CONVITE AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO EM VIGOR NA SPMS PARA A AQUISIÇÃO DE SERVIÇOS DE CIBERSEGURANÇA

Ref.ª

CONVITE

DECRETO-LEI N.º 18/2008, DE 29 DE JANEIRO

(ARTIGO 241.º-B CONVITE À APRESENTAÇÃO DE PROPOSTA)

ÍNDICE

CAPÍTULO I DISPOSIÇÕES GERAIS 4

ARTIGO 1.º OBJETO DO PROCEDIMENTO 4
ARTIGO 2.º PROCEDIMENTO DE AQUISIÇÃO 4
ARTIGO 3.º ÓRGÃO QUE TOMOU A DECISÃO DE CONTRATAR 4

CAPÍTULO II DO PROCEDIMENTO E APRESENTAÇÃO DE PROPOSTAS 5

ARTIGO 4.º JÚRI 5
ARTIGO 5.º PREÇO BASE 5
ARTIGO 6.º DISPONIBILIZAÇÃO DO PROCEDIMENTO 5
ARTIGO 7.º ESCLARECIMENTOS E ERROS E OMISSÕES 5
ARTIGO 8.º DOCUMENTOS QUE CONSTITUEM A PROPOSTA 6
ARTIGO 9.º PRAZO E MODO DE APRESENTAÇÃO DA PROPOSTA 8
ARTIGO 10.º PRAZO DE MANUTENÇÃO DA PROPOSTA 8
ARTIGO 11.º ESCLARECIMENTOS SOBRE A PROPOSTA 9
ARTIGO 12.º EXCLUSÃO DAS PROPOSTAS 9
ARTIGO 13.º LEILÃO ELETRÓNICO 9
ARTIGO 14.º CRITÉRIO DE ADJUDICAÇÃO 9
ARTIGO 15.º PREÇO 10
ARTIGO 16.º CONDIÇÕES DE PAGAMENTO 10
ARTIGO 17.º PENALIDADES CONTRATUAIS 11
ARTIGO 18.º LOCAL E PRAZO DE ENTREGA 11
ARTIGO 19.º OBRIGAÇÕES DO ADJUDICATÁRIO 11
ARTIGO 20º OBRIGAÇÕES DA ENTIDADE ADJUDICANTE 12
ARTIGO 21º PRAZO DE VIGÊNCIA 13

CAPÍTULO III DO RELATÓRIO PRELIMINAR E ADJUDICAÇÃO 14

ARTIGO 22º RELATÓRIO PRELIMINAR 14
ARTIGO 23º AUDIÊNCIA PRÉVIA 14
ARTIGO 24º RELATÓRIO FINAL 14
ARTIGO 25º DECISÃO E NOTIFICAÇÃO DE ADJUDICAÇÃO 14
ARTIGO 26º DOCUMENTOS DE HABILITAÇÃO 15
ARTIGO 27º MINUTA DO CONTRATO 15
ARTIGO 28º RECLAMAÇÕES CONTRA A MINUTA DO CONTRATO 16
ARTIGO 29º OUTORGA DO CONTRATO 16
ARTIGO 30º GESTOR DO CONTRATO 16

CAPÍTULO IV DISPOSIÇÕES FINAIS 17

ARTIGO 31º LEGISLAÇÃO E FORO COMPETENTE 17

ANEXO I REQUISITOS MÍNIMOS 18

ANEXO II MODELO DE DECLARAÇÃO 36

ANEXO III MODELO DE DECLARAÇÃO 38

Capítulo I

Disposições gerais

Artigo 1.º

Objeto do procedimento

1. O objeto do presente procedimento consiste na **aquisição de Serviços de Cibersegurança, ao abrigo do(s) lote (s) ___ do Sistema de Aquisição Dinâmico (SAD) em vigor na Serviços Partilhados do Ministério da Saúde (SPMS, E.P.E.),** prosseguindo os trâmites previstos no artigo 241-B.º do Código dos Contratos Públicos (doravante CCP), e aplicando-se-lhe, com as necessárias adaptações, em tudo o que não estiver especialmente regulado, as disposições do Caderno de Encargos do Procedimento para a "Instituição de um Sistema de Aquisição Dinâmico para a Prestação de Serviços de Cibersegurança".
2. As especificações técnicas dos serviços encontram-se identificadas no **Anexo I** ao presente convite.

Artigo 2.º

Procedimento de aquisição

O presente convite é efetuado ao abrigo do(s) lote(s) _____ do Sistema de Aquisição Dinâmico para a **Aquisição de Serviços de Cibersegurança** nos termos do disposto na alínea a) do n.º 1 artigo 261.ºdo CCP.

Artigo 3.º

Órgão que tomou a decisão de contratar

Para os efeitos previstos no CCP apenas para a fase de formação do contrato, a decisão de contratar foi adotada pelo Conselho de Administração da _____. (identificação da entidade adjudicante) / da Serviços Partilhados do Ministério da Saúde, EPE. (SPMS), agindo em representação da entidade adjudicante do procedimento pré-contratual, ao abrigo de contrato de mandato administrativo. (caso seja a SPMS a desenvolver o procedimento em nome de outra(S) entidade(s))

Capítulo II

Do procedimento e apresentação de propostas

Capítulo III

Artigo 4.º

Júri

Nos termos e para os efeitos previsto no artigo 67.º do CCP, o procedimento é conduzido por um júri, designado pelo órgão competente para a decisão de contratar.

Artigo 5.º

Preço base

1. O preço base do presente procedimento é de **XXXXX,XX €** (), a que acresce IVA à taxa legal em vigor, e fixado por lote, de acordo com os seguintes montantes:
   - **Lote X** – (Designação) **XXXX,XX €** (), acrescido de IVA à taxa legal em vigor;
   - **Lote X** – (Designação) **XXXX,XX €** (), acrescido de IVA à taxa legal em vigor;
2. O preço base constante no número anterior corresponde ao preço máximo que a entidade adjudicante se dispõe a pagar pela prestação de todos os serviços que constituem o objeto do contrato a celebrar.

Artigo 6.º

Disponibilização do procedimento

O presente procedimento é integralmente disponibilizado na Plataforma Eletrónica de contratação pública, acessível através do sítio eletrónico www.comprasnasaude.pt.

Artigo 7.º

Esclarecimentos e erros e omissões

1. Os esclarecimentos necessários à boa compreensão e interpretação das peças do procedimento são da competência dos serviços da entidade adjudicante, designado pelo órgão que tomou a decisão de contratar.
2. Os esclarecimentos mencionados no número anterior devem ser solicitados por escrito, até ao termo do primeiro terço do prazo fixado para a apresentação das propostas, através da plataforma eletrónica de contratação www.comprasnasaude.pt .

3. Os esclarecimentos serão prestados, por escrito, até ao dia anterior do termo do prazo fixado para a apresentação da proposta, através da plataforma eletrónica de contratação www.comprasnasaude.pt.
4. O órgão competente para a decisão de contratar pode proceder à retificação de erros ou omissões das peças do procedimento nos termos e no prazo previstos no número anterior.
5. Os esclarecimentos e as retificações referidos nos números anteriores serão disponibilizados na plataforma eletrónica de contratação e juntos às peças do procedimento que se encontrem patentes para consulta.
6. Os esclarecimentos e as retificações referidos nos n.ºs 2 a 4 fazem parte integrante das peças do procedimento a que dizem respeito e prevalecem sobre estas em caso de divergência.
7. Quando as retificações ou esclarecimentos sejam comunicados para além do prazo estabelecido para o efeito, o prazo fixado para a apresentação das propostas deve ser prorrogado, no mínimo, por período equivalente ao do atraso verificado.
8. Quando as retificações referidas, independentemente do momento da sua comunicação, ou a aceitação de erros ou de omissões das peças do procedimento, implicarem alterações de aspetos fundamentais das peças do procedimento, o prazo fixado para a apresentação da proposta deve ser prorrogado, no mínimo, por período equivalente ao tempo decorrido desde o início daquele prazo até à comunicação das retificações ou à publicitação da decisão de aceitação de erros ou de omissões.
9. As decisões de prorrogação nos termos do disposto nos números anteriores cabem ao órgão competente para a decisão de contratar e devem ser juntas às peças do procedimento.

Artigo 8.º

Documentos que constituem a proposta

1. A proposta deve ser instruída no mínimo pelos seguintes documentos:
    a) Declaração de aceitação do conteúdo do caderno de encargos, elaborada em conformidade com o modelo constante do Anexo I do CCP (*template* em **Anexo II** ao presente convite);
    b) Modelo de resposta, devendo o mesmo indicar os seguintes elementos:
        i. O preço da proposta em euros e com apenas 2 casas decimais.
        ii. Acréscimo de IVA à taxa legal em vigor aos preços apresentados.
        iii. Gestor do contrato do operador económico;

c) Certidão Permanente por forma a atestar os representantes que têm poderes para obrigar a empresa;

d) Documento descritivo dos serviços a prestar;

e) Curriculum Vitae do(s) perfi(s) a contratar e documentação comprovativa dos requisitos enunciados no n.º 2 das cláusulas 1ª a 14ª do anexo I ao presente Convite.

2. Os documentos previstos nos números anteriores devem ser redigidos em língua portuguesa, sem prejuízo da possibilidade de apresentação de outros documentos em língua estrangeira, desde que acompanhados de respetiva tradução legalmente certificada, prevalecendo esta última para todos os efeitos em caso de contradição com o original. Apenas podem ser apresentados documentos em língua inglesa os documentos que em função da sua especificidade técnica sejam redigidos originariamente nessa língua.

3. A(s) entidade(s) adjudicante(s) pode(m), ainda, solicitar aos concorrentes a indicação nas suas propostas de quaisquer informações relativas às especificações e requisitos dos serviços propostos, nomeadamente as seguintes certificações respeitantes aos serviços a contratar e de acordo com a tipologia de serviços pretendida, conforme:

	I	II	III	IV	V	VI
Categoria 1: Projetos de conformidade e segurança de informação, análise dos riscos e continuidade de negócio	X	X	X	X		
Categoria 2: Projetos de deteção de incidentes de cibersegurança	X	X	X	X	X	X
Categoria 3: Projetos de resposta e recuperação a incidentes de cibersegurança	X	X	X	X	X	X
Categoria 4: Análise forense e auditorias técnicas de segurança	X	X	X	X	X	X
Categoria 5: Projetos de arquiteturas de redes e comunicações seguras	X	X	X	X		
Categoria 6: Projetos de segurança no desenvolvimento de software	X	X	X	X		
Categoria 7: Projetos de gestão e controlo identidades e acessos	X	X	X	X		

I - Certificação no Selo de Maturidade Digital - Cibersegurança

II - Certificação sobre a gestão da segurança da informação, ISO/IEC 27001 ou equivalente

III - Certificação com o Quadro Nacional de Referência para a Cibersegurança (EC QNRCS);

IV - Credenciação de Segurança (CRESO)

V - Comprovativo de membro da Rede Nacional de CSIRT, ou outra rede CSIRT similar;

VI - Certificação de serviços de Cibersegurança (CNCS)

4. Podem também integrar a proposta quaisquer outros documentos que o concorrente considere indispensáveis para explicitar os termos da proposta.

5. A apresentação dos documentos constitutivos da proposta obedece, nomeadamente, ao disposto nos n.ºs 4 e 5 do artigo 57.º do CCP e na Lei n.º 96/2015, de 17 de agosto.

Artigo 9.º

Prazo e modo de apresentação da proposta

1. Os documentos que constituem a proposta devem ser apresentados em suporte eletrónico, nos termos e modelos definidos no procedimento criado na plataforma eletrónica www.comprasnasaude.pt.
2. Cada um dos documentos que constituem as propostas deve ser assinado eletronicamente mediante a utilização de certificados de assinatura eletrónica qualificada, nos termos da Lei n.º 96/2015, de 17 de agosto.
3. Nos documentos eletrónicos com ficheiros compactados em formato "ZIP" ou equivalente, a aposição de uma assinatura eletrónica qualificada deve ocorrer em cada um dos documentos eletrónicos que os constituem, sob pena de exclusão da proposta nos termos da alínea l) do n.º 2 do artigo 146.º *ex vi* do n.º 2 do artigo 122.º ambos do CCP.
4. Nos casos em que o certificado digital não possa relacionar o assinante com a sua função e poder de assinatura, o concorrente deve submeter na plataforma eletrónica um documento indicando o poder de representação (nomeadamente certidão permanente onde conste os poderes para representar ou procuração).
5. A proposta deverá ser enviada através da referida plataforma, nos termos do n.º 1 do art.º 62.º do CCP, até às **18H00 do 10.º dia** contados desde a remessa do presente convite, nos termos do previsto na alínea b) do artigo 87.º do CPA, aplicável ex vi dos ns.º 1 e 3 do artigo 470.º do CCP.
6. Quando o termo do prazo para apresentação de propostas coincida com dia em que o serviço esteja encerrado (sábado, domingo ou feriado), transfere-se para o primeiro dia útil seguinte, nos termos da alínea f) do artigo 87.º do CPA.
7. O prazo referido no número 5 pode, a pedido da entidade convidada, e em casos devidamente fundamentados, ser prorrogado por prazo considerado necessário, nas condições previstas no artigo 64.º do CCP.

Artigo 10.º

Prazo de manutenção da proposta

Os concorrentes ficam obrigados a manter as suas propostas pelo prazo fixado no artigo 65.º do CCP.

Artigo 11.º

Esclarecimentos sobre a proposta

1. O Júri do procedimento pode pedir aos concorrentes quaisquer esclarecimentos sobre as propostas apresentadas que considere necessários para efeito da análise e da avaliação das mesmas.
2. Os esclarecimentos prestados pelos respetivos concorrentes fazem parte integrante das mesmas, desde que não contrariem os elementos constantes dos documentos que as constituem, não alterem ou completem os respetivos atributos, nem visem suprir omissões que determinam a sua exclusão.
3. Os esclarecimentos referidos no número anterior serão disponibilizados na plataforma eletrónica www.comprasnasaude.pt, sendo todos os concorrentes imediatamente notificados desse facto.

Artigo 12.º

Exclusão das propostas

1. São excluídas as propostas cuja análise revele alguma das situações previstas no n.º 2 do artigo 146º, designadamente:
    a) Que não sejam constituídas por todos os documentos exigidos nos termos do disposto no artigo 8º do presente convite.
    b) Que não respeitem o modo de apresentação dos documentos, nos termos do artigo 9º do presente convite.
2. Só são avaliadas as propostas que não forem excluídas.

Artigo 13.º

Leilão eletrónico

Não haverá lugar a leilão eletrónico.

Artigo 14.º

Critério de adjudicação

1. As entidades adjudicantes estabelecem nos convites desenvolvidos ao abrigo do presente Sistema de Aquisição Dinâmico, que a adjudicação é feita de acordo com o critério da proposta economicamente mais vantajosa nas modalidades:

a) Multifator, de acordo com a qual o critério de adjudicação é densificado por um conjunto de fatores, e eventuais subfatores, correspondentes a diversos aspetos da execução do contrato a celebrar; ou
b) Monofator, de acordo com a qual o critério de adjudicação é densificado por um fator correspondente a um único aspeto da execução do contrato a celebrar, designadamente o preço.

2. O preço dos serviços propostos deve incluir os seguintes parâmetros, sempre que aplicável:
   a) Despesas de alojamento;
   b) Despesas de alimentação;
   c) Despesas de deslocação de meios humanos;
   d) Taxas, impostos e encargos;
   e) Outros custos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante.

Artigo 15.º

Preço

1. A formação dos preços tem subjacente os preços unitários, os quais devem ser indicados com duas casas decimais, em algarismos e por extenso.
2. Aos preços apresentados pelos concorrentes acresce IVA à taxa legal em vigor.
3. O preço dos serviços é o que resultar do disposto neste convite e da proposta adjudicada.

Artigo 16.º

Condições de pagamento

1. As entidades adjudicantes são exclusivamente responsáveis pelo pagamento do preço dos serviços que lhe sejam prestados, não podendo, em caso algum, o adjudicatário emitir faturas à SPMS, EPE, na qualidade da entidade que celebrou o Sistema de Aquisição Dinâmico objeto do presente procedimento.
2. O preço a apresentar às entidades adjudicantes é o que resultar do disposto neste caderno de encargos e da proposta adjudicada no procedimento celebrado ao abrigo do Sistema de Aquisição Dinâmico.
3. O prazo de pagamento é o que for praticado por cada entidade adjudicante, nos termos da lei.

4. O atraso no pagamento confere ao adjudicatário o direito aos juros de mora calculados nos termos da lei.
5. Não podem ser realizados quaisquer pagamentos no âmbito da aquisição sem que se mostrem pagos os emolumentos devidos por fiscalização prévia do contrato respetivo por parte do Tribunal de Contas.

Artigo 17.º

Penalidades Contratuais

A entidade adjudicante deve definir quais as penalidades contratuais a aplicar, em virtude dos níveis de serviço determinados ou termos e condições estabelecidos. Na falta de definição de penalidades contratuais, pode, a entidade considerar a cláusula *48º - Sanções Contratuais* que consta do caderno de encargos do SAD, para sua aplicação.

Artigo 18.º

Local e Prazo para a Prestação dos Serviços

1. Os serviços a prestar no âmbito do Sistema de Aquisição Dinâmico são prestados em local a indicar pelas entidades adjudicantes.
2. O prazo de início para a execução dos serviços deverá ser acordado entre a entidade adjudicante e o adjudicatário, se o convite nada referir.
3. Pode a entidade adjudicante, se assim o entender, estabelecer cronogramas para a execução dos serviços.
4. Sempre que ocorra um caso de força maior, devidamente comprovado e que implique a suspensão da entrega, devem os adjudicatários, logo que dele tenham conhecimento, requerer à entidade adjudicante que lhes seja concedida uma prorrogação adequadamente fundamentada do respetivo prazo.

Artigo 19.º

Obrigações do Adjudicatário

Para além das previstas no CCP, constituem obrigações do(s) Adjudicatário(s):

a) Disponibilização dos serviços, no prazo definido pela entidade adjudicante, nos termos da cláusula 35.ª do Caderno de Encargos do Sistema de Aquisição Dinâmico, ou na proposta adjudicada, o qual, pode ser prorrogado, mediante acordo entre as partes;

b) Executar o contrato, em perfeita conformidade com as condições estabelecidas nos documentos contratuais, podendo a entidade adjudicante exercer, por si ou através de consultores especializados, a fiscalização e acompanhamento da execução do contrato;
c) Prestar de forma correta e fidedigna as informações referentes às condições em que são prestados os serviços, bem como prestar todos os esclarecimentos que se justifiquem, de acordo com as circunstâncias;
d) Recorrer a todos os meios humanos, materiais e tecnológicos que sejam necessários e adequados à prestação do contrato, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo;
e) Informar a entidade adjudicante sobre as alterações verificadas durante a execução do contrato;
f) Comunicar à entidade adjudicante, com uma antecedência mínima de 30 (trinta) dias, os factos que tornem total ou parcialmente impossível a prestação dos serviços definidos no caderno de encargos do SAD e demais documentos contratuais;
g) Elaborar, no final da execução do contrato, um relatório final, com informação detalhada sobre as situações ocorridas e os prazos assumidos para a resolução/indemnização dos mesmos;
h) Manter a validade de todas as autorizações legalmente exigidas para o exercício da sua atividade;
i) São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização de marcas registadas, patentes registadas ou licenças.
j) Respeitar os termos e condições dos acordos celebrados com o Estado que se encontrem em vigor;
k) Respeitar e prestar o serviço no estrito cumprimento da Legislação Geral de Cibersegurança em Portugal e na EU, designadamente a Lei n.º 46/2018 (Regime Jurídico da Segurança do Ciberespaço) e o Decreto-Lei n.º 65/2021, que regulamentam a Diretiva NIS e o Cybersecurity Act em Portugal;

Artigo 20º

Obrigações da entidade Adjudicante

1. Constituem obrigações das entidades adjudicantes, no âmbito e nos limites fixados:
   a) Reportar toda a informação relevante ao fiel e pontual cumprimentos dos contratos celebrados ao abrigo do Sistema de Aquisição Dinâmico até 10 (dez) dias úteis após a adjudicação e quando solicitado pela SPMS, EPE;

b) Efetuar os procedimentos aquisitivos segundo as regras definidas no Sistema de Aquisição Dinâmico;
c) Utilizar a plataforma eletrónica de contratação www.comprasnasaude.pt para a tramitação do procedimento pré-contratual;
d) Colocar em todas as Notas de Encomenda, e em qualquer título executório do contrato, a respetiva referência e identificação do instrumento especial de contratação a que a mesma diz respeito;
e) Nomear um gestor responsável pela gestão do(s) contrato(s) a celebrar ao abrigo do Sistema de Aquisição Dinâmico, bem como comunicar quaisquer alterações a essa nomeação aos Candidatos com quem tenham celebrado contrato;
f) Monitorizar o cumprimento contratual no que respeita às respetivas condições e aplicar as devidas sanções em caso de incumprimento;
g) Reportar os resultados da monitorização referida na alínea anterior e comunicar, no prazo de 5 (cinco) dias úteis à SPMS, EPE, os aspetos relevantes que tenham impacto no cumprimento do Sistema de Aquisição Dinâmico ou dos contratos celebrados ao seu abrigo.
h) No final da vigência de cada contrato celebrado ao abrigo do Sistema de Aquisição Dinâmico, deve a entidade adjudicante, através do gestor do contrato, proceder a avaliação do adjudicatário.

2. A informação referida na alínea a) do número anterior deve ser enviada através de relatórios de contratação, elaborados em conformidade com o modelo a disponibilizar pela SPMS, EPE.

Artigo 21º

Prazo de vigência

O contrato a celebrar entra em vigor no dia __ de _____ de 202_ ou no dia seguinte ao da sua assinatura, consoante o que ocorra posteriormente, e vigora até ___ de _____ de 202_, sem prejuízo das obrigações acessórias que tenham sido estabelecidas a favor da entidade adjudicante, incluindo as de confidencialidade e garantia.

Capítulo IV

Do Relatório Preliminar e Adjudicação

Artigo 22º

Relatório preliminar

1. Após a análise das propostas, o Júri elabora fundamentadamente o relatório preliminar, no qual deve propor a ordenação das mesmas, com base no critério de adjudicação indicado no presente convite.
2. No relatório preliminar a que se refere o número anterior, deve o júri também propor, fundamentadamente, a exclusão das propostas ao abrigo do n.º 2 do artigo 146.º *ex vi* do n.º 2 do artigo 122.º ambos do CCP.
3. Do relatório preliminar deve ainda constar referência aos esclarecimentos prestados pelos concorrentes nos termos do artigo 72º do CCP.

Artigo 23º

Audiência prévia

O relatório preliminar será notificado a todos os concorrentes para que, querendo, no prazo de 3 (três) dias úteis, se pronunciarem por escrito, ao abrigo do direito de audiência prévia.

Artigo 24º

Relatório final

Cumprido o disposto no artigo anterior, o júri elaborará um relatório final fundamentado, no qual analisa as observações dos concorrentes efetuadas ao abrigo do direito de audiência prévia, podendo manter o teor e as conclusões do relatório preliminar e ainda propor a exclusão de qualquer proposta se verificar, nesta fase, a ocorrência de qualquer dos motivos previstos no n.º 2 do artigo 146.º *ex vi* do n.º2 do artigo 122.º ambos do CCP.

Artigo 25º

Decisão e notificação de adjudicação

1. A decisão de adjudicação é notificada a todos os concorrentes.
2. De acordo com o artigo 77.º do CCP, juntamente com a notificação da decisão de adjudicação, o órgão competente para a decisão de contratar deve notificar o adjudicatário para:
   a) Apresentar todos os documentos de habilitação. de acordo com o artigo 77.º do CCP;

b) Prestar caução, se aplicável.

c) Confirmar, no prazo que lhe for determinado, se for o caso, os compromissos assumidos por terceiras entidades relativos aos atributos ou a termos e condições da proposta adjudicada.

Artigo 26º

Documentos de habilitação

1. O adjudicatário deve, no prazo de 3 (três) dias úteis a contar da notificação da adjudicação, entregar:

   a) Declaração referida na alínea a) do n.º 1 do artigo 81.º do CCP, emitida conforme modelo constante do **Anexo III** ao presente convite e do qual faz parte integrante;
   b) Certidão Permanente da empresa com indicação dos órgãos que vinculam a empresa;
   c) Certidão comprovativa da regularização da situação tributária;
   d) Certidão comprovativa da situação contributiva da Segurança Social;
   e) Certificados dos registos criminais do adjudicatário e tratando-se de pessoa coletiva dos titulares dos órgãos de administração, direção ou gerência;
   f) Registo Central do Beneficiário Efetivo.

2. Nos termos previstos nos nº 5 e 6 da Portaria nº 372/2017, de 14 de dezembro, está dispensada a entrega dos documentos previstos no n.º 1 do presente artigo, desde que os mesmos se encontrem disponíveis no Catálogo de Compras Públicas da Saúde, através do link www.catalogo.min-saude.pt, devidamente válidos à data da sua apresentação, preenchendo com esta indicação o n.º 2 da Declaração constante no Anexo II ao CCP.
3. A adjudicação caduca caso o adjudicatário não apresente os documentos de habilitação, nos termos indicados no número 1, bem como sejam apresentados documentos falsos, prestadas falsas declarações, ou não seja prestada a caução no prazo e termos exigidos.

Artigo 27º

Minuta do contrato

1. O contrato será reduzido a escrito de acordo com o preceituado na alínea a) do n.º 1 do artigo 95.º do CCP, sendo composto pelo respetivo cláusula do contratual e os seus anexos.
2. A minuta de contrato é enviada ao adjudicatário, para aceitação, juntamente com a notificação de adjudicação.

Artigo 28º

Reclamações contra a minuta do contrato

1. As reclamações contra a minuta do contrato só podem ter por fundamento a previsão de obrigações que contrariem ou não constem dos documentos que integram o contrato ou ainda a recusa dos ajustamentos propostos.
2. No prazo de 10 (dez) dias a contar da apresentação da reclamação, a entidade adjudicante comunica ao reclamante a sua decisão.
3. Decorrido o prazo fixado no número anterior sem que a entidade adjudicante se pronuncie sobre a reclamação apresentada, considera-se que a mesma foi indeferida.

Artigo 29º

Outorga do contrato

1. Os contratos devem ser celebrados no prazo de 30 (trinta) dias contados da data da aceitação da minuta ou da decisão sobre a reclamação, mas nunca antes de:
   a) Apresentados todos os documentos de habilitação exigidos;
   b) Confirmados os compromissos assumidos por terceiras entidades, se for o caso;
   c) Comprovação da prestação da caução (quando aplicável).
2. A entidade adjudicante comunica ao adjudicatário, com a antecedência mínima de 5 (cinco) dias, a data, a hora e local da outorga do Contrato, salvo se estabelecida a outorga via assinatura digital.

Artigo 30º

Gestor do contrato

1. Nos termos do art.º 290-A do CCP, a entidade adjudicante, designará um gestor do contrato, com a função de acompanhar permanentemente a execução deste.
2. O contrato que resultar do presente procedimento reveste-se de especiais características de complexidade técnica pelo que, sem prejuízo das funções que sejam definidas pela entidade adjudicante, o gestor elaborará indicadores de execução quantitativos e qualitativos adequados ao tipo de contrato, que permitam, entre outros aspetos, medir os níveis de desempenho do adjudicatário na execução do contrato.
3. Caso o gestor detete desvios, defeitos ou outras anomalias na execução do contrato, deve comunicá-los de imediato ao órgão competente, propondo em relatório fundamentado as medidas corretivas que, em cada caso, se revelem adequadas.

4. Ao gestor do contrato podem ser delegados poderes para a adoção das medidas a que se refere o número anterior, exceto em matéria de modificação e cessação do contrato.

Capítulo V

Disposições finais

Artigo 31º

Legislação e foro competente

1. A tudo o que não esteja especialmente previsto no presente convite aplica-se:
   a) O Caderno de Encargos do SAD para Aquisição de Serviços de Cibersegurança.
   b) O previsto no CCP e demais legislação aplicável.
2. Para resolução de todos os litígios decorrentes do contrato aplica-se o previsto no Código de Processo nos Tribunais Administrativos.

Anexos:

Anexo I – Especificações Técnicas do Serviço

Anexo II – Anexo I do CCP

Anexo III – Anexo II do CCP

ANEXO I

REQUISITOS MÍNIMOS

Cláusula 1.ª

Gestor de projeto / serviço

1. O perfil de gestor de projeto/serviço, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Gestão de projetos de tecnologias de informação, segurança da informação ou cibersegurança;
   b) Planeamento, organização e gestão de projetos apoiando na definição de âmbito, planeamento, recursos necessários e riscos;
   c) Acompanhar a evolução de projetos, identificando desvios e propondo soluções;
   d) Produção de documentação;
   e) Reportar o status do projeto às partes interessadas;
   f) Identificação oportunidades de melhoria.
2. Os concorrentes obrigam-se no âmbito do presente convite a assegurar que o perfil de Gestor de projeto/serviço cumpre as os seguintes requisitos obrigatórios:
   a) Licenciatura ou grau académico superior em Gestão de Sistemas de Informação, Sistemas e Tecnologias de Informação ou similares, ou formação de técnico profissional nas mesmas áreas;
   b) Experiência comprovada em gestão de projeto ≥ 3 anos;
   c) Inglês Intermédio/avançado (mínimo B2);
   d) Conhecimentos avançados em ferramentas de gestão de projeto, por exemplo, Microsoft Project e PowerBI.
3. Os concorrentes devem ainda procurar que o perfil de Gestor de projeto/serviço apresente os seguintes requisitos recomendados:
   a) Certificação em gestão de projetos segundo os referenciais PM2, IPMA ou PMI;
   b) Experiência comprovada em projetos de segurança de informação e cibersegurança ≥ 3 anos.
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 2.ª

Gestor de projeto / serviço - Sénior

1. O perfil de Gestor de projeto/serviço - Sénior, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Gestão de projetos de tecnologias de informação, segurança da informação ou cibersegurança;
   b) Planeamento, organização e gestão de projetos apoiando na definição de âmbito, planeamento, recursos necessários e riscos;
   c) Acompanhar a evolução de projetos, identificando desvios e propondo soluções;
   d) Produção de documentação;
   e) Reportar o status do projeto às partes interessadas;
   f) Identificação oportunidades de melhoria.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Gestor de projeto/serviço - Sénior cumpre as os seguintes requisitos obrigatórios:
   a) Licenciatura ou grau académico superior em Gestão de Sistemas de Informação, Sistemas e Tecnologias de Informação ou similares, ou formação de técnico profissional nas mesmas áreas;
   b) Experiência comprovada em gestão de projeto ≥ 5 anos;
   c) Inglês Intermédio/avançado (mínimo B2);
   d) Conhecimentos avançados em ferramentas de gestão de projeto, por exemplo, Microsoft Project;
   e) Certificação em gestão de projetos segundo os referenciais PM2, IPMA ou PMI;
3. Os concorrentes devem ainda procurar que o perfil de Gestor de projeto/serviço apresente os seguintes requisitos recomendados
   a) Experiência comprovada em projetos de segurança de informação e cibersegurança ≥ 5 anos.
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 3.ª

Analista de cibersegurança

1. O perfil de Analista de cibersegurança, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
    a) Monitorizar os sistemas e as infraestruturas de segurança;
    b) Manter as operações de cibersegurança;
    c) Tratar e responder de incidentes de cibersegurança;
    d) Apoiar a organização na definição de padrões e políticas para a cibersegurança;
    e) Desenvolver documentação de segurança.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Analista de cibersegurança cumpre as os seguintes requisitos obrigatórios:
    a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas
    b) Experiência profissional comprovada na área das TIC ≥ 2 anos;
    c) Experiência profissional enquanto analista de cibersegurança;
    d) Experiência comprovada nas seguintes funções:
        i. Execução de atividades TIER 1 do SOC: triagem e classificação de alertas, eventos e incidentes;
        ii. Análise e resposta a incidentes.
        iii. Análise de malware;
        iv. Recolha e tratamento de IOCs;
        v. Criação de planos de resposta para contenção/mitigação de incidentes de segurança.
3. Os concorrentes devem ainda procurar que o perfil de Analista de cibersegurança apresente os seguintes requisitos recomendados:
    a) Certified Information Systems Security Professional (CISSP);
    b) CompTIA Security+, Network+, CySA;
    c) GIAC Security Essentials (GSEC);
    d) CCNA Cyber Ops.
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 4.ª

Analista de cibersegurança - Sénior

1. O perfil de Analista de cibersegurança - Sénior, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
    a) Monitorizar os sistemas e as infraestruturas de segurança;
    b) Manter as operações de cibersegurança;
    c) Tratar e responder aos incidentes de cibersegurança;
    d) Apoiar a organização na definição de padrões e políticas para a cibersegurança;
    e) Desenvolver documentação de segurança.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Analista de cibersegurança - Sénior cumpre as os seguintes requisitos obrigatórios:
    a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
    b) Experiência comprovada na área das TIC ≥ 5 anos;
    c) Experiência profissional como SOC/CSIRT Analyst ou Incident Responder≥ 3 anos;
    d) Experiência comprovada nas seguintes funções:
        i. Execução de atividades TIER 2 do SOC: análise e resposta a incidentes complexos;
        ii. Criação de planos de resposta para contenção/mitigação de incidentes de segurança;
        iii. Análise de malware;
        iv. Disponibilização de informação acionável na proteção de sistemas e dados contra ameaças cibernéticas;
        v. Análise de dados e identificação de padrões e tendências que possam indicar potenciais ameaças ou vulnerabilidades;
        vi. Recolha e tratamento de IOCs;
        vii. Verificação do estado de operacionalidade das ferramentas de proteção e de segurança;
        viii. Configuração e manutenção das fontes de dados para sistema de monitorização e análise.
3. Os concorrentes devem ainda procurar que o perfil de Analista de cibersegurança - Sénior apresente os seguintes requisitos recomendados:
    a) Certified Information Systems Security Professional (CISSP);

b) CompTIA Security+, Network+, CySA;
c) GIAC Security Essentials (GSEC);
d) CCNA Cyber Ops.

4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 5.ª

Engenheiro de cibersegurança de redes e infraestrutura

1. O perfil de Engenheiro de cibersegurança de redes e infraestruturas, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Definir requisitos de arquitetura de segurança da organização;
   b) Traduzir os requisitos da arquitetura de segurança em soluções de segurança;
   c) Desenvolver ou supervisionar a implementação dos requisitos da arquitetura de segurança;
   d) Gerir a qualidade e a melhoria contínua da arquitetura de segurança;
   e) Implementar soluções de segurança incluindo redes e infraestruturas seguras, soluções de proteção de ativos e de monitorização de segurança;
   f) Rever arquiteturas de segurança de soluções de TI e prestar consultoria no desenho de alternativas para controlos de segurança e proteção;
   g) Desenvolvimento de diretrizes e normas técnicas de segurança de redes e infraestrutura;
   h) Apoio a projetos internos que integrem tecnologias emergentes e subsequente análise de ameaças de cibersegurança no contexto tecnológico.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Engenheiro de cibersegurança de redes e infraestruturas cumpre as os seguintes requisitos obrigatórios:
   a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas
   b) Experiência profissional comprovada na área das TIC ≥ 2 anos;
   c) Experiência profissional enquanto engenheiro / analista de cibersegurança de redes e infraestrutura;
   d) Experiência comprovada nas seguintes funções:
      i. Desenho de arquiteturas de rede seguras e controlos de segurança;

ii. Implementação e operação de qualquer uma das seguintes soluções de segurança: NGFW, SASE, VPN, Proxy/Web filter, NAC, ADC, etc.;

iii. Operação de ferramentas de segurança de perímetro de rede, deteção/prevenção de intrusões, modelagem de segurança de aplicativos e integridade de sistemas;

iv. Fornecimento de assessoria em segurança técnica, recomendações e consultoria em redes e infraestrutura.

3. Os concorrentes devem ainda procurar que o perfil de Engenheiro de cibersegurança de redes e infraestruturas apresente os seguintes requisitos recomendados:
   a) Certified Information Systems Security Professional (CISSP);
   b) CompTIA Security+;
   c) CISCO CCNA, CCNP Security, CCIE Security;
   d) Certificações Cloud Security (AWS, Azzure ou equivalente);
   e) Certificação CCNA Cyber Ops, CompTIA Security+, Network+ ou CySA;
   f) Conhecimentos em frameworks de arquitetura empresarial como CRISP, TOGAF, COBIT, ISO.
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 6.ª

Engenheiro de cibersegurança de redes e infraestrutura - Sénior

1. O perfil de Engenheiro de cibersegurança de redes e infraestruturas - Sénior, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Definir requisitos de arquitetura de segurança da organização;
   b) Traduzir os requisitos da arquitetura de segurança em soluções de segurança;
   c) Desenvolver ou supervisionar a implementação dos requisitos da arquitetura de segurança;
   d) Gerir a qualidade e a melhoria contínua da arquitetura de segurança;
   e) Implementar soluções de segurança incluindo redes e infraestruturas seguras, soluções de proteção de ativos e de monitorização de segurança;
   f) Rever arquiteturas de segurança de soluções de TI e prestar consultoria no desenho de alternativas para controlos de segurança e proteção;
   g) Desenvolvimento de diretrizes e normas técnicas de segurança de redes e infraestrutura;

h) Apoio a projetos internos que integrem tecnologias emergentes e subsequente análise de ameaças de cibersegurança no contexto tecnológico.

2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Engenheiro de cibersegurança de redes e infraestruturas - Sénior cumpre as os seguintes requisitos obrigatórios:
    a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
    b) Experiência comprovada na área das TIC ≥ 5 anos;
    c) Experiência profissional em projetos de cibersegurança de redes e infraestrutura ≥ 3 anos;
    d) Experiência comprovada nas seguintes funções:
        i. Desenho de arquiteturas de rede seguras e controlos de segurança;
        ii. Implementação e operação de qualquer uma das seguintes soluções de segurança: NGFW, SASE, VPN, Proxy/Web filter, NAC, ADC, etc.;
        iii. Operação de ferramentas de segurança de perímetro de rede, deteção/prevenção de intrusões, modelagem de segurança de aplicativos e integridade de sistemas;
        iv. Fornecimento de assessoria em segurança técnica, recomendações e consultoria em redes e infraestrutura.
3. Os concorrentes devem ainda procurar que o perfil de Engenheiro de cibersegurança de redes e infraestruturas - Sénior apresente os seguintes requisitos recomendados:
    a) Certified Information Systems Security Professional (CISSP);
    b) CompTIA Security+;
    c) CISCO CCNA, CCNP Security, CCIE Security;
    d) Certificações Cloud Security (AWS, Azzure, ou equivalente);
    e) Certificação CCNA Cyber Ops, CompTIA Security+, Network+ ou CySA.;
    f) Conhecimentos em frameworks de arquitetura empresarial como CRISP, TOGAF, COBIT, ISO.
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 7.ª

Engenheiro de cibersegurança aplicacional

1. O perfil de Engenheiro de cibersegurança aplicacional, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
    a) Definir requisitos numa abordagem devsecops da organização;
    b) Desenvolver ou supervisionar a implementação dos requisitos da segurança aplicacionais;
    c) Implementar controlos de segurança em sistemas de informação;
    d) Gerir sistemas de segurança de desenvolvimento;
    e) Desenho e integração de soluções e abordagens de segurança no processo de desenvolvimento de sistemas;
    f) Apoio à definição de projetos de arquitetura de soluções e stack tecnológica;
    g) Analisar e rever arquitetura de dados, sistemas, integrações e implementação de API;
    h) Desenvolvimento de diretrizes e normas técnicas de segurança aplicacional;
    i) Apoio a projetos internos que integrem tecnologias emergentes e subsequente análise de ameaças de cibersegurança no contexto tecnológico.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Engenheiro de cibersegurança aplicacional cumpre as os seguintes requisitos obrigatórios:
    a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
    b) Experiência profissional comprovada na área das TIC ≥ 2 anos;
    c) Experiência profissional enquanto engenheiro / analista de cibersegurança aplicacional;
    d) Experiência comprovada nas seguintes funções:
        i. Desenho e implementação de arquiteturas de sistemas e controlos de segurança;
        ii. Implementação de standards; protocolos de segurança; encriptação e mecanismos de autenticação;
        iii. Linguagem/estrutura de desenvolvimento ou scrips (p.e. PowerShell, Python, .Net);
        iv. Desenvolvimento seguro;
        v. Apoio na aplicação e conformidade com controlos de segurança em sistemas de informação;
        vi. Fornecimento de assessoria em segurança técnica, recomendações e consultoria em produtos e serviços.

3. Os concorrentes devem ainda procurar que o perfil de Engenheiro de cibersegurança aplicacional apresente os seguintes requisitos recomendados:
    a) Experiência prévia como programador ≥ 2 anos;
    b) Certified Information Systems Security Professional (CISSP);
    c) CompTIA Security+, Server+;
    d) EC-Council CND;
    e) CISCO CCNA, CCNP Enterprise, CCIE Security ou equivalente;
    f) Certificações Cloud Security (AWS, Azzure, ou equivalentes);
    g) Certificação CCNA Cyber Ops, CompTIA Security+, Network+ ou CySA.
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 8.ª

Engenheiro de cibersegurança aplicacional - Sénior

1. O perfil de Engenheiro de cibersegurança aplicacional - Sénior, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:

    Definir requisitos numa abordagem devsecops da organização;
    a) Desenvolver ou supervisionar a implementação dos requisitos da segurança aplicacionais;
    b) Implementar controlos de segurança em sistemas de informação;
    c) Gerir sistemas de segurança de desenvolvimento;
    d) Desenho e integração de soluções e abordagens de segurança no processo de desenvolvimento de sistemas;
    e) Apoio à definição de projetos de arquitetura de soluções e stack tecnológica;
    f) Analisar e rever arquitetura de dados, sistemas, integrações e implementação de API;
    g) Desenvolvimento de diretrizes e normas técnicas de segurança aplicacional;
    h) Apoio a projetos internos que integrem tecnologias emergentes e subsequente análise de ameaças de cibersegurança no contexto tecnológico.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Engenheiro de cibersegurança aplicacional - Sénior cumpre as os seguintes requisitos obrigatórios:
    a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;

b) Experiência comprovada na área das TIC ≥ 5 anos;
c) Experiência profissional em projetos de devsecops ≥ 3 anos;
d) Experiência comprovada nas seguintes funções:
   i. Desenho e implementação de arquiteturas de sistemas e controlos de segurança;
   ii. Implementação de standards; protocolos de segurança; encriptação e mecanismos de autenticação;
   iii. Linguagem/estrutura de desenvolvimento ou scrips (p.e. PowerShell, Python, .Net);
   iv. Desenvolvimento seguro;
   v. Configuração e manutenção de sistemas de devsecops;
   vi. Apoio na aplicação e conformidade com controlos de segurança em sistemas de informação;
   vii. Fornecimento de assessoria em segurança técnica, recomendações e consultoria em produtos e serviços.

3. Os concorrentes devem ainda procurar que o perfil de Engenheiro de cibersegurança aplicacional - Sénior apresente os seguintes requisitos recomendados:
   a) Experiência prévia como programador ≥ 5 anos
   b) Certified Information Systems Security Professional (CISSP);
   c) CompTIA Security+, Server+;
   d) EC-Council CND;
   e) CISCO CCNA, CCNP Enterprise, CCIE Security ou equivalente;
   f) Certificações Cloud Security (AWS, Azzure ou equivalentes);
   g) Certificação CCNA Cyber Ops, CompTIA Security+, Network+ ou CySA.
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 9.ª

Pentester

1. O perfil de Pentester, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Planear, coordenar e conduzir atividades de simulação de ameaças de cibersegurança;
   b) Fornecer recomendações técnicas para a mitigação de vulnerabilidades e minimização do risco;

c) Criar casos de teste através de análise técnica aprofundada de riscos e vulnerabilidades típicas;
d) Executar testes de intrusão para identificar inconsistências e falta de robustez;
e) Analisar e interpretar os relatórios de ameaças e de cyber threat intelligence.

2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Pentester cumpre as os seguintes requisitos obrigatórios:
   a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
   b) Experiência profissional comprovada na área das TIC ≥ 2 anos;
   c) Experiência profissional enquanto pentester;
   d) Experiência em métodos de ataque, métodos de teste de penetração manual e ferramentas de hacking – Nmap Metasploit, Linux Kali, Burp Suite Pro.Experiência comprovada nas seguintes funções:
      i. Execução de testes de intrusão em sistemas, infraestruturas e atividades de Red Team;
      ii. Realização de investigações técnicas de cibersegurança em ativos;
      iii. Análise técnica de riscos e vulnerabilidades;
      iv. Fornecimento de assessoria em segurança técnica, recomendações e consultoria em redes, infraestrutura, produtos e serviços.
3. Os concorrentes devem ainda procurar que o perfil de Pentester apresente os seguintes requisitos recomendados:
   a) Certified in Risk and Information Systems Control (CRISC);
   b) CompTIA Network+, Security+, Linux+, Pentest+;
   c) EC-Council CEH;
   d) OSCP;
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 10.ª

Pentester - Sénior

1. O perfil de Pentester - Sénior, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
    a) Planear, coordenar e conduzir atividades de simulação de ameaças de cibersegurança;
    b) Fornecer recomendações técnicas para a mitigação de vulnerabilidades e minimização do risco;
    c) Criar casos de teste através de análise técnica aprofundada de riscos e vulnerabilidades típicas;
    d) Executar testes de intrusão para identificar inconsistências e falta de robustez;
    e) Analisar e interpretar os relatórios de ameaças e de cyber threat intelligence.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Pentester - Sénior cumpre as os seguintes requisitos obrigatórios:
    a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
    b) Experiência comprovada na área das TIC ≥ 5 anos;
    c) Experiência profissional enquanto pentester ≥ 3 anos;
    d) Experiência em métodos de ataque, métodos de teste de penetração manual e ferramentas de hacking – Nmap Metasploit, Linux Kali, Burp Suite Pro.
    e) Experiência comprovada nas seguintes funções:
        i. Execução de testes de intrusão em sistemas, infraestruturas e atividades de Red Team;
        ii. Realização de investigações técnicas de cibersegurança em ativos;
        iii. Análise técnica de riscos e vulnerabilidades;
        iv. Fornecimento de assessoria em segurança técnica, recomendações e consultoria em redes, infraestrutura, produtos e serviços.
3. Os concorrentes devem ainda procurar que o perfil de Pentester - Sénior apresente os seguintes requisitos recomendados:
    a) Certified in Risk and Information Systems Control (CRISC);
    b) CompTIA Network+, Security+, Linux+, Pentest+;
    c) EC-Council CEH;
    d) OSCP;

4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 11.ª

Consultor de segurança da informação

1. O perfil de Consultor de segurança da informação, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Contribuir para a definição de políticas, normas e procedimentos de segurança da informação e cibersegurança;
   b) Produção de documentação no âmbito segurança da informação e cibersegurança;
   c) Realização de avaliações de risco em apoio a projetos de implementação de SI e TI;
   d) Apoiar a configuração da solução gestão de risco garantindo consistência com processos locais;
   e) Definir indicadores-chave de risco e desempenho (KRIs/KPIs) para avaliar o desempenho da gestão de riscos;
   f) Determinação dos controlos apropriados para mitigar os riscos;
   g) Apoiar a elaboração de planos de continuidade de negócio e plano de crise de cibersegurança;
   h) Desenvolver e apoiar a realização de ações de formação e sensibilização em segurança de informação e cibersegurança;
   i) Produção de relatórios de avaliação de risco em cibersegurança.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Consultor de segurança da informação cumpre as os seguintes requisitos obrigatórios:
   j) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
   k) Experiência profissional comprovada na área das TIC ≥ 3 anos;
   l) Experiência profissional em projetos de segurança de informação;
   m) Experiência comprovada nas seguintes funções:
      i. Produção de documentação de segurança da informação e risco, nomeadamente, definição de políticas, normas e procedimentos;

ii. Desenho, implementação e acompanhamento de processos de implementação de Sistema de Gestão de Segurança da Informação (SGSI);
iii. Determinação dos controlos apropriados para mitigar os riscos;
iv. Monitorização, acompanhamento e gestão das medidas de mitigação e exceções de modo a garantir o estabelecimento de padrões e políticas de segurança apropriados;
v. Elaboração de planos de continuidade de negócio e plano de crise de cibersegurança.

3. Os concorrentes devem ainda procurar que o perfil de Consultor de segurança da informação apresente os seguintes requisitos recomendados:
   a) Certificação Certified Informaton Systems Security Professional (CISSP) ou Certified Information security manager (CISM);
   b) Certificação Certified Information Systems Security Professional (CISSP);
   c) Certificação ISO 27001 Lead Implementer;
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 12.ª

Consultor de segurança da informação - Sénior

1. O perfil de Consultor de segurança da informação - Sénior, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Contribuir para a definição de políticas, normas e procedimentos de segurança da informação e cibersegurança;
   b) Produção de documentação no âmbito segurança da informação e cibersegurança;
   c) Realização de avaliações de risco em apoio a projetos de implementação de SI e TI;
   d) Apoiar a configuração da solução gestão de risco garantindo consistência com processos locais;
   e) Definir indicadores-chave de risco e desempenho (KRIs/KPIs) para avaliar o desempenho da gestão de riscos;
   f) Determinação dos controlos apropriados para mitigar os riscos;
   g) Apoiar a elaboração de planos de continuidade de negócio e plano de crise de cibersegurança;

h) Desenvolver e apoiar a realização de ações de formação e sensibilização em segurança de informação e cibersegurança;

i) Produção de relatórios de avaliação de risco em cibersegurança.

2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Consultor de segurança da informação - Sénior cumpre as os seguintes requisitos obrigatórios:
   a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
   b) Experiência comprovada na área das TIC ≥ 5 anos;
   c) Experiência profissional em projetos de segurança de informação ≥ 3 anos;
   d) Experiência comprovada nas seguintes funções:
      i. Produção de documentação de segurança da informação e risco, nomeadamente, definição de políticas, normas e procedimentos;
      ii. Desenho, implementação e acompanhamento de processos de implementação de Sistema de Gestão de Segurança da Informação (SGSI);
      iii. Determinação dos controlos apropriados para mitigar os riscos;
      iv. Monitorização, acompanhamento e gestão das medidas de mitigação e excepções de modo a garantir o estabelecimento de padrões e políticas de segurança apropriados;
      v. Elaboração de planos de continuidade de negócio e plano de crise de cibersegurança.
      vi. Implementação de processos de conformidade ou certificação de ISO27001 ou similares
3. Os concorrentes devem ainda procurar que o perfil de Consultor de segurança da informação - Sénior apresente os seguintes requisitos recomendados:
   a) Certificação Certified Informaton Systems Security Professional (CISSP) ou Certified Information security manager (CISM);
   b) Certificação Certified Information Systems Security Professional (CISSP);
   c) Certificação ISO 27001 Lead Implementer;
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 13.ª

Auditor de cibersegurança

1. O perfil de Auditor de cibersegurança, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
    a) Desenvolver o plano de auditoria;
    b) Executar o plano de auditoria e avaliações de conformidade de cibersegurança e segurança da informação;
    c) Examinar mudanças no contexto tecnológico, legislação, ativos e tecnologias de TI da organização de modo a identificar potenciais riscos de cibersegurança;
    d) Contribuir para a melhoria da gestão do risco;
    e) Produção de documentação no âmbito segurança da informação e cibersegurança;
    f) Realização de avaliações de risco em apoio a projetos de implementação de SI e TI;
    g) Identificação de recomendações para melhorar a conformidade e abordar os riscos identificados;
    h) Produção de relatórios de avaliação de risco em cibersegurança.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Auditor de cibersegurança cumpre as os seguintes requisitos obrigatórios:
    a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
    b) Experiência profissional comprovada na área das TIC ≥ 3 anos;
    c) Experiência profissional em auditorias de cibersegurança;
    d) Experiência comprovada nas seguintes funções:
        i. Condução de atividades de auditoria de conformidade de segurança da informação;
        ii. Produção de recomendações de melhoria da conformidade e abordagem dos riscos identificados;
        iii. Programas de conformidade com obrigações legais e regulamentares em matérias de cibersegurança e segurança da informação;
        iv. Processos de certificação ISO 27001, SOC2, HIPAA, PCI ou equivalente.
3. Os concorrentes devem ainda procurar que o perfil de Auditor de cibersegurança apresente os seguintes requisitos recomendados:
    a) Certified Information Systems Security Professional (CISSP);
    b) Certified Information Systems Auditor (CISA);

c) GIAC Systems and Network Auditor (GSNA);
d) GIAC Critical Controls Certification (GCCC);
e) CompTIA Security+;
f) ISO27001 Auditor, Foundations, Practitioner;
g) Certified Information Security Manager (CISM);
h) Certified in Risk and Information Systems Control (CRISC).

4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

Cláusula 14.ª

Auditor de cibersegurança - Sénior

1. O perfil de Auditor de cibersegurança - Sénior, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
   a) Desenvolver o plano de auditoria;
   b) Executar o plano de auditoria e avaliações de conformidade de cibersegurança e segurança da informação;
   c) Examinar mudanças no contexto tecnológico, legislação, ativos e tecnologias de TI da organização de modo a identificar potenciais riscos de cibersegurança;
   d) Contribuir para a melhoria da gestão do risco;
   e) Produção de documentação no âmbito segurança da informação e cibersegurança;
   f) Realização de avaliações de risco em apoio a projetos de implementação de SI e TI;
   g) Identificação de recomendações para melhorar a conformidade e abordar os riscos identificados;
   h) Produção de relatórios de avaliação de risco em cibersegurança.
2. Os concorrentes obrigam-se no âmbito dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico a assegurar que o perfil de Auditor de cibersegurança – Sénior cumpre as os seguintes requisitos obrigatórios:
   a) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
   b) Experiência comprovada na área das TIC ≥ 5 anos;
   c) Experiência profissional enquanto auditor de cibersegurança ≥ 3 anos;
   d) Experiência comprovada nas seguintes funções:

i. Condução de atividades de auditoria de conformidade de segurança da informação;
ii. Produção de recomendações de melhoria da conformidade e abordagem dos riscos identificados;
iii. Programas de conformidade com obrigações legais e regulamentares em matérias de cibersegurança e segurança da informação;
iv. Processos de certificação ISO 27001, SOC2, HIPAA, PCI ou equivalente.

3. Os concorrentes devem ainda procurar que o perfil de Auditor de cibersegurança – Sénior apresente os seguintes requisitos recomendados:
   a) Certified Information Systems Security Professional (CISSP);
   b) Certified Information Systems Auditor (CISA);
   c) GIAC Systems and Network Auditor (GSNA);
   d) GIAC Critical Controls Certification (GCCC);
   e) CompTIA Security+;
   f) ISO27001 Auditor, Foundations, Practitioner;
   g) Certified Information Security Manager (CISM);
   h) Certified in Risk and Information Systems Control (CRISC).
4. Os requisitos definidos são mínimos, pelo que no convite à apresentação de propostas ao abrigo do sistema de aquisição dinâmico devem ser confirmados requisitos técnicos iguais ou superiores, bem como devem ser completados os indicados e adicionados outros necessários.

ANEXO II

MODELO DE DECLARAÇÃO

[a que se refere a alínea a) do n.º 1 do Artigo 57.º do CCP]

1. ... (nome, número de documento de identificação e morada), na qualidade de representante legal de (1) ...(firma, número de identificação fiscal e sede ou, no caso de agrupamento concorrente, firmas, números de identificação fiscal e sedes), tendo tomado inteiro e perfeito conhecimento do caderno de encargos relativo à execução do contrato a celebrar na sequência do procedimento de ... (designação ou referência ao procedimento em causa) e, se for o caso, do caderno de encargos do acordo quadro aplicável ao procedimento, declara, sob compromisso de honra, que a sua representada (2) se obriga a executar o referido contrato em conformidade com o conteúdo do mencionado caderno de encargos, relativamente ao qual declara aceitar, sem reservas, todas as suas cláusulas.
2. Declara também que executa o referido contrato nos termos previstos nos seguintes documentos, que junta em anexo (3):
    a) ...
    b) ...
3. Declara ainda que renuncia a foro especial e se submete, em tudo o que respeitar à execução do referido contrato, ao disposto na legislação portuguesa aplicável.
4. Mais declara, sob compromisso de honra, que não se encontra em nenhuma das situações previstas no n.º 1 do artigo 55.º do Código dos Contratos Públicos.
5. O declarante tem pleno conhecimento de que a prestação de falsas declarações implica, consoante o caso, a exclusão da proposta apresentada ou a caducidade da adjudicação que eventualmente sobre ela recaia e constitui contra-ordenação muito grave, nos termos do Artigo 456.º do Código dos Contratos Públicos, a qual pode determinar a aplicação da sanção acessória de privação do direito de participar, como candidato, como concorrente ou como membro de agrupamento candidato ou concorrente, em qualquer procedimento adotado para a formação de contratos públicos, sem prejuízo da participação à entidade competente para efeitos de procedimento criminal.
6. Quando a entidade adjudicante o solicitar, o concorrente obriga -se, nos termos do disposto no Artigo 81.º do Código dos Contratos Públicos, a apresentar os documentos comprovativos

se que não se encontra nas situações previstas nas alíneas b), d), e) e h) do n.º 1 do artigo 55.º do referido Código.

7. O declarante tem ainda pleno conhecimento de que a não apresentação dos documentos solicitados nos termos do número anterior, por motivo que lhe seja imputável, determina a caducidade da adjudicação que eventualmente recaia sobre a proposta apresentada e constitui contraordenação muito grave, nos termos do Artigo 456.º do Código dos Contratos Públicos, a qual pode determinar a aplicação da sanção acessória de privação do direito de participar, como candidato, como concorrente ou como membro de agrupamento candidato ou concorrente, em qualquer procedimento adotado para a formação de contratos públicos, sem prejuízo da participação à entidade competente para efeitos de procedimento criminal.

... (local), ... (data), ... [assinatura (4)].

(1) Aplicável apenas a concorrentes que sejam pessoas coletivas.

(2) No caso de o concorrente ser uma pessoa singular, suprimir a expressão «a sua representada».

(3) Enumerar todos os documentos que constituem a proposta, para além desta declaração, nos termos do disposto nas alíneas b), c) e d) do n.º 1 e nos nºs 2 e 3 do Artigo 57.º

(4) Nos termos do disposto nos nºs 4 e 5 do artigo 57.º

ANEXO III

MODELO DE DECLARAÇÃO

[a que se refere a alínea a) do nº 1 do Artigo 81º do CCP]

1. ... (nome, número de documento de identificação e morada), na qualidade de representante legal de (1)... (firma, número de identificação fiscal e sede ou, no caso de agrupamento concorrente, firmas, números de identificação fiscal e sedes), adjudicatário(a) no procedimento de... (designação ou referência ao procedimento em causa), declara, sob compromisso de honra, que a sua representada (2) não se encontra em nenhuma das situações previstas no n.º 1 do artigo 55.º do Código dos Contratos Públicos:

2. O declarante junta em anexo [ou indica...como endereço do sítio da Internet onde podem ser consultados (3)] os documentos comprovativos de que a sua representada (4) não se encontra nas situações previstas nas alíneas b), d), e) e h) do n.º 1 do artigo 55.º do Código dos Contratos Públicos.

3. O declarante tem pleno conhecimento de que a prestação de falsas declarações implica a caducidade da adjudicação e constitui contraordenação muito grave, nos termos do artigo 456.º do Código dos Contratos Públicos, a qual pode determinar a aplicação da sanção acessória de privação do direito de participar, como candidato, como concorrente ou como membro de agrupamento candidato ou concorrente, em qualquer procedimento adotado para a formação de contratos públicos, sem prejuízo da participação à entidade competente para efeitos de procedimento criminal.

... (local), ... (data), ... [assinatura (5)].,

(1) Aplicável apenas a concorrentes que sejam pessoas coletivas.

(2) No caso de o concorrente ser uma pessoa singular, suprimir a expressão «a sua representada».

(3) Acrescentar as informações necessárias à consulta, se for o caso.

(4) No caso de o concorrente ser uma pessoa singular, suprimir a expressão «a sua representada».

(5) Nos termos do disposto nos nºs 4 e 5 do artigo 57.º