além de fazer quarentena a uma aplicação, simplesmente bloqueá-la para impedir a sua execução.
         3.1.1.2. Deve ser possível definir aplicações a ser bloqueadas para ambientes Android
      3.1.2. Whitelist de aplicações
      3.1.3. Assinaturas customizadas
      3.1.4. Blacklist/Whitelist de IPs
4. Assinaturas customizadas
   4.1. A solução deve permitir ao administrador criar assinaturas para deteção de ficheiros. Os formatos suportados devem ser:
      4.1.1.1. MD5 signatures
      4.1.1.2. MD5, PE section-based signatures



4.1.1.3. File body-based signatures

4.1.1.4. Extended signature format (offsets, wildcards, regular expressions)

4.1.1.5. Logical signatures

4.1.1.6. Icon signatures

5. Análise estática e dinâmica de ficheiros
   5.1. A solução deve permitir fazer análise estática e dinâmica dos ficheiros recorrendo para isso a uma plataforma de sandbox. Nestes casos deve ser gerado um relatório que contenha indicações genéricas e detalhadas sobre a atividade do ficheiro analisado. Deve ainda ser possível visualizar através de um vídeo o comportamento do ficheiro na plataforma de sandboxing.
6. Deteção retrospetiva
   6.1. Deve ser possível receber alertas quando o veredito de um ficheiro muda (de clean ou desconhecido para malicioso). É essencial que a solução ofereça visibilidade sobre malware que evade as primeiras linhas de defesa ou malware que não é detetado durante a primeira análise ao ficheiro.
   6.2. A solução deve periodicamente verificar se um ficheiro clean ou unknown continua a ter o mesmo veredicto ou se esse veredito mudou.
7. Ligações externas
   7.1. A solução deve detetar conexões para o exterior que representem perigo (ex: Redes Command and Control)
8. Trajetória dos ficheiros na rede
   8.1. A solução deve monitorizar a atividade dos ficheiros dentro da rede, nomeadamente a forma como estes se propagam dentro da rede. No evento de um ficheiro ser classificado como malware depois de este ter entrado na rede, a solução deve permitir perceber como o ficheiro entrou na rede, como se propagou e que sistemas infetou a partir de um único dashboard. Deve ainda ser possível bloquear e colocar este tipo de ficheiros em quarentena com apenas alguns cliques, independentemente do número de endpoints infetados.
9. Trajetória dos ficheiros e processos dentro do dispositivo

9.1. A solução deve monitorizar toda a atividade de ficheiros, aplicações e processos dentro dos endpoints, de forma a permitir identificar qual foi a origem de um potencial malware. Deve existir um gráfico temporal onde seja possível verificar como os diferentes processos dentro dos endpoints interagem entre si.

10. Root Cause

10.1. A solução deve permitir identificar não apenas ficheiros maliciosos, mas também conseguir identificar qual foi a origem do problema. Exemplo: Se o Adobe Reader estiver comprometido e executar código malicioso, a solução proposta deve permitir identificar este comportamento e bloquear ou colocar em quarentena apenas a versão do Adobe que está comprometido em qualquer endpoint com o agente instalado.

11. Pesquisa

11.1. Deve ser possível pesquisar por um ficheiro/SHA ou por um IP de forma a perceber que sistemas possuem esse ficheiro ou que sistemas abriram alguma ligação para o IP pesquisado.

12. Submissão Automática de Ficheiros para sandbox

12.1. O sistema deve fazer tracking aos ficheiros executados na organização e automaticamente submeter ficheiros pouco comuns na organização para ser analisados num ambiente de sandboxing. Deve também ser possível enviar manualmente ficheiros para a plataforma de sandboxing.

12.2. A solução de sandboxing através de licenciamento adicional deve permitir ao administrador interagir diretamente com os ficheiros enquanto estes estão a ser analisados. Deve também dar acesso a um portal com o histórico de amostras analisadas pela organização.

12.3. O relatório de sandboxing deve gerar um relatório com as seguintes secções:

12.3.1. Metadata

12.3.2. Comportamento do ficheiro

12.3.3. Tráfico HTTP

12.3.4. Tráfico DNS

12.3.5. Streams TCP/IP

12.3.6. Processos executados



12.3.7. Artefactos observados

12.3.8. Actividade de Registry

12.3.9. Actividade no FileSystem

12.4. Deve ser possível fazer o download da sample analisada, visualizar um vídeo que mostre o comportamento do ficheiro analisado durante a sua execução e fazer download do PCAP e dos artefactos observados durante a execução do ficheiro.

13. Customização de Indicações de compromisso

13.1. O sistema deve suportar a criação e customização de indicações de compromisso nos endpoint, através da framework OpenIoC.

14. Vulnerabilidades

14.1. A solução deve identificar software presente nos endpoints que têm vulnerabilidades conhecidas (CVEs - Common Vulnerabilities and Exposures).

15. API

15.1. A solução deve ter uma API bi-direcional que permita a integração com sistemas de outros fabricantes

16. Visibilidade sobre argumentos passados por linha de comandos

16.1. O sistema deve garantir visibilidade sobre que argumentos que são passados por linha de comandos para lançar executáveis. Deve ser possível perceber se aplicações legítimas estão a ser usadas de forma maliciosa.

17. Integração com proxies

17.1. A solução deve poder ser integrada com diferentes fabricantes de proxy de forma a conseguir detetar máquinas comprometidas mesmo que estas não possuam um agente instalado.

18. Integração com NGFW e NGIPS

18.1. A solução deve pelo menos poder ser integrada com as soluções de NGFW e NGIPS do próprio fabricante de forma a ser possível correlacionar informação automaticamente para conseguir ter informação sobre máquinas comprometidas num único dashboard centralizado.

19. Arquitectura

19.1. A solução de endpoint deve fazer parte de uma arquitectura completa que inclua soluções de: endpoint, proxy, rede e email.

20. Relatórios
    20.1. A solução deve gerar automaticamente relatórios semanais com a seguinte informação:
        20.1.1. Conectores ativos
        20.1.2. Computadores potencialmente infetados
        20.1.3. Ficheiros maliciosos detetados
        20.1.4. Computadores que se tentaram ligar a IPs maliciosos fora da organização
        20.1.5. Ficheiros colocados em quarentena
        20.1.6. Aplicações bloqueadas
        20.1.7. Eventos retrospectivos – Falsos Positivos
        20.1.8. Indicações de Comprometimento
21. Heat Map
    21.1. Deve ser possível agrupar os endpoints em grupos e visualizar num heat map que grupos contêm endpoints infetados.

22. Deve ser possível a integração com uma consola de gestão central que permite a integração com: firewalls, email e web security, endpoint security, analítica de rede, autenticação forte, solução de network access control e segurança aplicacional. Deve ainda permitir:
    22.1. Orquestração e automação: deve integrar com as diversas soluções mencionadas e simplificar as operações de segurança permitindo criar e gerir workflows de resposta a incidentes
    22.2. Investigação e resposta a incidente: endereçar indicadores de compromisso (IoC) e efectuar investigações de segurança, disponibilizando informação de fontes de inteligência, analisar o risco e o impacto destes IoCs no contexto dos endpoints e com outros indicadores. Uma vez que a investigação se materialize em incidente de segurança, deverá ser possível desenvolver workflows automáticos e processos de remediação, tais como: bloquear IPs maliciosos, domínios, URL e ficheiros.
    22.3. Disponibilizar dashboards das ferramentas com que integra

22.4. Disponibilizar single sign-on.

8. Serviços Profissionais

Os serviços profissionais são todos os necessários e adequados à integral implementação e execução do objeto do contrato, devendo ser cumprido um conjunto de boas práticas que garantam o sucesso da implementação das tarefas planeadas dentro dos prazos estipulados. Devido ao nível de criticidade da solução, devem estar previstos pelo menos 20% dos trabalhos planeados fora de horas, garantindo o mínimo de disrupção possível na infraestrutura de produção.

Constituem ações críticas as seguintes:

Etapa Transversal

Gestão de Projeto ao longo de todo o projeto

Reunião de kickoff

Planeamento da solução a instalar/configurar

Gestão de projeto

Formação on-job

Acompanhamento entrada em produção (1 Semana)

Etapa Redes

Reunião de Kick-off

Instalação dos equipamentos em Bastidor

Instalação dos Access Points em locais a designar

Configuração de equipamentos ativos

Criação de redes (Vlans, SSDI)

Configuração de Captive Portal

Optimizações

Passagem à operação

Etapa Colaboração

Elaboração de Documento com Funcionalidades e Configurações

Mapeamento de funcionalidades e Configurações To-Be (SBC)

Elaboração de Documento com "Scope of Work" (SOW) de Funcionalidades e Configurações (To-Be) do SBC

Aprovação Documento com Funcionalidades e Configurações (To-Be) Cliente Final

Implementação Session Border Controller (SBC) & Gateway Analógicas

Instalação física de SBC

Confguração lógica de Connectividade ao SIP Provider Telco

Configuração lógica de Direct Routing com MS Teams Phone System

Testes Unitários e "Fine Tunning" - Conectividade SBC - SIP Provider

Testes Unitários e "Fine Tunning" - Conectividade SBC - MS Teams Phone System

Testes Globais e de Interoperabilidade (SIP Provider, SBC, MSTeams Phone System)

Implementação Microsoft Teams Phone System

Configuração de MS Teams - Genericas

Configuração de MS Teams Phone System

Mapeamento Utilizadores vs MS Active Directory

Testes Unitários e "Fine Tunning"

Testes Globais e de Interoperabilidade (SIP Provider, SBC, MSTeams Phone System)

Etapa Segurança

Instalação do router/firewall

Configuração do solução router/firewall

Configuração da solução de segurança de DNS

Configuração da Solução de segurança de dispositivo

Optimizações

Passagem à operação

Etapa Documentação

Elaboração de documentos técnicos de projeto (Descrição Técnica; Diagramas de rede; LLD; Plano de Testes)

O projeto deve ser implementado num prazo máximo de 1 mês após a chegada dos equipamentos.

9.Serviços de Manutenção e Suporte

9.1.Os serviços de manutenção e suporte pretendidos iniciam-se no dia seguinte ao da assinatura do CONTRATO mantendo-se em vigor pelo período de vigência do CONTRATO, e incluem as seguintes características mínimas:

a) Serviço em 24x7x365dias (4h de tempo de reposição).
b) Service Desk, para contactos através dos seguintes métodos:
    a. Web;
    b. E-mail;
    c. Telefone.
c) Suporte de fabricante, para escalonamento de incidentes e resolução através de troca de equipamento ou disponibilização de versão com bug fixing.
d) Suporte remoto ou local.
e) Serem disponibilizadas os acessos às últimas versões de software das soluções a serem suportadas.
f) Visita de manutenção preventiva, para verificação do estado das soluções e elaboração de relatório do ciclo de vida da solução.

9.2.Níveis de Serviço

Os serviços objeto do presente procedimento deverão ser prestados numa base de 24x7 onsite, devendo ainda ser cumpridos os tempos de resposta nos termos que seguidamente se descrevem:

As falhas serão classificadas de acordo com os seguintes níveis de prioridade:

NÍVEIS DE SERVIÇO	24x7x365 dias
Tempo de Resposta – Remoto/Local	
Prioridade 1 (*Severa*)	15 Min(remoto) / 4H (local)
Prioridade 2 (*Alta*)	1H(remoto) / 8H (local)
Prioridade 3 (*Normal*)	2H (remoto) / Dia útil seguinte (local)
Prioridade 4 (*baixa*)	4H (remoto) / Não se aplicável (local)

Os pedidos são categorizados de acordo com o nível de severidade:

- Prioridade 1 (Severa) – Equipamentos com avaria, provocando falha grave nas aplicações, ou serviço em baixo, não estando disponíveis backups ou redundâncias e causando um impacto crítico na atividade, se o serviço não for rapidamente reposto.
- Prioridade 2 (Alta) – Equipamentos com avaria, as aplicações estão seriamente degradadas, causando um impacto significativo na atividade.
- Prioridade 3 (Normal) - A performance da rede ou aplicações estão degradadas, a sua funcionalidade encontra-se afetada, embora sem impacto significativo na atividade.
- Prioridade 4 (Baixa) – Pedidos de informação e esclarecimento de dúvidas.

O suporte deverá ficar ativo desde a data da instalação dos equipamentos até ao termo da vigência do CONTRATO.

9.3 Requisitos da equipa técnica

De forma a assegurar que a equipa técnica está qualificada para os trabalhos a executar, a mesma deverá corresponder aos seguintes requisitos mínimos, sob pena de exclusão:

- Pelo menos 5 elementos com certificação Cisco Certified Network Expert (CCIE) – Com certificados válidos na data de adjudicação
- Pelo menos 3 elementos com certificação Cisco Certified Network Professional Security (CCNP Security)
- Pelo menos 1 elemento com certificação Cisco Customer Success Manager
- Pelo menos 1 elemento com a certificação PMP (gestor de projeto)

O prazo máximo de entrega relativo ao presente lote é de vinte semanas, sendo excluídas as propostas que apresentem prazo superior.