Aprovado em reunião
de CA de 04/06/2025

Sandra Cavaca

Assinado de forma digital por Sandra Cavaca
DN: c=PT, title=Presidente do Conselho de Administração, o=Serviços Partilhados do Ministério da Saúde EPE, sn=Cavaca, givenName=Sandra, cn=Sandra Cavaca
Dados: 2025.06.05 14:22:57 +01'00'

Assinado de forma digital por Luis Miguel dos Santos Ferreira
DN: c=PT, o=Cartão do Cidadão, ou=Chave Móvel Digital de Assinatura Qualificada do Cidadão, ou=Cidadão, ou=RemoteQSCDManagement, sn=dos Santos Ferreira, givenName=Luis Miguel, serialNumber=BI09620008, cn=Luis Miguel dos Santos Ferreira
Dados: 2025.06.05 17:59:43 +01'00'

Nuno Miguel Ramos da Costa

Assinado de forma digital por Nuno Miguel Ramos da Costa
Dados: 2025.06.14 13:57:02 +01'00'

INSTITUIÇÃO DE UM SISTEMA DE AQUISIÇÃO DINÂMICO PARA PRESTAÇÃO DE SERVIÇOS DE CIBERSEGURANÇA

REF.ª 1621/2025

CADERNO DE ENCARGOS

MAIO, 2025

Índice

CAPÍTULO I

PARTE I

DO SISTEMA DE AQUISIÇÃO DINÂMICO

SECÇÃO I

DISPOSIÇÕES GERAIS

CLÁUSULA 1.ª

DEFINIÇÕES

Para efeitos do presente caderno de encargos, entende-se por:

a) **Sistema de Aquisição Dinâmico (SAD)** – instrumento procedimental especial que possibilita à SPMS, E.P.E., enquanto central de compras da saúde, avaliar os candidatos de acordo com os requisitos de capacidade técnica e financeira definidos, com vista a disciplinar as relações contratuais futuras relativas à Prestação de Serviços de Cibersegurança, mediante a fixação antecipada dos respetivos termos, durante o período de vigência do SAD, de 4 (quatro) anos.

b) **SPMS, EPE** – Serviços Partilhados do Ministério da Saúde, Entidade Pública Empresarial, criada pelo Decreto-Lei n.º 19/2010, de 22 de março, alterado pelo Decreto-Lei n.º 108/2011, de 17 de novembro, pelo Decreto-Lei n.º 209/2015, de 25 de setembro, pelo Decreto-Lei n.º 32/2016, de 28 de junho, com o objeto e atribuições conforme definidos nos seus Estatutos, publicados em anexo ao referido diploma.

c) **Interessados** – Entidade, pessoa singular ou coletiva, de potencial participação na fase de qualificação;

d) **Candidatos** – Entidade, pessoa singular ou coletiva, que participa na fase de qualificação, mediante a apresentação de uma candidatura;

e) **Candidatos qualificados** – Entidade, pessoa singular ou coletiva, qualificada no Sistema de Aquisição Dinâmico;

f) **Concorrentes** – Entidade, pessoa singular ou coletiva, que participar em qualquer procedimento de formação de um contrato mediante a apresentação de uma proposta;

g) **Adjudicatários** – Entidade adjudicatária dos contratos celebrados ao abrigo do Sistema de Aquisição Dinâmico.

h) **Entidade Adjudicante** – Qualquer organismo do Ministério da Saúde e entidade do Serviço Nacional de Saúde que preste cuidados de saúde, ou qualquer outra com quem a SPMS já tenha celebrado ou venha a celebrar Protocolo de Adesão aos Acordos Quadro Transversais.

i) **Contratos** – Contratos a celebrar entre as entidades adjudicantes e os adjudicatários, nos termos do presente caderno de encargos.

j) **Gestor do Contrato** – Responsável pela gestão do Sistema de Aquisição Dinâmico e dos contratos celebrados ao abrigo do mesmo.

k) **Gestor de categoria** – Responsável pela gestão dos contratos celebrados ao abrigo do Sistema de Aquisição Dinâmico.

CLÁUSULA 2.ª

OBJETO

1. O presente procedimento tem por objeto a seleção de candidatos para a prestação de serviços de cibersegurança, ao abrigo do Sistema de Aquisição Dinâmico, e rege-se com as necessárias adaptações, pelo disposto nos artigos 162.º a 192.º do CCP.
2. O Sistema de Aquisição Dinâmico resultante do presente procedimento disciplinará as relações contratuais futuras a estabelecer entre os candidatos qualificados e qualquer outro organismo do Ministério da Saúde, entidade do Serviço Nacional de Saúde, bem como os organismos de Serviço de Saúde das Regiões Autónomas dos Açores e da Madeira.
3. A classificação CPV (Vocabulário Comum para os Contratos Públicos) é a seguinte: 72150000-1- Serviços de consultoria em matéria de auditoria informática e de hardware (CPV).

CLÁUSULA 3.ª

CONSTITUIÇÃO DOS LOTES DO SISTEMA DE AQUISIÇÃO DINÂMICO

1. O presente procedimento de Aquisição Dinâmico é composto por 7 categorias e 58 lotes, nos termos seguintes:

Categoria 1: Projetos de conformidade e segurança de informação, análise dos riscos e continuidade de negócio

i. Lote 1: Gestor de projeto / serviço
ii. Lote 2: Gestor de projeto / serviço- Sénior
iii. Lote 3: Consultor de segurança da informação
iv. Lote 4: Consultor de segurança da informação- Sénior
v. Lote 5: Auditor de cibersegurança
vi. Lote 6: Auditor de cibersegurança- Sénior
vii. Lote 7: Engenheiro de cibersegurança aplicacional
viii. Lote 8: Engenheiro de cibersegurança aplicacional – Sénior

Categoria 2: Projetos de deteção de incidentes de cibersegurança

i. Lote 9: Gestor de projeto / serviço
ii. Lote 10: Gestor de projeto / serviço – Sénior
iii. Lote 11: Analista de cibersegurança
iv. Lote 12: Analista de cibersegurança- Sénior
v. Lote 13: Engenheiro de cibersegurança de redes e infraestrutura
vi. Lote 14: Engenheiro de cibersegurança de redes e infraestrutura- Sénior
vii. Lote 15: Consultor de segurança da informação
viii. Lote 16: Consultor de segurança da informação- Sénior

Categoria 3: Projetos de resposta e recuperação a incidentes de cibersegurança

i. Lote 17: Gestor de projeto / serviço
ii. Lote 18: Gestor de projeto / serviço – Sénior
iii. Lote 19: Analista de cibersegurança
iv. Lote 20: Analista de cibersegurança- Sénior
v. Lote 21: Engenheiro de cibersegurança de redes e infraestrutura
vi. Lote 22: Engenheiro de cibersegurança de redes e infraestrutura- Sénior
vii. Lote 23: Engenheiro de cibersegurança aplicacional
viii. Lote 24: Engenheiro de cibersegurança aplicacional – Sénior
ix. Lote 25: Consultor de segurança da informação
x. Lote 26: Consultor de segurança da informação- Sénior
xi. Lote 27: Auditor de cibersegurança
xii. Lote 28: Auditor de cibersegurança- Sénior

Categoria 4: Análise forense e auditorias técnicas de segurança

i. Lote 29: Gestor de projeto / serviço
ii. Lote 30: Gestor de projeto / serviço- Sénior
iii. Lote 31: Pentester
iv. Lote 32: Pentester – Sénior
v. Lote 33: Auditor de cibersegurança
vi. Lote 34: Auditor de cibersegurança- Sénior

Categoria 5: Projetos de arquiteturas de redes e comunicações seguras

i. Lote 35: Gestor de projeto / serviço
ii. Lote 36: Gestor de projeto / serviço- Sénior
iii. Lote 37: Engenheiro de cibersegurança de redes e infraestrutura
iv. Lote 38: Engenheiro de cibersegurança de redes e infraestrutura- Sénior

v. Lote 39: Consultor de segurança da informação
vi. Lote 40: Consultor de segurança da informação- Sénior

Categoria 6: Projetos de segurança no desenvolvimento de software

i. Lote 41: Gestor de projeto / serviço
ii. Lote 42: Gestor de projeto / serviço- Sénior
iii. Lote 43: Engenheiro de cibersegurança aplicacional
iv. Lote 44: Engenheiro de cibersegurança aplicacional – Sénior
v. Lote 45: Pentester
vi. Lote 46: Pentester – Sénior
vii. Lote 47: Consultor de segurança da informação
viii. Lote 48: Consultor de segurança da informação- Sénior

Categoria 7: Projetos de gestão e controlo identidades e acessos

i. Lote 49: Gestor de projeto / serviço
ii. Lote 50: Gestor de projeto / serviço- Sénior
iii. Lote 51: Engenheiro de cibersegurança de redes e infraestrutura
iv. Lote 52: Engenheiro de cibersegurança de redes e infraestrutura- Sénior
v. Lote 53: Engenheiro de cibersegurança aplicacional
vi. Lote 54: Engenheiro de cibersegurança aplicacional – Sénior
vii. Lote 55: Consultor de segurança da informação
viii. Lote 56: Consultor de segurança da informação- Sénior
ix. Lote 57: Auditor Cibersegurança
x. Lote 58: Auditor Cibersegurança – Sénior

2. Os requisitos técnicos e os requisitos ambientais, encontram-se definidos no "**Anexo I – Especificações Técnicas**" e no "**Anexo III – Requisitos Técnicos**" do presente Caderno de Encargos.

3. Caso aplicável, relativamente às especificações/características técnicas fixadas neste caderno de encargos e/ou nos seus anexos, no cumprimento do previsto nos n.ºs 8 e 9 do artigo 49.º do Código dos Contratos Públicos (CCP), a referência, a título excecional, a quaisquer normas, a um fabricante ou uma proveniência determinada, a um processo específico de fabrico, a marcas, patentes ou modelos e a uma dada origem ou produção devem ser consideradas acompanhadas da menção «**ou equivalente**».

CLÁUSULA 4.ª

PRAZO DE VIGÊNCIA

1. Para efeitos da al. a) do n.º 1 do artigo 240.º do CCP, o sistema de aquisição dinâmico tem a duração de 2 (dois) anos, a contar da data da sua entrada em vigor, e considera-se automaticamente renovado por períodos de 1 (um) ano se a SPMS, EPE o denunciar, mediante notificação à outra parte por carta registada com aviso de receção, com a antecedência mínima de 60 (sessenta) dias em relação ao seu termo.
2. Após a renovação a que se refere o número anterior, o sistema de aquisição dinâmico pode ser revogado a qualquer momento, mediante acordo entre todas as partes, e desde que seja precedida de notificação por carta registada com aviso receção, com uma antecedência mínima de 90 (noventa) dias em relação à data do termo pretendida.
3. O prazo máximo de vigência do sistema de aquisição dinâmico, incluindo renovações, é de 4 (quatro) anos, a contar da data da sua entrada em vigor.

CLÁUSULA 5.ª

CONTRATO(S)

1. O(s) contrato(s) celebrado(s) ao abrigo do presente Sistema de Aquisição Dinâmico, são reduzidos a escrito e composto(s) pelo respetivo clausulado contratual, integra os seguintes elementos:
    a) Os suprimentos dos erros e das omissões das peças procedimentais identificados pelos concorrentes e expressamente aceites pelo órgão competente para a decisão de contratar, nos termos do disposto no artigo 50.º do Código dos Contratos Públicos (CCP) ou pelo órgão a quem esta competência tenha sido delegada;
    b) Os esclarecimentos e as retificações relativos às peças do procedimento;
    c) O presente Caderno de Encargos e seus anexos;
    d) A Proposta Adjudicada;
    e) Os esclarecimentos sobre a proposta adjudicada prestados pelo Adjudicatário.
2. Sem prejuízo do disposto no número seguinte, em caso de divergência entre os vários documentos que integram o contrato, a prevalência é determinada pela ordem por que vêm enunciados no número anterior.
3. Os ajustamentos propostos pela SPMS, EPE nos termos previstos no artigo 99.º do Código dos Contratos Públicos e aceites pelo Adjudicatário nos termos previstos no artigo 101.º do mesmo código prevalecem sobre todos os documentos referidos no n.º 1 da presente cláusula.

4. Além dos documentos indicados no n.º 1, o candidato obriga-se também a respeitar, no que lhe seja aplicável, as normas europeias e portuguesas, as especificações e homologações de organismos oficiais e fabricantes ou entidades detentoras de patentes.

SECÇÃO II

OBRIGAÇÕES DAS PARTES

CLÁUSULA 6.ª

OBRIGAÇÕES DOS CANDIDATOS ADMITIDOS

1. Para além das previstas no CCP, constituem obrigações dos candidatos qualificados:
    a) Prestar os serviços às entidades adjudicantes conforme as normas legais vigentes aplicáveis ao exercício da atividade, e nos termos e condições definidos no presente caderno de encargos;
    b) Comunicar à SPMS, EPE e às entidades adjudicantes, logo que deles tenham conhecimento, os factos que tornem total ou parcialmente impossível o cumprimento de qualquer das suas obrigações, designadamente:
        i. Impossibilidade temporária de prestação de serviços;
        ii. Impossibilidade legal de prestação de serviços;
        iii. Alteração da denominação e sede social, os seus representantes legais, a sua situação jurídica ou a sua situação comercial, bem como as alterações aos contactos e moradas indicados no contrato para a gestão do Sistema de Aquisição Dinâmico.
    c) Não alterar as condições do contrato a celebrar, fora dos casos previstos no caderno de encargos;
    d) Não ceder, sem prévia autorização da SPMS, EPE., a sua posição contratual no(s) contrato(s) a celebrar com as entidades adjudicantes;
    e) Prestar de forma correta e fidedigna as informações referentes às condições em que são prestados os serviços, bem como conceder todos os esclarecimentos que se justifiquem, de acordo com as circunstâncias;
    f) Comunicar à SPMS, EPE. qualquer facto que ocorra durante a execução do Sistema de Aquisição Dinâmico e dos contratos celebrados ao seu abrigo e que altere, designadamente, a sua denominação e sede social, os seus representantes legais, a sua situação jurídica ou a sua situação comercial, bem como as alterações aos contactos e moradas indicados no contrato para a gestão do Sistema de Aquisição Dinâmico;

g) Sempre que solicitado pela SPMS, EPE., disponibilizar declaração emitida por um Revisor Oficial de Contas ou pela entidade fiscalizadora das contas da empresa, na qual se certifiquem os valores comunicados nos relatórios de faturação entregues, relativos aos procedimentos realizados ao abrigo do Sistema de Aquisição Dinâmico;

h) Comunicar à SPMS, EPE e às entidades adjudicantes a nomeação do gestor do contrato responsável pela gestão do Sistema de Aquisição Dinâmico e do(s) contrato(s) a celebrar ao abrigo do mesmo, bem como quaisquer alterações relativamente à sua nomeação;

i) Disponibilizar a informação relevante para a gestão dos contratos à SPMS, EPE. e às entidades adjudicantes;

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;

l) Para efeitos de habilitação nos procedimentos de aquisição ao abrigo do Sistema de Aquisição Dinâmico, manter permanentemente atualizados os documentos de habilitação, bem como os documentos que atestem o poder de representação do candidato;

m) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenham no âmbito da formação e da execução do Sistema de Aquisição Dinâmico, e não utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos;

n) Proceder ao registo de faturas relativas aos processos de aquisição tramitados pela Central de Compras da Saúde, através da opção fornecida no site www.catalogo.min-saude.pt (registo de faturas);

o) Produzir relatórios de faturação no âmbito dos contratos celebrados ao abrigo do Sistema de Aquisição Dinâmico e enviar estes relatórios à SPMS, EPE., com uma periodicidade trimestral, designadamente para efeitos estatísticos, autorizando expressamente a SPMS, EPE. ao tratamento dos dados fornecidos;

p) Retificar os relatórios de faturação apresentados nos termos da alínea anterior, sempre que sejam detetadas irregularidades nos valores;

q) Envio trimestral dos elementos estatísticos (vendas) referentes às aquisições efetuadas pelas entidades adquirentes, devendo fazer referência ao código, marca, quantidade e valor global de vendas;

r) Os elementos estatísticos devem ser submetidos à SPMS impreterivelmente até ao dia 20 (vinte) do mês seguinte em relação ao trimestre de vigência do contrato, através da opção fornecida no site www.catalogo.min-saude.pt (registo de faturas).

CLÁUSULA 7.ª

OBRIGAÇÕES DAS ENTIDADES ADJUDICANTES NA GESTÃO DO SISTEMA DE AQUISIÇÃO DINÂMICO

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) 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;
   d) 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;
   e) Monitorizar o cumprimento contratual no que respeita às respetivas condições e aplicar as devidas sanções em caso de incumprimento;
   f) 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.
   g) 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.

CLÁUSULA 8.ª

OBRIGAÇÕES DA SPMS, E.P.E.

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente caderno de encargos e respetivos anexos, constituem obrigações da SPMS, EPE, as seguintes:

a) Fiscalizar o cumprimento do Sistema de Aquisição Dinâmico e dos contratos celebrados ao abrigo do mesmo, designadamente para apuramento do cumprimento das obrigações contratuais por parte dos candidatos e das entidades adjudicantes.

b) Monitorizar a qualidade da prestação de serviços, designadamente realizando auditorias e tratando a informação recebida ao abrigo do disposto nas cláusulas anteriores e, quando justificado, aplicar sanções em caso de incumprimento, incluindo a suspensão temporária ou a exclusão de algum candidato qualificado do Sistema de Aquisição Dinâmico, designadamente em caso de:

   i. Reiterado reporte de falta de qualidade e/ou de falhas inesperadas na utilização dos bens e serviços fornecidos por parte dos serviços utilizadores das entidades adjudicantes e/ou incumprimento reiterado dos prazos de entrega dos bens e da prestação dos serviços.

   ii. Deteção dos casos reiterados referidos na subalínea i) anterior, em ações de monitorização pela SPMS, EPE.

c) Promover a atualização do Sistema de Aquisição Dinâmico, mantendo o tipo de prestação e os objetos identificados no Sistema de Aquisição Dinâmico, conforme resulta da cláusula seguinte.

CLÁUSULA 9.ª

ATUALIZAÇÃO DO SISTEMA DE AQUISIÇÃO DINÂMICO

1. A SPMS, EPE. promoverá, mediante consulta aos candidatos qualificados e com uma periodicidade anual, a atualização das especificações técnicas dos serviços a adquirir ao abrigo deste instrumento de contratação especial, modificando-os ou substituindo-os por outros, nomeadamente por inovação tecnológica ou descontinuidade das especificações técnicas mínimas definidas no Sistema de Aquisição Dinâmico, desde que se mantenha o tipo de prestação e os seus objetivos.
2. A atualização deve respeitar o seguinte:
   a) As especificações devem respeitar a tipologia de serviço genericamente definido em relação a cada categoria e lote, não devendo alterar a essencialidade e os objetivos das especificações técnicas mínimas fixadas no sistema de Aquisição Dinâmico;
   b) Os serviços devem obedecer, no mínimo, aos requisitos e demais condições previstas no presente caderno de encargos;
   c) A atualização por inovação tecnológica não determina a eliminação no CAPS (Catálogo de Aprovisionamento Público da Saúde) da especificação técnica mínima anterior, exceto se se verificar a descontinuidade da mesma.

3. Cabe à SPMS, EPE proceder à aprovação e à publicação das atualizações previstas nos números anteriores.
4. A atualização não pode conduzir à modificação do objeto principal do Sistema de Aquisição Dinâmico nem configurar uma forma de impedir, restringir ou falsear a concorrência garantida na fase de formação do mesmo.

CLÁUSULA 10.ª

ACOMPANHAMENTO E FISCALIZAÇÃO DO MODO DE EXECUÇÃO DO CONTRATO

1. Nos termos e para os efeitos do disposto no artigo 290.º-A do Código dos Contratos Públicos:
    a) A gestão dos contratos decorrentes do presente procedimento e cuja celebração se reveste no Sistema de Aquisição Dinâmico, será efetuada pela Central de Compras da Saúde.
    b) É da responsabilidade das entidades adjudicantes como contraentes públicos designarem um gestor do contrato, com função de acompanhar permanentemente a execução dos contratos celebrados ao abrigo do presente Sistema de Aquisição Dinâmico.
    c) No exercício das suas funções, o gestor pode acompanhar, examinar e verificar, presencialmente, a execução do contrato pelo Adjudicatário.
    d) Caso o gestor do contrato detete desvios, defeitos ou outras anomalias na execução do contrato, determina ao Prestador de serviços que adote as medidas que, em cada caso, se revelem adequadas à correção dos mesmos.
    e) O desempenho das funções de acompanhamento e fiscalização do modo de execução do contrato não exime o prestador de serviços de responsabilidade por qualquer incumprimento ou cumprimento defeituoso das suas obrigações.

CLÁUSULA 11.ª

AUDITORIA

A qualquer momento a SPMS, EPE. e as entidades adjudicantes ou outras entidades mandatadas para o efeito, podem solicitar informação ou realizar auditorias com vista à monitorização da qualidade da execução dos contratos e o cumprimento das obrigações legais e, quando justificado, aplicar as devidas sanções.

SECÇÃO III

DAS RELAÇÕES ENTRE AS PARTES NO SISTEMA DE AQUISIÇÃO DINÂMICO

CLÁUSULA 12.ª

DADOS PESSOAIS

1. Os candidatos deverão apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas, que garantam a conformidade de quaisquer tratamentos de dados satisfaça os requisitos do RGPD – Regulamento (EU) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e assegure a defesa dos direitos do titular dos dados, nomeadamente, através da existência e do cumprimento de um código de conduta ou de procedimento de certificação aprovado conforme referido nos artigos 40.º e 42.º do RGPD.
2. Compete aos candidatos informar, imediatamente, a SPMS, EPE. e a entidade adjudicante se, no seu entender, alguma instrução violar o presente Caderno de Encargos ou o RGPD ou outras disposições legais nacionais ou europeias em matéria de proteção de dados.

CLÁUSULA 13.ª

SIGILO E CONFIDENCIALIDADE

1. As partes devem guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa aos destinatários, de que possa ter conhecimento ao abrigo ou em relação com a execução do presente contrato.
2. O dever de sigilo previsto no número anterior abrange, designadamente, documentos escritos, dados pessoais, desenhos, planos, aplicações e programas informáticos no formato de código fonte ou código objeto, especificações, segredos comerciais, métodos e fórmulas, contratos de financiamento e situações internas, de natureza laboral ou outra.
3. A informação coberta pelo dever de sigilo não pode ser transmitida a terceiros, nem objeto de licenciamento ou qualquer outro uso ou modo de aproveitamento económico, salvo se tal for autorizado expressamente, por escrito, pela entidade adjudicante.
4. O candidato só pode transmitir informação confidencial aos seus colaboradores e, em qualquer caso, apenas se ocorrerem, cumulativamente, as seguintes circunstâncias:
    a) Os colaboradores em causa necessitarem de conhecer essa informação, tendo em vista o cumprimento das suas tarefas ao abrigo do contrato.
    b) Os colaboradores estiverem informados sobre a natureza confidencial da informação.
    c) Os colaboradores se obrigarem a cumprir o dever de sigilo emergente desta cláusula.

5. O candidato é responsável pelo cumprimento do dever de sigilo por parte dos seus colaboradores, qualquer que seja a natureza jurídica do vínculo, inclusivamente após a cessação deste, independentemente da causa da cessação.
6. O candidato é ainda responsável perante a entidade adjudicante, em caso de violação do dever de sigilo pelos terceiros por si subcontratados, bem como por quaisquer colaboradores desses terceiros.

CLÁUSULA 14.ª

REQUISITOS DE NATUREZA AMBIENTAL OU SOCIAL

Na execução do contrato, o Adjudicatário deve garantir o cumprimento das normas ambientais e de saúde públicas aplicáveis, devendo o adjudicatário garantir a sua adequação a novas formas ou exigências.

CLÁUSULA 15.ª

DIREITOS DE PROPRIEDADE INTELECTUAL E INDUSTRIAL

1. São da responsabilidade dos candidatos quaisquer encargos decorrentes da utilização, no âmbito do Sistema de Aquisição Dinâmico ou dos contratos celebrados ao seu abrigo, de direitos de propriedade intelectual ou industrial.
2. O candidato garante que respeita as normas relativas à propriedade intelectual e industrial, designadamente, direitos de autor, licenças, patentes e marcas registadas, relacionadas com o hardware, software e documentação técnica que utilizam no desenvolvimento da sua atividade.
3. A propriedade e a posse de todo o material produzido pelo(s) Adjudicatário(s) no âmbito da execução do Contrato, nomeadamente quaisquer documentos e informação, estudos, matrizes de avaliação, relatórios, produtos e outros, pertencem exclusivamente as Entidades Adjudicantes, livre de ónus ou encargos.
4. Correm inteiramente por conta do(s) Adjudicatário(s), os encargos e responsabilidades decorrentes da utilização, na execução dos serviços objeto do contrato, de software, hardware ou de outros a que respeitem quaisquer patentes, licenças, marcas, desenhos registados e outros direitos de propriedade industrial ou direitos de autor ou conexos.
5. Se a(s) Entidade(s) Adjudicante(s) vier(em) a ser demandada por ter sido infringido, na execução dos serviços objeto do contrato, qualquer dos direitos referidos no ponto anterior, o(s) Adjudicatário(s) responderão nos termos do disposto no n.º 2 do artigo 447.º do CCP.

CLÁUSULA 16.ª

CASOS FORTUITOS OU DE FORÇA MAIOR

1. Não podem ser impostas sanções contratuais ao Adjudicatário, nem é havido como inadimplemento, a não realização pontual das obrigações contratuais a cargo de qualquer das partes que resulte de caso de força maior.
2. Para efeitos do contrato, só são consideradas de força maior as circunstâncias que, cumulativamente e em relação à parte que as invoca:
    a) Impossibilitem o cumprimento das obrigações emergentes do contrato;
    b) Sejam alheias à sua vontade;
    c) Não fossem por ela conhecidas ou previsíveis à data da celebração do contrato;
    d) Não lhe seja razoavelmente exigível contornar ou evitar os efeitos produzidos por aquelas circunstâncias.
3. Não constituem força maior, designadamente, quando aplicáveis:
    a) Circunstâncias que não constituam força maior para os subcontratados do Adjudicatário, na parte em que intervenham;
    b) Greves ou conflitos laborais limitados às sociedades do Adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
    c) Determinações governamentais, administrativas ou judiciais de natureza sancionatória, ou de outra forma resultantes do incumprimento pelo Adjudicatário de deveres ou ónus que sobre ele recaiam;
    d) Manifestações populares devidas ao incumprimento pelo Adjudicatário de normas legais;
    e) Incêndios ou inundações com origem nas instalações do Adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
    f) Avarias nos sistemas informáticos ou mecânicos do Adjudicatário não devidas a sabotagem;
    g) Eventos que estejam ou devam estar cobertos por seguros.
4. A parte que invocar caso de força maior deve comunicar e justificar tal situação à outra parte, logo após a sua ocorrência, bem como informar o prazo previsível para restabelecer o cumprimento das obrigações contratuais.
5. A suspensão, total ou parcial, do cumprimento pelo Adjudicatário das suas obrigações contratuais fundada em força maior, por prazo superior a 30 (trinta) dias, autoriza a SPMS, EPE a resolver o contrato ao abrigo do n.º 1 do artigo 335.º do CCP, não tendo o Adjudicatário direito a qualquer indemnização.

CLÁUSULA 17.ª

SUSPENSÃO OU RESOLUÇÃO SANCIONATÓRIA POR INCUMPRIMENTO CONTRATUAL

1. O incumprimento, por qualquer dos Candidatos admitidos, das obrigações que sobre si recaem nos termos do Sistema de Aquisição Dinâmico, do(s) contrato(s) celebrado(s) ao seu abrigo ou dos demais documentos contratuais aplicáveis, confere à SPMS, EPE o direito à resolução ou suspensão do Sistema de Aquisição Dinâmico relativamente àquele, podendo a SPMS solicitar o correspondente ressarcimento de todos os prejuízos causados.
2. O incumprimento dos requisitos da prestação de serviços deve ser reportado pelas entidades adjudicantes à SPMS, EPE.
3. Para efeitos da presente cláusula, e sem prejuízo de outras disposições legais e contratuais aplicáveis, considera-se consubstanciar incumprimento a verificação de qualquer das seguintes situações, em relação a cada um dos candidatos:
    a) Incumprimento de normas legais ou regulamentares aplicáveis ao exercício da sua atividade;
    b) Incumprimento das suas obrigações relativas aos pagamentos das contribuições à Administração Fiscal ou à Segurança Social, nos termos das disposições legais aplicáveis;
    c) Prestação de falsas declarações;
    d) Não apresentação dos relatórios previstos na cláusula 49.ª do presente caderno de encargos;
    e) Recusa do serviço a uma entidade adjudicante;
    f) Incumprimento dos requisitos previstos no presente caderno de encargos;
    g) Fornecimento de bens ou prestação de serviços que não integrem o Sistema de Aquisição Dinâmico;
    h) Incumprimento da obrigação de sigilo e confidencialidade prevista na cláusula 13.ª do presente caderno de encargos.
    i) Incumprimento das obrigações que resultam dos contratos celebrados ao abrigo do presente Sistema de Aquisição Dinâmico.
4. Em função da ponderação da gravidade e reiteração do incumprimento por parte do candidato, a verificação das situações *supra* elencadas, podem determinar a aplicação da suspensão do presente Sistema de Aquisição Dinâmico.
5. Para efeitos do disposto nas alíneas f), g) e h) do n.º 3, considera-se haver incumprimento definitivo quando, após advertência e aplicação de sanção, o candidato continue a incorrer em incumprimento.

6. A sanção de suspensão ou resolução é notificada ao candidato em causa, por carta registada com aviso de receção, da qual conste a indicação da situação de incumprimento e respetivos fundamentos.
7. A resolução do Sistema de Aquisição Dinâmico relativamente a um candidato não prejudica a aplicação de qualquer das sanções previstas nas cláusulas 18.ª e 48.ª do presente caderno de encargos.
8. A suspensão ou resolução do Sistema de Aquisição Dinâmico relativamente a um cocontratante só produz efeitos para os procedimentos iniciados após a publicação da decisão definitiva de aplicação da referida sanção na plataforma eletrónica www.comprasnasaude.pt.

CLÁUSULA 18.ª

SANÇÕES PELO INCUMPRIMENTO DAS OBRIGAÇÕES DOS COCONTRATANTES NA GESTÃO E ACOMPANHAMENTO DO SISTEMA DE AQUISIÇÃO DINÂMICO

1. Pelo incumprimento de obrigações emergentes do presente Sistema de Aquisição Dinâmico (SAD), a SPMS pode exigir aos cocontratantes o pagamento de sanções pecuniárias nos termos do presente caderno de encargos, ou pode a entidade adjudicante definir outras sanções a aplicar em cada procedimento.
2. A SPMS pode exigir aos cocontratantes o pagamento de sanções pecuniárias, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
    a) Em caso de incumprimento da apresentação dos relatórios de faturação previstos na cláusula 6.º, pode ser aplicada uma sanção pecuniária de €250,00, por cada relatório em falta e dia de atraso;
    b) No caso de se verificar que os valores apresentados nos relatórios de faturação são inferiores aos valores efetivamente faturados às entidades, será aplicada uma sanção pecuniária de 1% da diferença entre os valores, com um valor mínimo de €50,00 (aplicável para diferenças inferiores a €5.000) e um limite máximo de €500,00.

CAPÍTULO II

PARTE II

DOS PROCEDIMENTOS DE CONTRATAÇÃO AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

SECÇÃO I

OBRIGAÇÕES DAS ENTIDADES ADJUDICANTES NO ÂMBITO DOS CONTRATOS CELEBRADOS AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

CLÁUSULA 19.ª

CONTRATAÇÃO AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

1. A contratação ao abrigo do Sistema de Aquisição Dinâmico é efetuada através de convite a todos os candidatos qualificados ao lote do Sistema de Aquisição Dinâmico ao abrigo do qual será lançado o procedimento, nos termos do artigo 237.º do CCP.
2. Os procedimentos lançados ao abrigo do Sistema de Aquisição Dinâmico devem ser efetuados através da plataforma eletrónica disponível em www.comprasnasaude.pt, nos termos do disposto na Portaria n.º 227/2014, de 6 de novembro, alterado pela portaria n.º 21/2015, de 4 de fevereiro.
3. Para efeitos do n.º 2 do artigo 241.º-B do CCP, tendo sido o sistema de aquisição dinâmico dividido em lotes, a entidade adjudicante convida apenas os candidatos qualificados para o lote que abrange o serviço a contratar.
4. A entidade adquirente responsável pelo convite pode recorrer ao leilão eletrónico, nos termos previstos no CCP, para melhorar as condições propostas pelos concorrentes.
5. Os preços unitários devem ser indicados com duas casas decimais, em algarismos e por extenso, e devem incluir todas despesas de alojamento, alimentação, deslocação do pessoal do adjudicatário, taxas, impostos e restantes condições, não sendo admitidos portes ou outras taxas adicionais em qualquer circunstância.

CLÁUSULA 20.ª

DOCUMENTOS DA PROPOSTA NOS PROCEDIMENTOS DESENVOLVIDOS AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

1. Devem fazer parte dos documentos que integram as propostas apresentadas a procedimentos desenvolvidos ao abrigo do presente Sistema de Aquisição Dinâmico:
    a) Os documentos previstos nas alíneas a), b) e c) do n. º1 do artigo 57.º do CCP;
    b) Apresentação de preço, de acordo com o modelo de resposta disponibilizado pela entidade adjudicante;
    d) A identificação do gestor do contrato do operador económico;
    e) Documento descritivo dos serviços a prestar, se aplicável;
    f) As entidades adjudicantes podem, ainda, solicitar aos concorrentes a indicação nas suas propostas de quaisquer informações relativas às especificações e requisitos dos serviços propostos, incluindo as seguintes certificações:
        I. Certificação com o Quadro Nacional de Referência para a Cibersegurança (EC QNRCS);
        II. Comprovativo de membro da Rede Nacional de CSIRT, ou outra rede CSIRT similar;

III. Comprovativo de credenciação de segurança (CRESO), que habilite a manusear informação classificada de marca Nacional e grau Confidencial, emitida pela Autoridade Nacional de Segurança do Gabinete Nacional de Segurança;

IV. Certificado de conformidade QNRCS - Quadro Nacional de Referência para a Cibersegurança (EC QNRCS), no nível Básico, Substancial e Elevado, emitida por uma entidade devidamente acreditada para o efeito;

CLÁUSULA 21.ª

DEFINIÇÃO DAS PRESTAÇÕES A CONTRATUALIZAR

1. As entidades adjudicantes devem em cada procedimento:
   a) Definir os serviços a adquirir ao abrigo do Sistema de Aquisição Dinâmico;
   b) Definir as condições específicas que se aplicam à contratualização em causa, as quais podem ser da seguinte natureza:
      i. Termos de aceitação;
      ii. Quantidades;
      iii. Prazos de entrega;
      iv. Prazos de garantia, o qual deverá cumprir um período mínimo após a data de emissão da declaração de aceitação, e indicar se é prevista a extensão de garantia;
      v. Definir os níveis de serviço exigíveis;
      vi. Modelo de monitorização;
      vii. Controlo dos níveis de serviço.
      viii. Penalidades contratuais;
      ix. Cronogramas de execução de projeto
2. Preencher o inquérito de satisfação a disponibilizar pela SPMS, E.P.E., de modo a poder avaliar os adjudicatários e aferir a qualidade dos fornecimentos, devendo ser definido um nível de serviço mínimo para esse questionário (exemplo consta em Anexo II ao presente documento).
3. As entidades adjudicantes podem, no convite à apresentação de propostas, atualizar as características dos serviços a adquirir ao abrigo do Sistema de Aquisição Dinâmico, modificando-as ou substituindo-as por outras, em função da ocorrência de inovações tecnológicas, desde que se mantenham os objetivos das especificações fixadas no presente caderno de encargos.
4. Para efeitos do número anterior as entidades adjudicantes podem exigir outras especificações e requisitos que concretizem, desenvolvam ou complementem os já previstos, ou exigir especificações

e requisitos superiores aos previstos no presente Sistema de Aquisição Dinâmico, desde que em cumprimento com o disposto no artigo 49.º do CCP.

CLÁUSULA 22.ª

CRITÉRIOS DE ADJUDICAÇÃO NOS PROCEDIMENTOS AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

1. As entidades adjudicantes e a SPMS, EPE. em representação daquelas, 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.
3. Caso o critério de adjudicação a aplicar seja determinado na modalidade multifator, deverá preferencialmente incluir um subfactor ou um conjunto de subfatores de sustentabilidade ambiental, de acordo com a Resolução do Conselho de Ministros n.º 132/2023 ou outra legislação em vigor.

CLÁUSULA 23.ª

CRITÉRIO DE DESEMPATE

1. Para efeitos de critério de desempate nos procedimentos desenvolvidos ao abrigo do Sistema de Aquisição Dinâmico objeto do presente procedimento, se após a aplicação do critério de adjudicação supra indicado ocorrer um empate no topo da classificação, serão aplicados os seguintes fatores de desempate, sucessivamente, até ser encontrado o adjudicatário:
    a) 1º Critério: Melhor pontuação por via da qualidade global da proposta;
    b) 2º Critério: Menor preço proposto;

c) 3º Critério: Sorteio, a desenrolar presencialmente com os interessados, do qual será lavrada ata por todos os presentes.

CLÁUSULA 24.ª

RELATÓRIO PRELIMINAR E AUDIÊNCIA PRÉVIA

1. Após análise das propostas, o júri elabora fundamentadamente um relatório preliminar no qual deve propor a ordenação das propostas que não devam ser excluídas.
2. O relatório preliminar será notificado a todos os concorrentes para que, querendo, no prazo de 5 (cinco) dias úteis, se pronunciem por escrito, ao abrigo do direito de audiência prévia.

CLÁUSULA 25.ª

RELATÓRIO FINAL

Cumprido o disposto na cláusula anterior, o júri elabora um relatório final fundamentado, no qual analisa as observações dos concorrentes efetuadas ao abrigo do direito de audiência prévia, podendo manter ou modificar 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 do CCP.

CLÁUSULA 26.ª

NOTIFICAÇÃO DA DECISÃO DE ADJUDICAÇÃO

1. Para efeitos do disposto no artigo 77.º do CCP, 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;
   b) 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.

CLÁUSULA 27.ª

DOCUMENTOS DE HABILITAÇÃO

1. Sob pena de caducidade da adjudicação, no prazo de 10 (dez) dias úteis a contar da notificação da decisão de adjudicação, o(s) Adjudicatário(s) deve(m) apresentar na plataforma eletrónica de contratação pública, os seguintes Documentos de Habilitação:
   a) Declaração emitida conforme modelo constante do Anexo II do CCP;

b) Documentos comprovativos de que não se encontram nas situações previstas nas alíneas b), d), e) e h) do artigo 55.º do CCP, nomeadamente certidões do registo criminal do candidato qualificado e de todos os titulares dos órgãos sociais de administração, direção ou gerência, que se encontrem em efetividade de funções e, declarações de não dívida à Segurança Social e às Finanças (ou respetivas autorizações para consulta dos dados).

2. Quando o adjudicatário for um agrupamento, os documentos referidos nos números anteriores devem ser entregues por todos os membros que o constituem.
3. O órgão competente para a decisão de contratar pode sempre exigir aos adjudicatários a apresentação, em prazo a fixar para o efeito, dos originais de quaisquer documentos cuja reprodução tenha sido apresentada nos termos do disposto no n.º 1, em caso de dúvida fundamentada sobre o conteúdo ou autenticidade destes, sendo aplicável, com as necessárias adaptações, o disposto no artigo 86.º do CCP.

CLÁUSULA 28.ª

IDIOMA DOS DOCUMENTOS DE HABILITAÇÃO

1. Os documentos de habilitação devem ser redigidos em língua portuguesa.
2. Quando, pela sua própria natureza ou origem, os documentos de habilitação estiverem redigidos em língua estrangeira, devem as entidades adjudicatárias fazê-los acompanhar da respetiva tradução certificada.

CLÁUSULA 29.ª

NÃO APRESENTAÇÃO DOS DOCUMENTOS DE HABILITAÇÃO

1. A adjudicação caduca se, por facto que lhe seja imputável, os Adjudicatários não apresentarem os documentos de habilitação no prazo fixado no presente caderno de encargos
2. Quando as situações previstas no número anterior se verifiquem por facto que não seja imputável aos adjudicatários, será concedido, em função das razões invocadas, um prazo adicional de cinco dias para apresentação dos documentos em falta, sob pena de caducidade da adjudicação.

CLÁUSULA 30.ª

FALSIDADE DE DOCUMENTOS

Sem prejuízo da participação às entidades competentes para efeitos de procedimento criminal, a falsificação de quaisquer documentos de habilitação ou a prestação culposa de falsas declarações determina a caducidade da qualificação.

CAPÍTULO III

PARTE III

SECÇÃO I

CELEBRAÇÃO E EXECUÇÃO DO CONTRATO AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

CLÁUSULA 31.ª

ACEITAÇÃO DA MINUTA DO CONTRATO

1. A Minuta do Contrato será enviada, juntamente com a decisão de adjudicação, ao(s) adjudicatário(s) de cada Lote, através da plataforma eletrónica utilizada pela SPMS nos termos do presente caderno de encargos, para aceitação.
2. A minuta do Contrato considera-se aceite por cada um dos adjudicatários quando haja aceitação expressa ou quando em relação à mesma não seja apresentada reclamação nos cinco dias subsequentes à respetiva notificação.

CLÁUSULA 32.ª

RECLAMAÇÕES DA MINUTA

1. As reclamações da 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, o órgão que aprovou a minuta do contrato comunica ao reclamante a sua decisão.
3. Decorrido o prazo fixado no número anterior sem que órgão que aprovou a minuta do contrato se pronuncie sobre a reclamação apresentada, considera-se que a mesma foi rejeitada.

CLÁUSULA 33.ª

OUTORGA DO CONTRATO

1. O contrato será assinado por recurso a assinatura digital, e considerar-se-á outorgado na última data de aposição de assinatura.
2. O prazo concedido para a outorga e remessa do contrato pelo Adjudicatário ser-lhe-á comunicado com a antecedência mínima de 5 (cinco) dias úteis.
3. O incumprimento do prazo concedido para a outorga e remessa do contrato pelo Adjudicatário é causa de caducidade da adjudicação, assim como, no caso de agrupamento, se os seus membros não

se tiverem associado, nos termos previstos no n.º 4 do artigo 54.º do CCP e no artigo 6.º do programa de procedimento.

4. Nos casos previstos no número anterior, será adjudicada a proposta ordenada em lugar subsequente ao do último Adjudicatário selecionado.
5. No caso previsto no n.º 3, poderá ser instaurado ao concorrente selecionado um processo de contraordenação, nos termos consignados nos artigos 455.º e seguintes do CCP.

CLÁUSULA 34.ª

FORMA E PRAZO DE VIGÊNCIA DOS CONTRATOS CELEBRADOS AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

1. Os contratos que sejam celebrados ao abrigo do Sistema de Aquisição Dinâmico podem produzir efeitos para além da vigência do Sistema de Aquisição Dinâmico, desde que não ultrapassem as durações previstas na lei.
2. A instituição de novo Sistema de Aquisição Dinâmico com o mesmo objeto impossibilita qualquer renovação, por parte das entidades adjudicantes, dos contratos celebrados ao abrigo do Sistema de Aquisição Dinâmico objeto do presente caderno de encargos.

CLÁUSULA 35.ª

CONDIÇÕES E PRAZO DE ENTREGA

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 entrega poderá ser acordado entre a entidade adjudicante e o adjudicatário.
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.

CLÁUSULA 36.ª

INSPEÇÃO E TESTES

1. Efetuada a prestação dos serviços objeto do contrato, poderá a entidade adjudicante, por si ou através de terceiro por ela designado, proceder à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar, respetivamente, se os mesmos correspondem às quantidades estabelecidas nas

peças procedimentais e se reúnem as características, especificações e requisitos técnicos e operacionais aí exigidos e na proposta adjudicada, bem como demais requisitos exigidos por lei.

2. Durante a fase de realização de testes, que não poderá ter uma duração superior a 30 (trinta) dias, o adjudicatário deve prestar à entidade adjudicante toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a realização daqueles, através de pessoas devidamente credenciadas para o efeito.
3. Os encargos com a realização dos testes, devidamente comprovados, são da responsabilidade do Adjudicatário.

CLÁUSULA 37.ª

INOPERACIONALIDADE, DEFEITOS OU DISCREPÂNCIAS

1. No caso de os testes previstos na cláusula anterior não comprovarem a total operacionalidade dos bens e/ou serviços objeto do contrato, bem como a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as caraterísticas, especificações e requisitos técnicos definidos no presente Convite, a entidade adjudicante deve informar, por escrito, o adjudicatário.
2. No caso previsto no número anterior, o adjudicatário deve proceder, à sua custa e no prazo máximo de 5 (cinco) dias úteis, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e/ou serviços e o cumprimento das exigências legais e das caraterísticas, especificações e requisitos técnicos exigidos.
3. O adjudicatário dispõe de um prazo até 5 (cinco) dia úteis a contar da comunicação para suprir as deficiências e irregularidades detetadas, que não impliquem a rejeição dos serviços.
4. Após a realização das reparações ou substituições necessárias pelo adjudicatário, no prazo respetivo, a entidade adjudicante procede à realização de novos testes de aceitação, nos termos da cláusula anterior.
5. O Adjudicatário obriga-se prestar os serviços objeto do contrato com as características, especificações e requisitos técnicos previstos nas peças procedimentais.
6. Os serviços objeto do contrato deverão ser executados em perfeita conformidade com as condições estabelecidas nos documentos contratuais e legislação aplicável.
7. O Adjudicatário é responsável perante as entidades adjudicantes por qualquer defeito ou discrepância dos serviços objeto do contrato.

CLÁUSULA 38.ª

ACEITAÇÃO DOS BENS E SERVIÇOS

1. Caso os testes a que se refere a cláusula anterior comprovem a total operacionalidade dos bens e/ou serviços objeto do contrato, bem como a sua conformidade com as exigências legais e contratuais, e neles não sejam detetados quaisquer defeitos ou discrepâncias com as caraterísticas, especificações e requisitos técnicos definidos nas Peças Procedimentais, deve ser emitido uma declaração de aceitação, assinada pelos representantes do adjudicatário e da entidade adjudicante.
2. A assinatura de declaração a que se refere o número anterior não implica a aceitação de eventuais defeitos ou discrepâncias dos serviços e equipamentos objeto do contrato com as exigências legais ou com as caraterísticas, especificações e requisitos técnicos previstos no Convite.

CLÁUSULA 39.ª

CONFORMIDADE E GARANTIA TÉCNICA

O(s) Adjudicatário(s) fica(m) sujeito(s), com as devidas adaptações e no que se refere aos elementos entregues à SPMS em execução do(s) contrato(s), às exigências legais, obrigações do(s) Cocontratante(s) e prazos respetivos aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código dos Contratos Públicos e demais legislação aplicável.

CLÁUSULA 40.ª

CONDIÇÕES E PRAZOS 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.

SECÇÃO II

OBRIGAÇÕES DO ADJUDICATÁRIO NO ÂMBITO DOS CONTRATOS CELEBRADOS AO ABRIGO DO SISTEMA DE AQUISIÇÃO DINÂMICO

CLÁUSULA 41.ª

OBRIGAÇÕES DO(S) ADJUDICATÁRIO(S)

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 presente Caderno de Encargos, 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 fornecidos os bens e/ou 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 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;

CLÁUSULA 42.ª

TRATAMENTO DE DADOS PESSOAIS

1. No caso de o Adjudicatário necessitar de aceder a dados pessoais no decurso da execução do contrato, deve fazê-lo exclusivamente na medida do estritamente necessário para integral e adequada prossecução dos fins constantes do contrato, na qualidade de subcontratante, e por conta e de acordo com as instruções da SPMS, EPE, nos termos da legislação aplicável à proteção de dados pessoais.
2. O Adjudicatário não pode proceder à reprodução, gravação, cópia ou divulgação dos dados pessoais para outros fins que não constem do contrato, ou para proveito próprio.
3. O Adjudicatário deve cumprir rigorosamente as instruções da SPMS, EPE no que diz respeito ao acesso, registo, transmissão ou qualquer outra operação de tratamento de dados pessoais.
4. O Adjudicatário deve proceder à implementação de medidas de segurança de tratamento de dados pessoais e adotar medidas técnicas e organizativas para proteger os dados contra destruição acidental ou ilícita, perda acidental, alterações, difusão ou acesso não autorizados, e contra qualquer outra forma de tratamento ilícito dos mesmos.
5. O Adjudicatário deve tomar as medidas adequadas para assegurar a idoneidade dos seus trabalhadores ou colaboradores, a qualquer título, que tenham acesso aos dados pessoais fornecidos pela SPMS, EPE ou por quem atue em representação destes.
6. As medidas a que se refere o número anterior devem garantir um nível de segurança adequado em relação aos riscos que o tratamento de dados apresenta, à natureza dos dados a proteger e aos riscos, de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares.
7. O Adjudicatário deve assegurar que o acesso aos dados pessoais é limitado às pessoas que efetivamente necessitam de aceder aos mesmos para cumprir com as obrigações impostas pelo presente contrato e que os trabalhadores, colaboradores ou subcontratados assumiram um compromisso de confidencialidade ou estão sujeitos a adequadas obrigações legais de confidencialidade, sendo o Segundo Outorgante responsável pela utilização dos dados pessoais por parte dos mesmos.

8. Mediante solicitação escrita da SPMS, EPE, o Adjudicatário deve, no prazo de 15 (quinze) dias, informar quais as medidas tomadas para assegurar o cumprimento dos deveres referidos nos números anteriores.
9. O Adjudicatário deve comunicar de imediato a SPMS, EPE, quaisquer reclamações ou questões colocadas pelos titulares dos dados pessoais.
10. O Adjudicatário encontra-se adstrito a notificar de imediato a SPMS, EPE, de qualquer monitorização, auditoria ou controlo por parte de entidades reguladoras/de supervisão de que seja objeto.
11. Se o Adjudicatário tomar conhecimento, ou suspeitar, de violações de dados pessoais que resultem, ou possam resultar, na destruição acidental ou não autorizada de dados, na perda, alteração, acesso ou revelação não autorizada dos dados, deve notificar, por escrito, a S SPMS, EPE disponibilizando-lhe uma descrição da violação de dados ocorrida, informando-o das categorias e número de titulares de dados afetados, das prováveis consequências da violação, assim como fornecer-lhe qualquer outra informação que a SPMS, EPE possa razoavelmente solicitar.
12. Quando se verifique uma violação de dados pessoais, por causas imputáveis ao Adjudicatário, este compromete-se a adotar as seguintes medidas, sem quaisquer custos adicionais para a SPMS, EPE:
    a) Tomar de imediato as medidas necessárias para investigar a violação ocorrida, identificar e prevenir a repetição dessa violação, e encetar esforços razoáveis para mitigar os efeitos dessa violação;
    b) Desenvolver as ações necessárias para remediar a violação; e
    c) Documentar todas as circunstâncias referentes à violação para efeitos de controlo por parte da autoridade de supervisão.
13. O adjudicatário obriga-se a ressarcir a SPMS, EPE, por todos os prejuízos em que este venha a incorrer em virtude da utilização ilegal e/ou ilícita de dados pessoais, nomeadamente por indemnizações e despesas em que tenha incorrido na sequência de reclamações ou processos propostos pelos titulares dos dados, bem como por taxas, coimas e multas que tenha de pagar.
14. O incumprimento dos deveres estabelecidos na presente cláusula por parte do adjudicatário e a verificação de inexistência de garantias de *compliance* por este é fundamento de resolução do presente contrato com justa causa pela SPMS, EPE, podendo implicar o dever de indemnização por eventuais violações que lhe sejam imputadas.

CLÁUSULA 43.ª

CONSERVAÇÃO DE DADOS PESSOAIS

1. O Adjudicatário não pode, em circunstância alguma conservar os dados pessoais tratados, devendo proceder à sua destruição, quando os mesmos deixarem de ser necessários para a execução do contrato, e sempre em prazo não superior a um ano após a cessação do contrato que esteve na base da licitude do seu tratamento e de acordo com as instruções dadas pela Entidade Adjudicante.
2. Dependendo da opção da Entidade Adjudicante, o Adjudicatário apagará ou devolverá todos suportes físicos que contenham os dados pessoais, depois de concluída a execução do contrato, a menos que a conservação dos dados seja exigida ao abrigo da legislação aplicável.

CLÁUSULA 44.ª

TRANSFERÊNCIA DE DADOS PESSOAIS

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

CLÁUSULA 45.ª

DEVER DE COOPERAÇÃO

O Adjudicatário deve cooperar com a SPMS, EPE, mediante solicitação, designadamente nas seguintes situações:

a) Quando um titular de dados pessoais exerça os seus direitos ou cumpra as suas obrigações nos termos da legislação aplicável, relativamente aos dados pessoais tratados pelo Segundo Outorgante em representação da SPMS, EPE;
b) Quando a SPMS, EPE deva cumprir ou dar sequência a qualquer avaliação, inquérito, notificação ou investigação da Comissão Nacional de Proteção de Dados ou entidade administrativa com atribuições e competências legais equiparáveis.

CLÁUSULA 46.ª

CESSÃO DA POSIÇÃO CONTRATUAL E SUBCONTRATAÇÃO

1. Além da situação prevista na alínea a) do n.º 1 do artigo 318.º do Código dos Contratos Públicos, o(s) Adjudicatários(s) pode(m) ceder a sua posição contratual aos candidatos admitidos ao Sistema de Aquisição Dinâmico, na fase de execução do contrato, mediante autorização da SPMS, EPE.

2. Para efeitos da autorização a que se refere o número anterior, o(s) Adjudicatário(s) deve(m) apresentar uma proposta fundamentada e instruída com os documentos previstos no n.º 2 do artigo 318.º do Código dos Contratos Públicos.
3. A SPMS, EPE deve pronunciar-se sobre a proposta do Cedente no prazo de 30 (trinta) dias a contar da respetiva apresentação, desde que regularmente instruída, considerando-se o referido pedido rejeitado se, no termo desse prazo, a mesma não se pronunciar expressamente.
4. A subcontratação total ou parcial pelo(s) Adjudicatário(s) depende de autorização prévia e por escrito da SPMS, EPE, nos termos do Código dos Contratos Públicos.

CLÁUSULA 47.ª

SEGUROS

1. É da responsabilidade do adjudicatário a cobertura, através de contratos de seguro de acidentes pessoais, de quaisquer riscos de acidentes pessoais sofridos pelo seu pessoal ou por pessoal dos seus subcontratados, no contexto de ações no âmbito do presente contrato.
2. Os seguros de acidentes pessoais devem prever que as indemnizações sejam pagas aos sinistrados ou, em caso de morte, a quem prove ter a elas direito, nos termos da lei sucessória ou de outras disposições legais aplicáveis.

CLÁUSULA 48.ª

SANÇÕES CONTRATUAIS

1. As entidades adquirentes podem ainda aplicar as seguintes sanções:
   a) Pelo incumprimento do prazo fixado no n.º 2 da Cláusula 35.ª, pode ser aplicada uma sanção pecuniária calculada de acordo com a seguinte fórmula:

      VS = VA x até 1% x DA

      Em que,

      VS = Valor da sanção (em euros)

      VA = Valor do contrato adjudicado

      DA = Número de dias de atraso

   b) Pelo incumprimento do prazo previsto no ponto iv) da alínea b) do n.º 1 da Cláusula 21.ª, pode ser aplicada uma sanção pecuniária calculada de acordo com a seguinte fórmula:

      VS = VA x até 1% x DA

      Em que,

      VS = Valor da sanção (em euros)

      VA = Valor do contrato adjudicado

DA = Número de dias de atraso

c) Pelo incumprimento dos níveis de serviços, previstos no ponto v da alínea b) do n.º 1 da Cláusula 21.ª, pode ser aplicada uma sanção pecuniária calculada de acordo com a seguinte fórmula:

VS = VA x até 1% x DI

Em que,

VS = Valor da sanção (em euros)

VA = Valor do contrato adjudicado

DI = Número de dias de incumprimento

2. O valor das penalizações constantes do número anterior pode ser descontado na fatura relativa ao período em que se deu o facto que originou a sua aplicação.
3. Aos valores constantes da presente cláusula acresce o IVA à taxa legal em vigor.
4. O valor acumulado das sanções contratuais a aplicar não pode exceder o limite máximo de 20% do preço contratual.
5. Nos casos em que seja atingido o limite de 20% e o SPMS decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.
6. As entidades Adjudicantes podem descontar o valor das sanções contratuais devidas nos termos da presente cláusula nos pagamentos devidos ao Adjudicatário.
7. As sanções contratuais previstas na presente cláusula não obstam a que as Entidades Adjudicantes exijam uma indemnização pelo dano excedente.

PARTE III

REPORTE

CLÁUSULA 49.ª

REPORTE E MONITORIZAÇÃO

1. Constitui obrigação dos adjudicatários produzir e enviar os seguintes relatórios de gestão do Sistema de Aquisição Dinâmico:
    a) Relatórios específicos sobre aspetos relacionados com a execução do contrato e níveis de serviço com a periodicidade acordada com a entidade adjudicante.
2. Para efeitos do disposto no número anterior, a entidade adjudicante deverá notificar previamente o adjudicatário para, num prazo não superior a 5 (cinco) dias, emitir o relatório em falta ou corrigir a informação em falta no relatório enviado.
3. Os relatórios são emitidos tendo em conta a existência de 2 (dois) perfis diferenciados:
    a) SPMS, EPE. – recebe a informação respeitante aos contratos celebrados por cada uma das entidades adjudicantes.
    b) Entidade adjudicante – recebe a informação individualizada do contrato celebrado por si.
4. Os relatórios de níveis de serviço devem obrigatoriamente conter os seguintes elementos:
    a) Identificação da entidade adjudicante;
    b) Número de contrato;
    c) Vigência do contrato (dias);
    d) Datas de início e de fim do contrato;
    e) Descrição dos bens e serviços;
    f) Número de dias decorridos entre a data do pedido do serviço e a data de prestação do serviço;
    g) Tipo e quantidade de bens e/ou serviços fornecidos sem a qualidade requerida;

h) Justificação para eventuais incumprimentos nos fornecimentos e prestação de serviços;

i) Sanções aplicadas pela entidade adjudicante e respetiva justificação.

5. Os relatórios dos níveis de serviço devem ser enviados à SPMS, EPE, até ao dia 20 (vinte) do mês subsequente do período a que respeitam, conforme periodicidade prevista no n.º 1 da presente cláusula, em formato eletrónico a definir pela SPMS, EPE., e pela entidade adjudicante respetivamente.

CAPÍTULO III

DISPOSIÇÕES FINAIS

CLÁUSULA 50.ª

DEVERES DE INFORMAÇÃO

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

CLÁUSULA 51.ª

COMUNICAÇÕES E NOTIFICAÇÕES

1. Quaisquer comunicações ou notificações entre a SPMS, EPE e os candidatos qualificados relativas ao Sistema de Aquisição Dinâmico, devem ser efetuadas através de correio eletrónico com aviso de entrega, carta registada com aviso de receção.
2. Qualquer comunicação ou notificação 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 ou notificação feita por correio eletrónico é considerada recebida na data constante na respetiva comunicação de receção transmitida pelo recetor para o emissor.

4. As notificações e as comunicações que tenham como destinatário a SPMS, EPE ou entidades adjudicantes, e que sejam efetuadas através de correio eletrónico, ou outro meio de transmissão escrita e eletrónica de dados, feitas após as 17 horas do local de receção ou em dia não útil nesse mesmo local, presumem-se feitas às 10 horas do dia útil seguinte.

CLÁUSULA 52.ª

CONTAGEM DOS PRAZOS NA FASE DE EXECUÇÃO DO SISTEMA DE AQUISIÇÃO DINÂMICO E DOS CONTRATOS CELEBRADOS AO SEU ABRIGO

Para efeitos do disposto no artigo 471.º do Código dos Contratos Públicos, à contagem de prazos na fase de execução do Sistema de Aquisição Dinâmico e dos contratos celebrados ao seu abrigo, são aplicáveis as seguintes regras:

a) Não se inclui na contagem do prazo o dia em que ocorrer o evento a partir do qual o mesmo começa a correr;
b) Os prazos são contínuos, não se suspendendo nos sábados, domingos e feriados;
c) O prazo fixado em semanas, meses ou anos, a contar de certa data, termina às 24 horas do dia que corresponda, dentro da última semana, mês ou ano, a essa data;
d) O prazo que termine em sábado, domingo, feriado ou em dia em que o serviço, perante o qual deva ser praticado o ato, não esteja aberto ao público, ou não funcione durante o período normal, transfere-se para o 1º dia útil seguinte.

CLÁUSULA 53.ª

INTERPRETAÇÃO E VALIDADE

1. O Sistema de Aquisição Dinâmico e demais documentos contratuais regem-se pela lei portuguesa, sendo interpretados de acordo com as suas regras.
2. As partes no Sistema de Aquisição Dinâmico que tenham dúvidas acerca do significado de quaisquer documentos contratuais, devem colocá-las à parte contrária a quem o significado dessa disposição diga diretamente respeito.
3. Se qualquer disposição do Sistema de Aquisição Dinâmico ou de quaisquer documentos contratuais for anulada ou declarada nula, as restantes disposições não serão prejudicadas por esse facto, mantendo-se em vigor.

CLÁUSULA 54.ª

DIREITO APLICÁVEL E NATUREZA DO(S) CONTRATO(S)

1. O(s) contratos ao abrigo do Sistema de Aquisição Dinâmico regem-se pelo direito português e têm natureza administrativa.
2. A tudo o que não esteja especialmente previsto no presente caderno de encargos aplica-se a legislação portuguesa e, em especial, o regime constante do Código dos Contratos Públicos, com as alterações vigentes, o qual prevalece sobre as disposições que lhe sejam desconformes.

CLÁUSULA 55.ª

FORO COMPETENTE

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

ANEXOS:

Anexo I – Especificações Técnicas

Anexo II – Exemplo de Inquérito de satisfação

Anexo III – Requisitos Mínimos

ANEXO I

ESPECIFICAÇÕES TÉCNICAS

CLÁUSULA 1.ª

ÂMBITO

1. O presente Sistema de Aquisição Dinâmico tem por objeto a seleção de candidatos para a prestação de serviços de cibersegurança, ao abrigo do Sistema de Aquisição Dinâmico, e rege-se com as necessárias adaptações, pelo disposto nos artigos 162.º a 192.º do CCP.
2. Considera-se serviços de cibersegurança as atividades desenvolvidas por recursos humanos nas áreas dos sistemas e tecnologias de informação e de comunicação, que têm em vista garantir a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação.
3. Nos termos do n.º 9 do artigo 49.º do Código dos Contratos Públicos, as referências a marcas comerciais ou modelos no presente Sistema de Aquisição Dinâmico são meramente indicativas, de forma a possibilitar uma descrição suficientemente precisa e inteligível do objeto, termos em que são acompanhadas da menção «ou equivalente».

CLÁUSULA 2.ª

REQUISITOS AMBIENTAIS

1. O adjudicatário deve garantir o cumprimento das normas ambientais e de saúde públicas aplicáveis, devendo garantir a sua adequação a novas normas ou exigências que entrem em vigor no período de vigência do contrato.
2. Nos convites desenvolvidos ao abrigo do presente Sistema de Aquisição Dinâmico, as entidades adjudicantes devem indicar para os serviços a adquirir a possibilidade de aplicação de critérios ecológicos, de acordo com a Resolução do Conselho de Ministros n.º 132/2023, sendo dispensadas da sua utilização em casos especialmente fundamentados.

CLÁUSULA 3.ª

REQUISITOS TÉCNICOS

1. O Sistema de Aquisição Dinâmico encontra-se estruturado da seguinte forma:

Categoria 1: Projetos de conformidade e segurança de informação, análise dos riscos e continuidade de negócio

ix. Lote 1: Gestor de projeto / serviço

x. Lote 2: Gestor de projeto / serviço- Sénior

xi. Lote 3: Consultor de segurança da informação

xii. Lote 4: Consultor de segurança da informação- Sénior

xiii. Lote 5: Auditor de cibersegurança

xiv. Lote 6: Auditor de cibersegurança- Sénior

xv. Lote 7: Engenheiro de cibersegurança aplicacional

xvi. Lote 8: Engenheiro de cibersegurança aplicacional – Sénior

Categoria 2: Projetos de deteção de incidentes de cibersegurança

ix. Lote 9: Gestor de projeto / serviço

x. Lote 10: Gestor de projeto / serviço – Sénior

xi. Lote 11: Analista de cibersegurança

xii. Lote 12: Analista de cibersegurança- Sénior

xiii. Lote 13: Engenheiro de cibersegurança de redes e infraestrutura

xiv. Lote 14: Engenheiro de cibersegurança de redes e infraestrutura- Sénior

xv. Lote 15: Consultor de segurança da informação

xvi. Lote 16: Consultor de segurança da informação- Sénior

Categoria 3: Projetos de resposta e recuperação a incidentes de cibersegurança

xiii. Lote 17: Gestor de projeto / serviço

xiv. Lote 18: Gestor de projeto / serviço – Sénior

xv. Lote 19: Analista de cibersegurança

xvi. Lote 20: Analista de cibersegurança- Sénior

xvii. Lote 21: Engenheiro de cibersegurança de redes e infraestrutura

xviii. Lote 22: Engenheiro de cibersegurança de redes e infraestrutura- Sénior

xix. Lote 23: Engenheiro de cibersegurança aplicacional

xx. Lote 24: Engenheiro de cibersegurança aplicacional – Sénior

xxi. Lote 25: Consultor de segurança da informação

xxii. Lote 26: Consultor de segurança da informação- Sénior

xxiii. Lote 27: Auditor de cibersegurança

xxiv. Lote 28: Auditor de cibersegurança- Sénior

Categoria 4: Análise forense e auditorias técnicas de segurança

vii. Lote 29: Gestor de projeto / serviço

viii. Lote 30: Gestor de projeto / serviço- Sénior

ix. Lote 31: Pentester

x. Lote 32: Pentester – Sénior

xi. Lote 33: Auditor de cibersegurança

xii. Lote 34: Auditor de cibersegurança- Sénior

Categoria 5: Projetos de arquiteturas de redes e comunicações seguras

vii. Lote 35: Gestor de projeto / serviço

viii. Lote 36: Gestor de projeto / serviço- Sénior

ix. Lote 37: Engenheiro de cibersegurança de redes e infraestrutura

x. Lote 38: Engenheiro de cibersegurança de redes e infraestrutura- Sénior

xi. Lote 39: Consultor de segurança da informação

xii. Lote 40: Consultor de segurança da informação- Sénior

Categoria 6: Projetos de segurança no desenvolvimento de software

ix. Lote 41: Gestor de projeto / serviço

x. Lote 42: Gestor de projeto / serviço- Sénior

xi. Lote 43: Engenheiro de cibersegurança aplicacional

xii. Lote 44: Engenheiro de cibersegurança aplicacional – Sénior

xiii. Lote 45: Pentester

xiv. Lote 46: Pentester – Sénior

xv. Lote 47: Consultor de segurança da informação

xvi. Lote 48: Consultor de segurança da informação- Sénior

Categoria 7: Projetos de gestão e controlo identidades e acessos

xi. Lote 49: Gestor de projeto / serviço

xii. Lote 50: Gestor de projeto / serviço- Sénior

xiii. Lote 51: Engenheiro de cibersegurança de redes e infraestrutura

xiv. Lote 52: Engenheiro de cibersegurança de redes e infraestrutura- Sénior

xv. Lote 53: Engenheiro de cibersegurança aplicacional

xvi. Lote 54: Engenheiro de cibersegurança aplicacional – Sénior

xvii. Lote 55: Consultor de segurança da informação

xviii. Lote 56: Consultor de segurança da informação- Sénior

xix. Lote 57: Auditor Cibersegurança

xx. Lote 58: Auditor Cibersegurança – Sénior

2. Os requisitos técnicos obrigatórios e recomendados, dos perfis de recursos humanos correspondente aos lotes estabelecidos, bem como a descrição de funções destes perfis, encontram-se disponíveis no "**Anexo III – Requisitos Mínimos**" ao presente Caderno de Encargos.
3. Para efeitos de compatibilidade e adequação dos serviços a prestar ao abrigo do presente Sistema de Aquisição Dinâmico, poderá ser referido por parte das entidades adjudicantes a infraestrutura,

equipamentos e aplicações já instalados, de modo a assegurar por parte dos adjudicatários a correta prestação dos serviços.

ANEXO II

EXEMPLO NÃO VINCULATIVO DE INQUÉRITO DE SATISFAÇÃO APÓS TERMINUS DE CONTRATO

Exemplo de Questionário de Satisfação

Questão	Avaliação	Comentários
Como classificaria o desempenho geral do fornecedor?	Escala da avaliação	
Qual o nível de cumprimento dos níveis de serviço impostos no contrato?	Escala da avaliação	
Qual o grau de satisfação para com o trabalho realizado?	Escala da avaliação	
Qual o grau de criação de valor do fornecedor?	Escala da avaliação	
Voltaria a trabalhar com o mesmo fornecedor?	Sim / Não	
Recomendaria o fornecedor a outras entidades clientes?	Sim / Não	

Escala de Avaliação:

5 – Muito Bom

1 – Muito Mau

ANEXO III

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 dos procedimentos de contratação ao abrigo do Sistema de Aquisição Dinâmico 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:

   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- 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;

Experiência em métodos de ataque, métodos de teste de penetração manual e ferramentas de hacking – Nmap Metasploit, Linux Kali, Burp Suite Pro.

d) 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

a) O perfil de Consultor de segurança da informação, nos lotes das categorias a que este se aplica, tem nas suas funções as atividades:
b) Contribuir para a definição de políticas, normas e procedimentos de segurança da informação e cibersegurança;

c) Produção de documentação no âmbito segurança da informação e cibersegurança;
d) Realização de avaliações de risco em apoio a projetos de implementação de SI e TI;
e) Apoiar a configuração da solução gestão de risco garantindo consistência com processos locais;
f) Definir indicadores-chave de risco e desempenho (KRIs/KPIs) para avaliar o desempenho da gestão de riscos;
g) Determinação dos controlos apropriados para mitigar os riscos;
h) Apoiar a elaboração de planos de continuidade de negócio e plano de crise de cibersegurança;
i) Desenvolver e apoiar a realização de ações de formação e sensibilização em segurança de informação e cibersegurança;
j) Produção de relatórios de avaliação de risco em cibersegurança.

1. 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:
   k) Licenciatura ou grau académico superior em Engenharia Informática, Engenharia Eletrotécnica ou Sistemas e Tecnologias de Informação, ou formação de técnico profissional nas mesmas áreas;
   l) Experiência profissional comprovada na área das TIC ≥ 3 anos;
   m) Experiência profissional em projetos de segurança de informação;
   n) 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.

2. 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;

3. 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.