



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

CONSULTA PRÉVIA

CADERNO DE ENCARGOS

**DESENVOLVIMENTO DE RELATÓRIO SOBRE OS SETORES DOS OPERADORES DE
SERVIÇOS ESSENCIAIS: CARACTERIZAÇÃO, REGULAMENTAÇÃO E
RECOMENDAÇÕES, NO ÂMBITO DO OBSERVATÓRIO DE CIBERSEGURANÇA**



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

CADERNO DE ENCARGOS
PARTE I – DO CONTRATO

Cláusula 1ª

Objeto Da Consulta Prévia

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 serviços de DESENVOLVIMENTO DE RELATÓRIO SOBRE OS SETORES DOS OPERADORES DE SERVIÇOS ESSENCIAIS: CARACTERIZAÇÃO, REGULAMENTAÇÃO E RECOMENDAÇÕES, NO ÂMBITO DO OBSERVATÓRIO DE CIBERSEGURANÇA, de acordo com as Cláusulas Técnicas descritas no Anexo I da Parte II do Caderno de Encargo.

Cláusula 2ª

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 – Presidência de Conselho de Ministros – Centro Nacional de Cibersegurança;

Adjudicatário – entidade a quem se adjudica a execução do contrato.

Cláusula 3ª

Forma e documentos contratuais

1. Fazem parte integrante do contrato os seguintes documentos:
 - a) Os suprimimentos dos erros e omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) Os esclarecimentos e as retificações relativos ao caderno de encargos;
 - c) O presente caderno de encargos;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos à proposta adjudicada prestados pelo adjudicatário.



PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

2. Em caso de divergência entre os documentos referidos no n.º 1, a prevalência é determinada pela ordem que nele se dispõe.
3. Em caso de divergência entre os documentos referidos no n.º 1 e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos ao conteúdo do contrato propostos pelo órgão competente para a decisão de contratar e aceites pelo adjudicatário.

Cláusula 4ª

Local de Prestação dos Serviços

A prestação de serviços, objeto deste contrato, deverá ser efetuada nas instalações do Adjudicatário e entregues no Centro Nacional de Cibersegurança (CNCS), sito na Rua da Junqueira N.º69, 1300-342 Lisboa.

Cláusula 5ª

Prazo e vigência do contrato

1. O prazo de execução final é de cento e oitenta (180) dias seguidos contados a partir da data de adjudicação do contrato, não sendo admitido prazo inferior a trinta (30) dias seguidos contados a partir desta mesma data.

Cláusula 6ª

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 cento e trinta e cinco mil euros (135 000€), 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 7ª

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 a 20% do preço base e contratual definido na cláusula 6ª do presente Caderno de Encargos, conforme consta também no Convite da Consulta Prévia.

Cláusula 8ª

Pagamento e condições de pagamento

1. As quantias devidas pelo 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 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.



PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

4. Nas condições de pagamento a apresentar pelos concorrentes, não podem ser propostos adiantamentos.

Cláusula 9ª

Caução

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

Cláusula 10ª

Requisitos sobre a execução do serviço

1. Após 7 dias da adjudicação do presente Caderno de Encargos, a entidade adjudicatária deverá reunir-se com o CNCS para validação da boa compreensão do serviço adjudicado e dos requisitos apresentados no presente Caderno de Encargos.
2. A entidade adjudicatária deverá informar o CNCS, semanalmente, do desenvolvimento do seu trabalho, para validação do bom andamento do projeto.
3. Sempre que necessário, o CNCS 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. Estas reuniões podem ser realizadas por videoconferência.
4. Caso se verifique ser necessário o agendamento de reuniões de trabalho envolvendo outras entidades que possam contribuir para o Desenvolvimento de Relatório sobre os Setores dos Operadores de Serviços Essenciais: Caracterização, Regulamentação e Recomendações, no Âmbito do Observatório de Cibersegurança (por exemplo, o Conselho Consultivo do Observatório de Cibersegurança), as mesmas deverão ser objeto de informação prévia ao CNCS, para efeitos de agendamento, acompanhamento ou moderação, entre outros.
5. A necessidade das reuniões de trabalho acima referidas poderá ser suscitada pelo adjudicatário, pelo CNCS ou por uma entidade interessada.

Cláusula 11ª

Transferência da propriedade

1. Todos os elementos/documentos produzidos pelo adjudicatário ao abrigo do presente procedimento passam a ser propriedade da entidade adjudicante, incluindo os direitos autorais sobre todas as eventuais criações intelectuais abrangidas pelos serviços a prestar.
2. Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente procedimento.



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

Cláusula 12ª

Dever de sigilo

1. O adjudicatário 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 da entidade adjudicante 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.

Cláusula 13ª

Penalidades

1. No caso de incumprimento dos prazos fixados no contrato e por causa imputável ao adjudicatário, poderá ser aplicada uma penalidade, calculada de acordo com o seguinte modo: por cada semana de atraso (7 dias) em relação aos prazos referidos na cláusula 5ª deste caderno de encargos, o valor a pagar ao adjudicatário reduz um oitavo (1/8).
2. No caso de o adjudicatário incumprir nos prazos fixados em mais de 30 dias, o GNS pode resolver o contrato, a título sancionatório, passando a vigorar a proposta classificada em segundo lugar.

Cláusula 14ª

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.



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

Cláusula 15ª

Cessão da posição contratual

1. O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da entidade adjudicante.
2. Para efeitos da autorização prevista no número anterior, deve:
 - a) Ser apresentada pelo cessionário toda a documentação exigida ao adjudicatário na presente consulta prévia;
 - b) A entidade adjudicante deverá apreciar, designadamente, se o cessionário 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 16ª

Responsabilidade do Adjudicatário

1. O adjudicatário responde pelos danos que causar à entidade contratante em razão do incumprimento culposo das obrigações que sobre ele impendam.
2. O adjudicatário responde ainda perante a entidade contratante 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.

Cláusula 17ª

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 anexada ao contrato inicial.

Cláusula 18ª

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 de funcionamento divergentes face à especificação funcional definida.

Cláusula 19ª

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.



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

Cláusula 20ª

Contagem dos Prazos

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

Cláusula 21ª

Legislação aplicável

O contrato é regulado pela legislação portuguesa.



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança
PARTE II – CLÁUSULAS TÉCNICAS

Cláusula Única

Caracterização dos serviços a prestar e especificações técnicas

As características dos serviços a prestar e especificações técnicas são as que se indicam no Anexo I:

- ANEXO I: DESENVOLVIMENTO DE RELATÓRIO SOBRE OS SETORES DOS OPERADORES DE SERVIÇOS ESSENCIAIS: CARACTERIZAÇÃO, REGULAMENTAÇÃO E RECOMENDAÇÕES, NO ÂMBITO DO OBSERVATÓRIO DE CIBERSEGURANÇA



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança
ANEXO I

**DESENVOLVIMENTO DE RELATÓRIO SOBRE OS SETORES DOS OPERADORES
DE SERVIÇOS ESSENCIAIS: CARACTERIZAÇÃO, REGULAMENTAÇÃO E
RECOMENDAÇÕES, NO ÂMBITO DO OBSERVATÓRIO DE CIBERSEGURANÇA**

A. REQUISITOS GERAIS

Considerando a Lei n.º 46/2018¹, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa a *medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*, o Centro Nacional de Cibersegurança deve *garantir que o País usa 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*.

E considerando os termos da Estratégia Nacional de Segurança do Ciberespaço 2019-2023² (ENSC), aprovada em Conselho de Ministros, no dia 23 de maio de 2019, e publicada através da resolução nº 92/2019, de 5 de junho de 2019, que define seis eixos de intervenção.

Decorre a necessidade de identificar o estado da cibersegurança em Portugal em vários domínios disciplinares e societais, com vista a acompanhar a execução e a avaliar o impacto desta mesma estratégia na sociedade, bem como a compreender a situação concreta da cibersegurança no país nas várias esferas em que incide, solicitando-se para o efeito a realização de um Relatório sobre os Setores dos Operadores de Serviços Essenciais: caracterização, regulamentação e recomendações (ROSE), no âmbito do Observatório de Cibersegurança. O ROSE deverá responder à referida necessidade mensurando o estado da cibersegurança nacional no que diz respeito aos diversos setores dos operadores de serviços essenciais (OSE) designados no RJSC.

O Observatório de Cibersegurança³ visa observar o fenómeno da cibersegurança em Portugal, nas suas mais variadas componentes, de modo a informar

¹ <https://dre.pt/home/-/dre/116029384/details/maximized>

² <https://dre.pt/web/guest/home/-/dre/122498962/details/maximized>

³ <https://www.cncs.gov.pt/pt/observatorio/>



PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

as partes interessadas e a suportar a definição de políticas públicas. O Observatório de Cibersegurança tem como missão ser uma plataforma de análise e sistematização de conhecimento, bem como de debate, em torno de temas multidisciplinares da cibersegurança, identificando tendências com referências temporais e articulando as várias partes interessadas na recolha de informação.

B. DEFINIÇÕES

No âmbito do presente documento consideram-se relevantes as definições contidas na Lei n.º 46/2018, de 13 de agosto, que define o RJSC, as comumente constantes na literatura técnica e normativa no âmbito da segurança das redes e dos sistemas de informação, bem como as que são expressas na ENSC. Devem ainda ser consideradas as disposições técnicas contidas no Decreto-Lei n.º 65/2021, de 30 de julho que regulamenta o RJSC e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019, e toda a regulamentação complementar ao RJSC, como o Regulamento n.º 183/2022, de 21 de fevereiro, que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança⁴.

C. REQUISITOS MÍNIMOS DOS ENTREGÁVEIS

O ROSE deverá integrar documentação que retrate os diversos setores dos OSE designados no RJSC e necessariamente incluir um documento base aprofundado e tematicamente transversal e um caderno simplificado por cada setor suscetível de constituir um guia a entregar aos OSE. Este retrato deve considerar as seguintes orientações:

1. Esta documentação deve incluir (pelo menos):

- a) Elementos de contexto: as dimensões económicas, sociais e técnicas destes setores em termos genéricos, mas sobretudo no que à cibersegurança diz respeito, nomeadamente identificando o estado dos seus indicadores de transição digital críticos para a segurança do ciberespaço;

⁴ <https://www.cncs.gov.pt/pt/regime-juridico/>



PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

- b) Ameaças: o tipo de ameaças no ciberespaço que mais afetam cada setor e construção dos respectivos cenários de risco;
- c) Capacitação: o histórico de capacitação em cibersegurança de cada setor;
- d) RJSC e legislação setorial: as especificidades e o nível de adaptação no que se refere ao RJSC e respetiva regulamentação de cada setor, além da evolução legislativa própria do setor e articulações dessa legislação com o RJSC;
- e) Investimento em cibersegurança: análise ao investimento realizado em cibersegurança por cada setor;
- f) Recomendações: conselhos, com base na análise, para cada um dos setores, numa lógica de melhoria contínua.

1.1. Especificidades de cada um dos aspetos a retratar, referidos de “a” a “f” do ponto 1:

- a) Elementos de contexto:

Contextualização de cada setor dos OSE na economia nacional, identificando os seus fatores de impacto na sociedade e as suas especificidades tecnológicas. Esta contextualização deverá colocar o setor numa linha de progressão da transição digital e seus indicadores, incluindo o seu grau de exposição às ameaças no ciberespaço. Tal análise deverá ser suportada por comparações com congéneres setoriais internacionais, privilegiando países da União Europeia (UE).
- b) Ameaças:

Identificação das principais ciberameaças que, com maior ou menor tipicidade, afetam cada setor, tendo em conta dados internacionais, mas também os nacionais, nomeadamente os produzidos no contexto do Observatório de Cibersegurança do CNCS, os quais deverão ser aprofundados e mais detalhados relativamente aos setores em causa. Esta análise deverá seguir as taxonomias adotadas pelo Observatório de Cibersegurança quanto a agentes de ameaça e ciberameaças, bem como o modelo de análise de risco disponibilizado pelo CNCS. Dever-se-á ainda definir uma metodologia de recolha e análise de dados que permita no futuro essa ser regular.



PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

c) Capacitação:

Descrição da cronologia dos momentos-chave de capacitação em cibersegurança de cada setor, tendo em conta três vertentes: humana, tecnológica e de processos. Esta análise deverá considerar os esforços de capacitação, mas também as evidências existentes relativamente aos seus resultados.

d) RJSC e legislação setorial:

Análise do impacto do RJSC e respetiva regulamentação em cada setor, em termos jurídicos, organizacionais e práticos, bem como dos principais desafios que se identificam a esse respeito, aspetos que também devem ser apreciados de forma comparativa com países da UE com contextos equiparáveis. Esta análise deve estabelecer uma constante articulação com a legislação setorial, identificando os casos em que cada quadro legislativo se sobrepõe ao outro ou quando explícita e implicitamente se interligam, intertextualmente;

e) Investimento em cibersegurança:

Análise ao investimento que cada setor realizou em cibersegurança, estimando a evolução temporal do mesmo, identificando as áreas da cibersegurança nas quais esse investimento foi aplicado e indicando as áreas mais carentes a este nível;

f) Recomendações:

Apresentação de conselhos sobre as melhores práticas a aplicar em cada setor com base nos vários aspetos analisados nos pontos anteriores. Estas recomendações devem estar organizadas em 4 tipos: técnicas, comportamentais, de conformidade com referenciais e de aplicação da legislação. Estas recomendações devem dar orientações para a conformidade com o RJSC.

2. Abordagem metodológica na construção do documento:

Os dados utilizados para a análise dos diversos elementos de caracterização dos setores dos OSE devem ser recolhidos nos seguintes tipos de fontes, tendo em conta as especificidades elencadas no ponto 1.1.:

- a) em fontes estatísticas abertas - nomeadamente estatísticas de entidades como o Instituto Nacional de Estatística, o Eurostat, o Eurobarómetro ou o Pordata (na



PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

medida em que coleta dados disponíveis) - que resultem de entidades reconhecidas como credíveis na produção de dados estatísticos e científicos;

- b) em documentação de especialistas, nomeadamente em cibersegurança e/ou nos setores em causa, como artigos científicos, relatórios ou documentos de outra natureza, desde que da responsabilidade dos referidos especialistas;
- c) em documentação de instituições reconhecidas no âmbito da cibersegurança e/ou dos setores em causa;
- d) em produção própria desenvolvida para o efeito, nomeadamente através de inquéritos, entrevistas, análise de conteúdo ou outras metodologias consideradas científicas e aceites pelo CNCS.

3. Formato, impressão e tradução:

O ROSE deverá apresentar as seguintes características de forma:

- a) Deverá ter coerência enquanto documento único, mas subdividir-se em tantos relatórios parcelares simplificados quanto o número de setores dos OSE, devendo cada relatório parcelar dedicar-se especificamente a cada um dos setores dos OSE.
- b) Deverá ter uma apresentação gráfica apelativa que utilize gráficos, figuras e/ou outro tipo de imagens de modo a providenciar uma leitura acessível. O *design* deverá ter um nível profissional e considerar a identidade visual dos documentos já publicados pelo Observatório de Cibersegurança do CNCS.
- c) O documento deverá integrar, em modo concretamente a definir, uma súmula adequada a uma leitura em cerca de quinze minutos.
- d) Além da versão em português, deverá ter uma versão em inglês (Reino Unido).
- e) Além de haver um formato digital, deverá haver um formato impresso, com 600 exemplares a cores, 300 da versão em português e 300 da versão em inglês.
- f) A circunstância de parte do ROSE poder ser tida como reservada — i.e., não pública — não prejudica as obrigações decorrentes das alíneas anteriores.