António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2021.07.05 09:45:02 +01'00'

CADERNO DE ENCARGOS

Aquisição de estudo de identificação de atribuições e competências de países no âmbito da Segurança da Informação, da Informação Classificada e da Cibersegurança

CADERNO DE ENCARGOS

PARTE I – DO CONTRATO

Cláusula 1

Objeto

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto a aquisição de um "ESTUDO DE IDENTIFICAÇÃO DE ATRIBUIÇÕES E COMPETÊNCIAS DE PAÍSES NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO, DA INFORMAÇÃO CLASSIFICADA E DA CIBERSEGURANÇA", doravante designado por "Estudo", de acordo com as Cláusulas Técnicas descritas no Anexo I da Parte II do Caderno de Encargos.

Cláusula 2

Definições

Para efeitos do presente Caderno de Encargos, adotam-se as seguintes definições:

CCP – Códigos dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na redação atual;

Contrato – contrato a celebrar entre a Entidade Adjudicante e o adjudicatário nos termos do presente caderno de encargos;

Órgão competente para a decisão de contratar – Exmo. Diretor Geral do Gabinete Nacional de Segurança, António Gameiro Marques;

"Entidade Adjudicante" ou "Adjudicante" – Presidência de Conselho de Ministros – Gabinete Nacional de Segurança – Centro Nacional de Cibersegurança;

"Entidade Adjudicatária" ou "Adjudicatário" – entidade a quem se adjudica a execução do contrato.

Cláusula 3

Local de Prestação dos Serviços

A prestação de serviços, objeto deste contrato, deverá ser efetuada nas instalações da Entidade Adjudicatária e entregue na sede da Entidade Adjudicante, sita na Rua da Junqueira Nº 69, 1300-342 Lisboa.

Cláusula 4

Prazo e vigência do contrato

A prestação de serviços a realizar no âmbito do contrato deverá ser executada até 60 dias após adjudicação, sem prejuízo dos prazos especiais constantes do Anexo I da Parte II do Caderno de Encargos e das obrigações acessórias que devem perdurar para além da cessação do contrato.

Cláusula 5

Preço base e preço contratual

1. Nos termos e para os efeitos, de acordo com o art.º 47 do CCP, o preço base do procedimento é fixado em **25.000,00 € (vinte e cinco mil Euros) acrescido de IVA à taxa legal em vigor**.
2. O preço base do procedimento constitui o limite máximo suscetível de ser apresentado nas propostas concorrentes, constituindo a sua violação causa de exclusão dessa proposta.

Cláusula 6

Preço ou custo anormalmente baixo

Nos termos e para os efeitos do art.º 71 do CCP, considera-se preço ou custo de uma proposta anormalmente baixo quando o preço base das propostas, não incluindo o valor relativo ao IVA, apresentar um valor inferior em 30% do preço base e contratual definido na cláusula 6ª do presente Caderno de Encargos.

Cláusula 7

Pagamento e condições de pagamento

1. As quantias devidas pelo GNS/CNCS serão pagas no prazo de 30 dias após a receção da fatura e vencimento da obrigação respetiva.
2. Para os efeitos do número anterior, a obrigação considera-se vencida após a aceitação, pelo GNS/CNCS, do objeto do contrato em causa.
3. Desde que devidamente emitida e observado o disposto no n.º 1, a fatura é paga através de transferência bancária.
4. Nas condições de pagamento a apresentar pelos concorrentes não podem ser propostos adiantamentos.

Cláusula 8

Caução

Não é exigida a prestação de caução dado que o preço contratual é inferior a € 200.000,00 (duzentos mil euros), nos termos da alínea a) do nº. 2 do Art.º 88.º do Código dos Contratos Públicos.

Cláusula 9

Dever de sigilo e confidencialidade

1. A Entidade Adjudicatária deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à Entidade Adjudicante, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.
4. O dever de sigilo a que alude os números anteriores mantém-se em vigor para além do termo de vigência, inicial ou que venha a ser acordado, sob pena de o adquirente dos serviços instaurar a competente ação judicial para efeitos de justa indemnização, em especial quando dessa revelação de informação venha a resultar dano ou prejuízo para a imagem do GNS/CNCS ou para os terceiros com os quais mantenha relações institucionais ou comerciais, caso em que a violação de quaisquer deveres legais a que o adjudicatário se encontre vinculado no âmbito da sua atividade, designadamente, os relativos à proteção de segredos comerciais ou outros conexos, será comunicada às autoridades administrativas e criminais competentes, para os devidos efeitos.
5. A Entidade Adjudicatária, para além de guardar sigilo, deve também garantir total confidencialidade sobre todos os assuntos constantes do objeto do presente caderno de encargos, e tratar como confidencial toda a informação e documentação a que

tenha acesso no âmbito da sua execução, sendo esta obrigação extensível a outras partes, colaboradores ou terceiros que as mesmas envolvam.

Cláusula 10

Proteção de Dados Pessoais

1. Qualquer acesso que a Entidade Adjudicatária venha a ter relativamente a qualquer dado pessoal apenas pode ocorrer para os fins constantes do presente caderno de encargos, e nos termos da legislação aplicável à proteção de dados pessoais.
2. A Entidade Adjudicatária não pode proceder à reprodução, gravação, cópia ou divulgação dos dados pessoais para outros fins que não constem no presente documento, comprometendo-se ainda ao seguinte:
    a. Respeitar integralmente o disposto na legislação europeia e nacional aplicável à proteção de dados pessoais e em qualquer outra legislação que a substitua e/ou venha a ser aplicável a esta matéria;
    b. Cumprir rigorosamente as instruções do caderno de encargos no que diz respeito ao acesso, registo, transmissão ou qualquer outra operação de tratamento de dados pessoais;
    c. Tratar os dados pessoais de forma lícita e com respeito pelo princípio da boa-fé, utilizando-os exclusivamente para as finalidades a que se reporta o Contrato, não podendo ser posteriormente tratados de forma incompatível com tais finalidades;
    d. Implementar 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 dados pessoais.
3. Se quaisquer dados se perderem ou forem danificados no âmbito da execução do Contrato, por causas imputáveis à Entidade Adjudicatária, esta compromete-se a adotar as medidas que forem necessárias com vista à recuperação dos dados, sem quaisquer custos adicionais.

Cláusula 11

Penalidades

1. No caso de incumprimento dos prazos fixados no contrato e por causa imputável ao

adjudicatário, será aplicada uma penalidade, por cada dia de atraso a partir do prazo estabelecido na Cláusula 5, no valor correspondente a um trigésimo (1/30) do valor do contrato.

2. No caso de o adjudicatário incumprir no prazo fixado em mais de 10 dias, a Entidade Adjudicante pode resolver o contrato, a título sancionatório, passando à contratação com o concorrente cuja proposta tenha sido classificada em segundo lugar, e assim sucessivamente.

Cláusula 12

Resolução por parte do contraente público

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o GNS pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grosseira ou negligente ou de modo grave ou reiterado qualquer uma das obrigações que lhe incumbem.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao adjudicatário.

Cláusula 13

Cessão da posição contratual e subcontratação

1. A Entidade Adjudicatária não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da Entidade Adjudicante.
2. A Entidade Adjudicatária não pode subcontratar total ou parcialmente os serviços incluídos no mesmo sem autorização prévia da Entidade Adjudicante
3. Para efeitos da autorização prevista no número anterior, deve:
   a) Ser apresentada pelo cessionário ou pela entidade subcontratada toda a documentação exigida ao adjudicatário no presente concurso;
   b) A Entidade Adjudicante deverá apreciar, designadamente, se o cessionário ou a entidade subcontratada não se encontra em nenhuma das situações previstas no artigo 55º do CCP, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual, e se tem capacidade técnica e financeira para assegurar o exato e pontual cumprimento do contrato.

Cláusula 14

Responsabilidade e Obrigações principais da Entidade Adjudicatária

1. A Entidade Adjudicatária responde pelos danos que causar à entidade contratante em razão do incumprimento culposo das obrigações que sobre ele impendam.
2. A Entidade Adjudicatária responde ainda perante a Entidade Adjudicante pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do contrato, como se tais atos ou omissões fossem praticados por aquele.
3. A Entidade Adjudicatária aceita e compromete-se a cumprir com as Obrigações de Segurança constantes da Cláusula 2ª da Parte II – Cláusulas Técnicas, do presente Caderno de Encargos.

Cláusula 15

Alterações ou aditamentos do contrato

Qualquer alteração ou aditamento ao contrato, que não diga respeito a questões fundamentais do procedimento, apenas será válida se resultar de acordo de ambos os contraentes, reduzido a escrito e anexado ao contrato inicial.

Cláusula 16

Garantias

1. A Entidade Adjudicatária, a título de garantia pelos serviços fornecidos, compromete-se a prestar no mínimo os períodos de garantias exigidos por lei, não podendo neste caso ser inferior a um ano.
2. A garantia cobre, nomeadamente, a correção de erros e divergências face à especificação do serviço definido.

Cláusula 17

Foro competente para resolução de litígios

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

Cláusula 18

Contagem dos Prazos

Os prazos previstos no contrato são contínuos, correndo em Sábados, Domingos e dias feriados.

Cláusula 19

Legislação aplicável

O contrato é regulado pela legislação portuguesa.

PARTE II – CLÁUSULAS TÉCNICAS

Cláusula 1

Caracterização do serviço a prestar e Requisitos

As características e requisitos do serviço a prestar são as que se indicam no Anexo I "AQUISIÇÃO DE ESTUDO DE IDENTIFICAÇÃO DE ATRIBUIÇÕES E COMPETÊNCIAS DE PAÍSES NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO, DA INFORMAÇÃO CLASSIFICADA E DA CIBERSEGURANÇA" do presente Caderno de Encargos.

Cláusula 2

Obrigações de Segurança

Pela aceitação do contrato e desenvolvimento das atividades relacionadas com o presente procedimento, a Entidade Adjudicatária, assim como entidades por ela subcontratadas ou pessoas que com ela colaborem no âmbito do procedimento, encontram-se obrigadas a cumprir com as Obrigações de Segurança constantes no Anexo II, regulamentos e demais legislação emanada pela Autoridade Nacional de Segurança ou do âmbito da proteção do segredo, nos termos dos artigos 4.º e 5.º das normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação (SEGNAC 2), aprovadas pela Resolução do Conselho de Ministros n.º 37/89, de 24 de outubro, e a Resolução do Conselho de Ministros n.º 50/88, de 3 de dezembro, que aprova as instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas (SEGNAC 1).

Cláusula 3

Gestor do contrato

3. A Entidade Adjudicante designará um gestor do contrato, com a função de acompanhar permanentemente a execução contratual nos termos e para os efeitos do artigo 290-A do CCP.

4. Caso o gestor do contrato detete desvios, defeitos ou outras anomalias na execução do contrato, deverá comunicá-los de imediato à Entidade Adjudicatária, propondo em relatório fundamentado, as medidas corretivas que se revelem necessárias.

ANEXO I

AQUISIÇÃO DE ESTUDO DE IDENTIFICAÇÃO DE ATRIBUIÇÕES E COMPETÊNCIAS DE PAÍSES NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO, DA INFORMAÇÃO CLASSIFICADA E DA CIBERSEGURANÇA

ENQUADRAMENTO

Com o objetivo de identificar boas práticas operacionais e ao nível de políticas públicas, tendo em vista o princípio de tomada de decisão informada para fazer face aos desafios que se colocam ao nível nacional e internacional, o Gabinete Nacional de Segurança (GNS) e o Centro Nacional de Cibersegurança (CNCS) pretendem desenvolver um estudo sobre a organização de atribuições e competências em vários países no âmbito de três áreas específicas, a saber: da segurança da informação, da gestão/segurança da informação classificada e da cibersegurança.

Para esse efeito, a atividade contratada visa identificar as competências e os modelos e estruturas de governação para cada uma das três áreas especificadas, interpretando as atribuições, atividades, papéis, responsabilidades, componentes e elementos críticos dos países a considerar, bem como a identificação das entidades e atores relacionados relevantes e os fluxos e trajetórias de atividade(s) nos países que venham a ser considerados no Estudo, contextualizando os seus quadros de políticas públicas e dos poderes de regulação, supervisão e execução (*enforcement*) que lhes estão atribuídos.

O documento a produzir deverá, assim, não apenas demonstrar a realidade organizacional Portuguesa no que diz respeito às três áreas específicas, como refletir uma análise fundamentada com uma análise das principais vantagens e desvantagens, preferencialmente SWOT, dos modelos identificados nos países considerados para o Estudo.

Serve assim o presente para a adjudicação do Estudo de identificação de atribuições e competências de países nas áreas da Segurança da Informação, da Informação Classificada e da Cibersegurança.

Para o efeito de realização do Estudo a adjudicar devem ser considerados os seguintes pontos que configuram o contexto a analisar:

1. O Gabinete Nacional de Segurança (GNS), enquanto serviço da administração direta do Estado, dotado de autonomia administrativa, que funciona no âmbito da Presidência do Conselho de Ministros (PCM), na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar", tendo por missão garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e exercer a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado - Infraestrutura de Chaves Públicas (SCEE);

2. O Centro Nacional de Cibersegurança (CNCS), enquanto Autoridade Nacional de Cibersegurança, tendo por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

3. O quadro estratégico e legislativo de âmbito nacional, europeu e internacional no âmbito da segurança da informação e da informação classificada (identificado em "R2. Gerais do Estudo");

4. O quadro estratégico e legislativo nacional e europeu no âmbito da cibersegurança (identificado em "R2. Gerais do Estudo");

5. O quadro atual de indicadores de referência de âmbito social, económico e tecnológico (identificado em "R2. Gerais do Estudo");

OBJETO

É objeto do presente caderno de encargos a realização de Estudo de identificação de atribuições e competências de países no âmbito da Segurança da Informação, da Informação Classificada e da Cibersegurança.

REQUISITOS

R1. Sobre a execução do serviço

1. Os concorrentes deverão apresentar uma proposta que refira os custos parciais e totais para o fornecimento do objeto supramencionado, detalhando a forma de abordagem e tempo a afetar para a resposta a todos e a cada um dos requisitos identificados.

2. Serão aceites as propostas de outras considerações pertinentes apresentadas pelos concorrentes sobre cada um dos requisitos.

3. Na proposta deverão ser incluídos todos os serviços necessários à boa prossecução do objeto referido.

4. Os resultados a entregar e todos os conteúdos produzidos devem ainda respeitar as regras, os logotipos, as normas gráficas de comunicação escrita e formatos de apresentação do GNS e CNCS.

5. O Estudo a produzir no âmbito deste procedimento deve ser entregue em formato editável e em PDF, em língua Portuguesa, sendo a propriedade dos materiais produzidos exclusiva do GNS e CNCS.

6. Os produtos[1] desenvolvidos no âmbito do presente procedimento serão propriedade exclusiva do GNS e CNCS.

7. Até 7 dias após a adjudicação do presente Caderno de Encargos, a Entidade Adjudicatária deverá reunir-se com a Entidade Adjudicante para validação da boa

[1] Incluindo a metodologia de elaboração do estudo e os dados utilizados.

compreensão do serviço adjudicado e dos requisitos apresentados no presente Caderno de Encargos.

8. A Entidade Adjudicatária deverá informar a Entidade Adjudicante, semanalmente e através de correio eletrónico, do desenvolvimento do seu trabalho, para validação do bom andamento do projeto.

9. Sempre que necessário, a Entidade Adjudicante e a Entidade Adjudicatária deverão reunir-se para uma reunião de acompanhamento do desenvolvimento, devendo estas reuniões ser realizadas, no mínimo, com uma periodicidade quinzenal, no formato presencial nas instalações do GNS e CNCS ou por videoconferência por acordo das partes.

10. Caso uma das partes, verifique ser necessário o agendamento de reuniões de trabalho para além das referidas, as mesmas deverão ser objeto de informação prévia à contraparte, para efeitos de agendamento, acompanhamento e moderação.

11. Nos serviços a desenvolver e proposta a apresentar não devem ser considerados custos com materiais e equipamentos de suporte à execução.

R2. Gerais do Estudo

1. A identificação dos países a considerar no Estudo a contratualizar deve obedecer a princípios passíveis de estabelecer paralelos com a realidade portuguesa, seja ao nível dos valores e/ou quadros normativos e estratégicos que servem de referência a Portugal. Nesse sentido, o objeto deste Estudo deve considerar, no mínimo, os seguintes aspetos:

1.1. O princípio de separação de poderes (legislativo, executivo e judicial);

1.2. O respeito pelas Liberdades, Garantias e Direitos fundamentais, tendo como principais referências a

1.3. Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais;

1.4. Declaração Universal dos Direitos Humanos; e a

1.5. Carta dos Direitos Fundamentais da União Europeia;

1.6. Indicadores de performance considerados em, pelo menos, no

1.6.1. Digital Economy and Society Index (DESI)

1.6.2. ITU Global Cybersecurity Index (GCI)

1.6.3. Institute for Management Development (IMD) World Digital Competitiveness Ranking

1.6.4. European Innovation Scoreboard

1.6.5. National Cyber Security Index

1.6.6. BSA EU Cybersecurity Maturity Dashboard

1.7. As principais referências legislativas e propostas para definição do quadro nacional e europeu, como

1.7.1. Lei orgânica do Gabinete Nacional de Segurança (Decreto Lei n.º 3/2012, de 16 de janeiro) Primeira alteração à Lei orgânica do Gabinete Nacional de Segurança (Decreto Lei n.º 162/2013, de 4 de dezembro)

1.7.1.1. Segunda alteração à Lei orgânica do Gabinete Nacional de Segurança estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança (Decreto Lei n.º 69/2014, de 9 de maio)

1.7.1.2. Terceira alteração à Lei orgânica do Gabinete Nacional de Segurança (Decreto Lei n.º 136/2017, de 6 de novembro)

1.7.2. Lei n.º 46/2018, de 13 de agosto - Regime Jurídico de Segurança do Ciberespaço

1.7.3. Estratégia Nacional de Segurança do Ciberespaço 2019-2023

1.7.4. Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro)

1.7.5. Lei de Segurança Interna (Lei n.º 53/2008, de 29 de Agosto)

1.7.6. Retificação à Lei de Segurança Interna (Declaração de Retificação n.º 66-A/2008, de 28 de outubro)

1.7.7. Primeira alteração à Lei de Segurança Interna (Lei n.º 59/2015, de 24 de junho)

1.7.8. Resolução do Conselho de Ministros n.º 50/88, de 3 de dezembro, que aprova as instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas (SEGNAC 1).

1.7.9. Declaração publicada no Diário da República, I Série, n.º 26, de 31 de janeiro, que retifica a RCM n.º 50/88, de 3 de dezembro.

1.7.10. Resolução do Conselho de Ministros n.º 13/93, de 6 de março, que altera a RCM n.º 50/88, de 3 de dezembro.

1.7.11. Resolução do Conselho de Ministros n.º 37/89, de 24 de outubro, que aprova as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação (SEGNAC 2).

1.7.12. Resolução do Conselho de Ministros n.º 16/94, de 22 de março, que aprova as instruções para a segurança nacional, segurança das telecomunicações (SEGNAC 3).

1.7.13. Resolução do Conselho de Ministros n.º 5/90, de 28 de fevereiro, que aprova as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança informática (SEGNAC 4).

1.7.14. Lei n.º 49/2009, de 5 de agosto, que regula as condições de acesso e exercício das atividades de comércio e indústria de bens e tecnologias militares.

1.7.15. Lei n.º 96/2015, de 17 de agosto, que regula a disponibilização e a utilização das plataformas eletrónicas de contratação pública.

1.7.16. Decreto-Lei n.º 116-A/2006, de 16 de junho, que procede à criação do Sistema de Certificação Eletrónica do Estado - Infraestrutura de Chaves Públicas e designa a ANS como autoridade credenciadora nacional (republicado).

1.7.17. Lei n.º 36/2003, de 22 de agosto, que estabelece normas de execução da decisão do Conselho da União Europeia que cria a EUROJUST, a fim de reforçar a luta contra as formas graves de criminalidade, e regula o estatuto e competências do respetivo membro nacional.

1.7.18. Lei n.º 20/2014, de 15 de abril, que procede à primeira alteração à Lei n.º 36/2003, de 22 de agosto.

1.7.19. Código Penal (aprovado pelo Decreto-Lei n.º 48/95, de 15 de março) - artigo 383.º.

1.7.20. Decreto-Lei n.º 12/2021 de 9 de fevereiro, que assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

1.7.21. Decreto do Presidente da República n.º 3/2000, de 6 de março, que ratifica o Acordo sobre a Segurança da Informação entre os Estados Parte do Tratado do Atlântico Norte, concluído em Bruxelas em 6 de março de 1997.

1.7.22. Resolução da Assembleia da República n.º 15/2000, de 6 de março, que aprova, para ratificação, o Acordo sobre a Segurança da Informação entre os Estados Parte do Tratado do Atlântico Norte, concluído em Bruxelas em 6 de março de 1997.

1.7.23. C-M(2002)49-REV1 Security within NATO (Public Disclosure - PDN(2021)0002), 20nov2020.

1.7.24. Decreto do Presidente da República n.º 152/2012, de 26 de setembro, que ratifica o Acordo entre os Estados membros da União Europeia, reunidos no Conselho, sobre a Proteção das Informações Classificadas Trocadas no Interesse da União Europeia, assinado em Bruxelas em 25 de maio de 2011.

1.7.25. Resolução da Assembleia da República n.º 125/2012, de 26 de setembro, que aprova o Acordo entre os Estados membros da União Europeia, reunidos no Conselho, sobre a Proteção das Informações Classificadas

Trocadas no Interesse da União Europeia, assinado em Bruxelas em 25 de maio de 2011.

1.7.26. Decisão n.º 2013/488/UE, do Conselho, de 23 de setembro, relativa às regras de segurança aplicáveis à Proteção das Informações Classificadas da UE.

1.7.27. Decisão (UE/EURATOM) n.º 2015/444, da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à Proteção das Informações Classificadas da UE.

1.7.28. Decisão n.º 2002/187/JAI, do Conselho, de 28 de fevereiro de 2002, relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade.

1.7.29. Decreto do Presidente da República n.º 12/2005, de 15 de fevereiro, que ratifica o Acordo entre os Estados Parte da Convenção para o Estabelecimento da Agência Espacial Europeia e a Agência espacial Europeia para a Proteção e Troca de Informação Classificada, feito em Paris em 9 de agosto de 2002.

1.7.30. Resolução da Assembleia da República n.º 8/2005, de 15 de fevereiro, que aprova, para ratificação, o Acordo entre os Estados Parte da Convenção para o Estabelecimento da Agência Espacial Europeia e a Agência espacial Europeia para a Proteção e Troca de Informação Classificada, feito em Paris em 9 de agosto de 2002.

1.7.31. Decisão n.º 1104/2011/UE, do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa às regras de acesso ao serviço público regulado oferecido pelo sistema mundial de radionavegação por satélite criado ao abrigo do programa GALILEO.

1.7.32. Regras de Segurança da Agência Espacial Europeia, REGULATIONS OF THE EUROPEAN SPACE AGENCY, Security Regulations, ESA/REG/004 of 18 January 2012 (versão em inglês).

1.7.33. Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019 relativo à ENISA (Agência da União Europeia para a

Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança).

1.7.34. Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa à segurança das redes e da informação em toda a União.

1.7.35. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

1.7.36. The European Data Strategy (COM(2020) 66 final, 19/02/2020)

1.7.37. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).

1.7.38. Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 - COM/2020/823 final.

R3. Específicos do Estudo

1. Com vista à concretização do Estudo que se pretende que demonstre a realidade organizacional Portuguesa e apresente uma análise fundamentada com uma análise, preferencialmente SWOT, das principais vantagens e desvantagens dos modelos organizacionais e estruturas de governação nas áreas da Segurança da Informação, da Informação Classificada e da Cibersegurança nos países considerados, com base na identificação de competências, atribuições e responsabilidades, e contextualizando os seus quadros de políticas públicas e dos

poderes de regulação, supervisão e execução (*enforcement*) que lhes estão atribuídos, deve proceder-se à execução das seguintes tarefas:

1.1. Planeamento do Estudo, que deverá considerar duas etapas (a designar por "Etapa 1" e "Etapa 2") perspetivando que:

1.1.1. O entregável, a definir, para a Etapa 1 seja desenvolvido até 30 dias após a adjudicação, salvo anuência expressa da Entidade Adjudicante para outro prazo que venha a ser proposto pela Entidade Adjudicatária;

1.1.2. O entregável da Etapa 2, i.e. a versão final do estudo, deve cumprir o prazo estabelecido em Cláusula 5ª da Parte I do Caderno de Encargos ("*A prestação de serviços a realizar no âmbito do contrato deverá ser executada até 60 dias após adjudicação* […]").

1.2. Para a Etapa 1 do Estudo:

1.2.1. Sob proposta da Entidade Adjudicatária e com aprovação pela Entidade Adjudicante, a definição das competências e categorias a identificar para a pesquisa nas áreas Segurança da Informação, da Informação Classificada e da Cibersegurança;

1.2.2. Sob proposta da Entidade Adjudicatária e com aprovação pela Entidade Adjudicante, a definição de critérios de análise para a Etapa 1 do Estudo;

1.2.3. Sob proposta da Entidade Adjudicatária e com aprovação pela Entidade Adjudicante, a identificação dos países a considerar na Etapa 1 do Estudo, e que deverá considerar uma amostra mínima de dois terços de países pertencentes à União Europeia, considerando-se para este efeito os países pertencentes ao Espaço Económico Europeu (EEE) e à Zona Europeia de Comércio Livre (EFTA);

1.2.4. Pela Entidade Adjudicatária, a recolha e análise da informação na Etapa 1 do Estudo com base nas competências identificadas e os modelos e estruturas de governação associados para as áreas da Segurança da Informação, da Informação Classificada e da Cibersegurança;

1.2.5. Pela Entidade Adjudicatária, a apresentação dos resultados da recolha e análise da informação para cada país identificado e para cada uma das áreas, nomeadamente a lista das competências, os modelos e estruturas

de governação identificados para cada área, identificando paralelos com o quadro organizacional de Portugal;

1.3. Para a Etapa 2 do Estudo:

1.3.1. Pela Entidade Adjudicante, a identificação, com base nos resultados apresentados na Etapa 1 do Estudo, de seis países a serem objeto de aprofundamento no Estudo;

1.3.2. Sob proposta da Entidade Adjudicatária e com orientação da Entidade Adjudicante, a revisão dos aspetos, critérios e/ou áreas a aprofundar ou desenvolver na Etapa 2 do Estudo;

1.3.3. Pela Entidade Adjudicatária, o aprofundamento da análise integrando uma análise, preferencialmente SWOT, tendo por base a informação recolhida na Etapa 1 e a informação que venha a ser identificada (em 1.3.2) como necessária para Etapa 2 do Estudo;

1.3.4. Apresentação da versão aceite do Estudo que demonstre a realidade organizacional Portuguesa e apresente uma análise através de uma análise, preferencialmente SWOT, detalhada e fundamentada, dos modelos organizacionais e estruturas de governação nas áreas da Segurança da Informação, da Informação Classificada e da Cibersegurança nos países considerados, tendo por base a identificação das competências, atribuições e responsabilidades, contextualizando os seus quadros de políticas públicas e dos poderes de regulação, supervisão e execução (*enforcement*).

2. A abordagem ao desenvolvimento do Estudo deve corresponder a uma perspetiva de análise isenta e adequada à realidade nacional e não seguir ou sugerir sem justificação qualquer solução específica preconcebida, a não ser quanto à observação dos parâmetros legalmente definidos. Nos casos em que se revele benéfico sugerir a adoção de modelos ou padrões de governação pré-estabelecidos como referência (por exemplo para efeitos de sugestão comparativa), esses padrões devem ser claramente identificados e justificados, devendo optar-se preferencialmente por padrões internacionalmente ou comummente aceites.

3. Deverá ser apresentada a metodologia de implementação que será utilizada na execução do projeto, devendo esta ser uma metodologia ágil, testada e comprovada, assegurando-se sprints no mínimo quinzenais.

4. Deverá ser indicada e descrita a metodologia a utilizar para todas as fases de execução do projeto, de forma a garantir a entrega do Estudo e demais documentação com a qualidade necessárias. Devem ser claramente indicadas as dependências entre as várias fases do projeto.

5. Deverá existir um Gestor de Projeto para este efeito, responsável por reportar a sua evolução à Entidade Adjudicante.

6. De acordo com a metodologia e planos apresentados, a Entidade Adjudicatária deverá indicar os recursos que pretende alocar, bem como a sua experiência profissional nessa área (conforme "R4. Perfis técnicos dos recursos humanos a afetar aos serviços").

7. Para este Estudo, a Entidade Adjudicatária deve apresentar, pelo menos, os seguintes documentos específicos:

7.1. Plano e calendário de ações para realização do estudo;

7.2. Quando existam, especificações técnicas e documentação anexa de referência, documentadas em suporte digital;

7.3. Metodologia de gestão de projeto, metodologia de elaboração do estudo e dados utilizados[2] em suporte digital;

7.4. Estudo na versão final aceite pela Entidade Adjudicante documentado em suporte digital.

8. Para efeitos deste Estudo, consideram-se níveis de serviço:

8.1. O entregável, a definir, para a Etapa 1 do Estudo, aceite pela Entidade Adjudicante até 30 dias após a adjudicação;

[2] Por dados utilizados entendem-se todos os dados primários utilizados para a realização do estudo, e todos os resultados ou produtos resultantes da atividade ou ação da Entidade Adjudicatária sobre esses dados, incluindo documentação sobre a recolha, seleção, tratamento e processamento dos dados e qualquer programa produzido pela Entidade Adjudicatária, incluindo o seu código-fonte, ou informação sobre programa produzido por entidade terceira que se revele necessário para aceder, ler, interpretar e reutilizar esses dados.

8.2. O entregável da Etapa 2 do Estudo, aceite pela Entidade Adjudicante até 60 dias após a adjudicação.

R4. Perfis técnicos dos recursos humanos a afetar aos serviços

1. A Entidade Adjudicatária deverá afetar à implementação da atividade contratada uma equipa de trabalho de acordo com a apresentada e definida na sua proposta nomeadamente quanto à estrutura e composição (número, perfil e identificação dos elementos, a afetar concretamente à realização dos trabalhos).

2. Deverá também adotar as responsabilidades associadas a cada perfil distinto, as etapas e tarefas da implementação em que os elementos com esse perfil participarão e o tipo de dedicação que terão (permanente ou parcial), conforme apresentado na sua proposta.

3. A Entidade Adjudicatária deverá disponibilizar e indicar uma equipa com pelo menos três elementos com mais de três anos de experiência na participação e/ou coordenação de equipas envolvidas em projetos de natureza semelhante, com os seguintes perfis e requisitos mínimos para execução do contrato:

3.1. Experiência anterior em Estudos de análise semelhantes;

3.2. Experiência na gestão de projetos tendo por base metodologias ágeis;

3.3. Formação superior e conhecimentos e competências comprovadas nas áreas relevantes para as matérias do estudo em questão, nomeadamente, mas não exclusivamente, em áreas de Engenharia, Economia, Gestão e Inovação, Sociologia das Organizações, Políticas Públicas, Políticas de Segurança, Tecnologias de Informação e Comunicação ou Direito;

3.4. Será valorizada a multidisciplinaridade ao nível formação superior ou experiência e conhecimento na equipa.

4. Qualquer alteração à composição da equipa indicada em sede de adjudicação deve ser previamente comunicada à Entidade Adjudicante e só será aceite se reunir os requisitos mínimos exigidos no número anterior, podendo, para o efeito, ser

solicitada informação e documentação adicional para confirmação dos elementos curriculares apresentados.

5. A substituição referida no número anterior deverá ocorrer da seguinte forma:

5.1. A Entidade Adjudicatária, em 5 dias úteis, identifica e notifica a Entidade Adjudicante acerca do seu melhor recurso considerando os requisitos mínimos exigidos e obtém a sua aceitação para o fim de substituição referido;

5.2. A Entidade Adjudicatária deverá assegurar que nos 5 dias úteis após a aceitação o recurso inicia a prestação do serviço.

6. Sempre que se constate a inadequação de algum elemento da equipa encarregue da execução dos serviços contratados, tendo em conta os requisitos exigidos e o comportamento comummente expectável, a Entidade Adjudicante poderá exigir a sua substituição, aplicando-se, com as devidas adaptações, o disposto nos números anteriores.

ANEXO II

AQUISIÇÃO DE ESTUDO DE IDENTIFICAÇÃO DE ATRIBUIÇÕES E COMPETÊNCIAS DE PAÍSES NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO, DA INFORMAÇÃO CLASSIFICADA E DA CIBERSEGURANÇA

OBRIGAÇÕES DE SEGURANÇA

1. Pela aceitação do contrato e desenvolvimento das atividades relacionadas com o presente procedimento, a Entidade Adjudicatária, assim como todas as entidades por ela subcontratadas ou pessoas que com ela colaborem no âmbito do procedimento, encontram-se obrigadas a cumprir com as presentes Obrigações de Segurança, regulamentos e demais legislação emanada pela Autoridade Nacional de Segurança ou do âmbito da proteção do segredo, nos termos dos artigos 4.º e 5.º das normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação (SEGNAC 2), aprovadas pela Resolução do Conselho de Ministros n.º 37/89, de 24 de outubro, e a Resolução do Conselho de Ministros n.º 50/88, de 3 de dezembro, que aprova as instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas (SEGNAC 1).

2. Toda a informação classificada no âmbito do procedimento e atividades relacionadas deverá ser protegida de acordo com as normas e regulamentos aplicáveis à segurança da informação classificada da marca e grau correspondente à classificação de segurança do procedimento.

3. Em particular, a Entidade Adjudicatária encontra-se obrigada a:
    a. Designar Encarregado de Segurança do Projeto (ESP) que deverá ser o responsável pela supervisão e aplicação das medidas de segurança adequadas ao procedimento e atividades relacionadas, de acordo com a classificação de segurança aplicável.

b. Submeter ou diligenciar atempadamente, quando necessário e junto do Gabinete Nacional de Segurança, a credenciação das entidades ou pessoas referidas anteriormente quando o grau de informação classificada for superior ou igual a CONFIDENCIAL.
c. Manter, preferencialmente através do ESP, a Entidade Adjudicante informada de todos os aspetos e assuntos relacionados com a segurança da informação relacionada com o procedimento.
d. Limitar ao mínimo necessário a produção de cópias ou disseminação da informação relacionada com o procedimento, no respeito pelas normas de manuseamento da informação classificada.
e. Fornecer atempadamente à Entidade Adjudicante todas as informações pessoais relativas às pessoas ou entidades subcontratadas que intervêm no procedimento e têm acesso a informação classificada nesse âmbito.
f. Manter uma lista atualizada das pessoas e entidades subcontratadas que têm acesso a informação classificada no âmbito do procedimento, com indicação do grau de credenciação e validade.
g. Assegurar a negação de acesso a informação classificada do procedimento a pessoas ou entidades que não tenham necessidade de intervir ou produzir qualquer atividade nesse âmbito e que não possuam a necessária credenciação de segurança.
h. Garantir que todas as pessoas que, de alguma forma, intervenham ou tenham acesso a informação classificada no âmbito do procedimento, são conhecedoras das suas obrigações e deveres processuais, regulamentares e legais no manuseamento de informação classificada. Neste âmbito, o ESP deverá garantir que as pessoas referidas assinam uma declaração de compromisso atestando esse facto.
i. Reportar ao Responsável de Segurança do Projeto da Entidade Adjudicante (RSP), no mais curto espaço de tempo possível e pelo meio mais expedito, qualquer violação de segurança da informação classificada, de facto ou presumida, associada ao procedimento, à quebra de confiança em pessoa ou entidade subcontratada ou a equipamento/serviço tecnológico ou outro associado ao desenvolvimento de qualquer atividade no âmbito do referido procedimento.

j. Obter um parecer prévio do RSP no que respeita à seleção ou subcontratação de pessoa ou entidade que deva ter acesso a informação classificada do procedimento.
k. Assegurar que todos os resultados da produção de atividades no âmbito do presente procedimento não são utilizados, reutilizados, cedidos, aplicados ou divulgados, no todo ou em parte, para fins que não os previstos no contrato de prestação de serviços com o Adjudicante, sem a prévia autorização expressa do RSP.
l. Assegurar a destruição segura, a todo o tempo e nos termos das normas aplicáveis à respetiva classificação de segurança, de toda a informação que não seja absolutamente necessário preservar e que não seja essencial para a produção das atividades contratadas.

4. Todas as entidades ou pessoas subcontratadas, que colaborem com a Entidade Adjudicatária no âmbito do presente procedimento, encontram-se obrigadas a possuir a necessária credenciação de segurança, com a marca e grau aplicável à classificação de segurança do procedimento com âmbito de aplicação e duração temporal limitada aos fins da prestação de serviços não sendo válida para quaisquer outras finalidades ou utilização diversa.

5. À Entidade Adjudicatária não é permitida, a todo o tempo e sem para tal estar autorizada, a divulgação a terceiros de informação classificada do âmbito do procedimento, no prosseguimento das suas tarefas e atividades de contratação, aquisição ou qualquer outra forma de relacionamento comercial com essas entidades terceiras.

6. À Entidade Adjudicatária não é permitida a alteração da classificação de segurança do procedimento e de qualquer informação ou artefacto associado ao mesmo, em termos de marca e grau, sem a autorização expressa do RSP.

7. Não será utilizado qualquer sistema ou instalação física que não obedeça aos requisitos de certificação e segurança associados à classificação de segurança do procedimento.

8. A Entidade Adjudicatária deve destruir ou devolver qualquer informação classificada fornecida ou gerada de acordo com o contrato, a menos que a Entidade Adjudicante tenha aprovado por escrito a retenção de tais informações classificadas, por exemplo, para fins de garantia.

9. A violação de qualquer das obrigações referidas no presente documento ou de qualquer norma aplicável ao manuseamento de informação classificada, resultará na cessação imediata do contrato e das atividades desenvolvidas ou a desenvolver no âmbito do procedimento, sem prejuízo de outras penalidades ou responsabilidades que possam ser aplicáveis por força da regulamentação e legislação aplicável.

10. A Entidade Adjudicatária reconhece, aceita e compreende todas as obrigações e requisitos de segurança constantes nas presentes Obrigações de Segurança.