



PRESIDÊNCIA DO CONSELHO DE MINISTROS

**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

## **CADERNO DE ENCARGOS**

**AQUISIÇÃO DE SERVIÇOS PARA ELABORAÇÃO DE ESQUEMA DE CERTIFICAÇÃO  
DA CONFORMIDADE COM O QUADRO NACIONAL DE REFERÊNCIA PARA A  
CIBERSEGURANÇA**



PRESIDÊNCIA DO CONSELHO DE MINISTROS

**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

## **CADERNO DE ENCARGOS**

### **PARTE I**

#### **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 serviços para elaboração de esquema de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança**, no âmbito da competência de desenvolvimento de esquemas nacionais específicos de certificação da cibersegurança atribuída à Autoridade Nacional de Certificação da Cibersegurança, conforme previsto no **Art.º20 do Decreto-Lei n.º 65/2021, de 30 de julho**, de acordo com as Cláusulas Técnicas descritas no Anexo I 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 – Presidência de Conselho de Ministros – Gabinete Nacional de Segurança / Centro Nacional de Cibersegurança;

Entidade adjudicatária – entidade a quem se adjudica a execução do contrato.

#### **Cláusula 3**

##### **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 pela entidade adjudicatária.
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 pela entidade adjudicatária.

#### **Cláusula 4**

##### **Local de Prestação dos Serviços**

1. A prestação de serviços objeto deste contrato será executada, preferencialmente, nas instalações da entidade adjudicante, sita na Rua da Junqueira Nº 69, 1300-342, Lisboa, ou em modo remoto a partir das instalações da entidade adjudicatária ou outras consideradas como convenientes, quando tal seja preferível tendo em conta a natureza da atividade concreta a desenvolver.
2. O disposto no número anterior não prejudica a manutenção das obrigações acessórias que tenham sido estabelecidas a favor da entidade adjudicante, incluindo as de confidencialidade e garantia.

#### **Cláusula 5**

##### **Prazo e vigência do contrato**

A prestação de serviços a realizar no âmbito do contrato deverá ser executada até 20 de dezembro de 2021, 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 6**

##### **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 € (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.
3. O preço base constante no número 1 corresponde ao preço máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do contrato a celebrar.
4. Não haverá lugar à revisão de preços durante a vigência do contrato.



## **Cláusula 7**

### **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 8**

### **Pagamento e condições de pagamento**

1. Face ao preço contratual, e considerando o prazo de vigência do contrato a celebrar, será realizado um pagamento do valor total contratual com entrada em vigor do contrato.
2. As quantias devidas pelo GNS / CNCS serão pagas no prazo de 30 dias após a receção da fatura e vencimento da obrigação respetiva.
3. Para os efeitos do número anterior, a obrigação considera-se vencida após a aceitação, pelo GNS / CNCS, do objeto do contrato em causa.
4. Para efeitos dos pagamentos referidos nos números anteriores, em caso de discordância por parte da entidade adjudicante quanto aos valores indicados nas faturas, deve esta comunicar à entidade adjudicatária, por escrito, os respetivos fundamentos, ficando este último obrigado a prestar os esclarecimentos devidos ou proceder à emissão de nova fatura corrigida ou da correspondente nota de débito/crédito.
5. Desde que devidamente emitida e observado o disposto no n.º 1, a fatura é paga através de transferência bancária.
6. Nas condições de pagamento a apresentar pelos concorrentes não podem ser propostos adiantamentos.

## **Cláusula 9**

### **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 10**

### **Dever de sigilo e confidencialidade**

1. Informação Confidencial é, para os efeitos restritos deste contrato, toda a informação revelada no âmbito dos projetos, seja sob qualquer forma (incluindo, mas não se limitando a, revelações feitas por escrito, oralmente ou sob a forma de dados pessoais, amostras, desenhos, planos, modelos, aplicações e programas informáticos no formato de código fonte ou código objeto,



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

especificações, segredos comerciais, métodos e fórmulas, contratos de financiamento e situações internas, de natureza laboral ou outra, ou qualquer outra forma) pela entidade adjudicante para os fins ou em conexão com o objeto do Acordo.

2. 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.
3. 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.
4. A entidade adjudicatária 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. 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.
6. A entidade adjudicatária 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.
7. 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.
8. 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



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

sua execução, sendo esta obrigação extensível a outras partes, colaboradores ou terceiros que as mesmas envolvam, mesmo depois do término do presente contrato.

### **Cláusula 11**

#### **Patentes, licenças e marcas registradas**

1. A entidade adjudicatária garante que respeita as normas relativas à propriedade intelectual e industrial, designadamente, direitos de autor, licenças, patentes e marcas registradas relacionadas com o hardware, software e documentação técnica que utilizam no desenvolvimento da sua atividade.
2. São da responsabilidade da entidade adjudicatária quaisquer encargos decorrentes da utilização de marcas registradas, patentes registradas ou licenças.
3. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, a entidade adjudicatária terá de a indemnizar de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar.
4. Sempre que legalmente admissível e na máxima extensão admitida na lei, o resultado da prestação dos serviços será registado a favor da entidade adjudicante, em sede de direito de propriedade industrial e/ou de propriedade intelectual, conforme o caso, ainda que se verifique a cessação do contrato por qualquer motivo.
5. A entidade adjudicatária obriga-se a colaborar e a prestar assistência à entidade adjudicante, relativamente aos procedimentos e às formalidades necessárias para a realização dos referidos registos.

### **Cláusula 12**

#### **Proteção de Dados Pessoais**

1. A entidade adjudicatária deverá apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma a que o tratamento de dados satisfaça os requisitos do RGPD – Regulamento (UE) 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. 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.



3. 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 accidental ou ilícita, perda accidental, alterações, difusão ou acesso não autorizados, e contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.
  - e) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade.
4. Se quaisquer dados se perderem ou forem danificados no âmbito da execução do Contrato, por causas imputáveis à entidade adjudicatária, este compromete-se a adotar as medidas que forem necessárias com vista à recuperação dos dados, sem quaisquer custos adicionais.

### **Cláusula 13**

#### **Penalidades**

- 1. No caso de incumprimento dos prazos fixados no contrato até 15 dias corridos e por causa imputável à entidade adjudicatária, poderá ser aplicada uma penalidade que representará  $1/500$  do custo da proposta adjudicada pelo total de dias úteis de atraso ( $P = \sum(Du) \times Pc/500$ ), em que (P) corresponde ao montante da penalidade, (Du) representa o total de dias corridos de atraso e (Pc) representa o custo da proposta adjudicada.
- 2. No caso de incumprimento dos prazos fixados no contrato em mais do que 15 dias corridos e por causa imputável à entidade adjudicatária, poderá ser aplicada uma penalidade que representará  $1/250$  do custo da proposta adjudicada pelo total de dias úteis de atraso ( $P = \sum(Du) \times Pc/250$ ), em que (P) corresponde ao montante da penalidade, (Du) representa o total de dias corridos de atraso após os 15 dias corridos referidos e (Pc) representa o custo da proposta adjudicada.
- 3. No caso de a entidade adjudicatária incumprir nos prazos fixados em mais de 30 dias úteis após os 15 dias corridos referidos em 1. da presente cláusula, a entidade adjudicante pode resolver o



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

contrato a título sancionatório, passando a vigorar a proposta classificada em segundo lugar ou, quando não a haja, sendo resolvido o contrato nos termos da cláusula 15.

4. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida nota de crédito.

#### **Cláusula 14**

##### **Força maior**

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, for impedida de cumprir as obrigações assumidas no contrato.
2. Entende-se por caso fortuito ou de força maior qualquer situação ou acontecimento imprevisível e excecional, independente da vontade das partes, e que não derive de falta ou negligência de qualquer delas.
3. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
4. A parte que invocar uma causa de força maior deve imediatamente, informar a outra da respetiva ocorrência e empenhar os seus melhores esforços para limitar as consequências daí decorrentes.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante de força maior.

#### **Cláusula 15**

##### **Resolução por parte do contraente público**

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, bem como de outras situações de grave violação das obrigações contratuais assumidas pelo Entidade adjudicatária, o GNS / CNCS 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 ou nos seguintes casos:
  - a) Incumprimento reiterado pela entidade adjudicatária das obrigações que decorrem do presente Contrato ou que dele resultem, sem prejuízo da aplicação do artigo 318.º-A do Código dos Contratos Públicos;
  - b) Prossecução deficiente do objeto do contrato por parte da entidade adjudicatária.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada à entidade adjudicatária.





3. A cessação dos efeitos do contrato não prejudica a verificação da responsabilidade civil ou criminal por atos ocorridos durante a execução da prestação.
4. Em caso de resolução do contrato a entidade adjudicatária é obrigado a entregar de imediato toda a documentação e informação, independentemente da forma que esta revista, produzida no âmbito do contrato e que esteja em sua posse, a qual é, para todos os efeitos, propriedade exclusiva da entidade adjudicante.

### **Cláusula 16**

#### **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 à entidade adjudicatária 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;
  - c) São impostas ao cessionário ou à entidade subcontratante as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato entre o GNS / CNCS e a entidade adjudicatária, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos do presente regulamento.
  - d) Em caso de violação das obrigações em matéria de proteção de dados pelo subcontratante, a entidade adjudicatária continua a ser plenamente responsável, perante o GNS / CNCS, pelo cumprimento das obrigações desse subcontratante.

### **Cláusula 17**

#### **Responsabilidade e Obrigações principais da Entidade Adjudicatária**

1. Sem prejuízo de outras obrigações previstas no caderno de encargos, nas cláusulas contratuais ou na legislação aplicável, da celebração do contrato decorrem para a entidade adjudicatária as seguintes obrigações principais para com a entidade adjudicante:



- a) Manutenção das condições de prestação de fornecimento, incluindo as premissas técnicas do mesmo descritas nas especificações técnicas do caderno de encargos;
  - b) Comunicação antecipada dos factos que tornem total ou parcialmente impossível o fornecimento dos bens ou a prestação do serviço ou o cumprimento de qualquer outra obrigação, nos termos do contrato;
  - c) Prestação de forma correta e fidedigna das informações referentes às condições em que é prestado o fornecimento, bem como prestação de todos os esclarecimentos que sejam solicitados;
  - d) Não ceder a sua posição contratual no contrato celebrado com a entidade adjudicante, sem autorização prévia desta;
  - e) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenham no âmbito da formação e da execução do Contrato, 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.
2. A entidade adjudicatária responde pelos danos que causar à entidade contratante em razão do incumprimento culposos das obrigações que sobre ele impendam.
3. A entidade adjudicatária 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.
4. A entidade adjudicatária aceita e compromete-se a cumprir com as Obrigações de Segurança constantes da Clausula 2ª da Parte II – Clausulas Técnicas, do presente Caderno de Encargos.

## **Cláusula 18**

### **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 19**

### **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 20**

### **Níveis de serviço**

A especificação dos níveis de serviço é efetuada no Anexo I - Especificações Técnicas | Elaboração de esquema de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança.

## **Cláusula 21**

### **Documentação e entregáveis**

A especificação da documentação e entregáveis é efetuada no Anexo I - Especificações Técnicas | Elaboração de esquema de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança.

## **Cláusula 22**

### **Perfis técnicos dos recursos a afetar aos serviços**

1. A entidade adjudicatária deverá afetar à implementação uma equipa de trabalho de acordo com a apresentada 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 especificação dos perfis técnicos dos recursos a afetar é efetuada no Anexo I - Especificações Técnicas | Elaboração de esquema de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança.

## **Cláusula 23**

### **Substituição das equipas**

1. Qualquer alteração à composição da(s) equipa(s) indicada(s) em sede de adjudicação deve ser previamente comunicada à entidade adjudicante e só será aceite se reunir os requisitos mínimos exigidos na cláusula anterior, podendo, para o efeito, ser solicitada informação e documentação adicional para confirmação dos elementos curriculares apresentados.
2. A substituição referida no número anterior deverá ocorrer da seguinte forma:
  - a) A entidade adjudicatária, em 5 dias úteis, deverá identificar o seu melhor recurso considerando os requisitos mínimos exigidos e obter a aceitação pela entidade adjudicante;
  - b) A entidade adjudicatária deverá assegurar que nos 5 dias úteis após a aceitação o recurso inicia a prestação do serviço.



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

3. 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 comumente expectável, a entidade adjudicante poderá exigir a sua substituição, aplicando-se, com as devidas adaptações, o disposto nos números anteriores.

#### **Cláusula 24**

##### **Critério de circularidade**

A entidade adjudicante adota as orientações para uma política de impressão ambientalmente responsável na Administração Pública, de acordo com a Resolução do Conselho de Ministros n.º 51/2017, de 19 de abril, principalmente uma mudança de cultura e de práticas que promovam processos de trabalho e de comunicação mais orientados aos objetivos das organizações e ao próprio serviço público: procedimentos desmaterializados, móveis, acessíveis e mais simples, quer dentro e entre a própria Administração Pública, quer entre esta e os cidadãos ou empresas.

#### **Cláusula 25**

##### **Requisitos de Natureza Social e Ambiental**

Na execução do contrato, a entidade adjudicatária deve garantir o cumprimento das normas ambientais aplicáveis, devendo ainda garantir a sua adequação a novas normas ou exigências que entrem em vigor no período de vigência do contrato, diretamente relacionadas com o objeto do contrato.

#### **Cláusula 26**

##### **Gestor do contrato**

1. A entidade adjudicante designará gestor do contrato, com a função de acompanhar permanentemente a execução contratual nos termos e para os efeitos do artigo 290-A do CCP.
2. Caso o gestor do contrato detete desvios, defeitos ou outras anomalias na execução do contrato, deverá comunicá-los de imediato à entidade adjudicante, propondo em relatório fundamentado, as medidas corretivas que se revelem necessárias.

#### **Cláusula 27**

##### **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 28**

##### **Contagem dos Prazos**

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



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

**Cláusula 29**

**Legislação aplicável**

1. O contrato é regulado pela legislação portuguesa.
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, aprovado pelo Decreto-Lei n.º 111-B/2017, de 31 de agosto, o qual prevalece sobre as disposições que lhes sejam desconformes.



PRESIDÊNCIA DO CONSELHO DE MINISTROS

**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

## **PARTE II – CLÁUSULAS TÉCNICAS**

### **Cláusula 1**

#### **Especificações Técnicas**

As especificações técnicas, contendo a caracterização e os requisitos dos serviços a prestar, são as que se indicam no Anexo I 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 ele subcontractadas ou pessoas que com ele colaborem no âmbito do procedimento, encontram-se obrigados a cumprir com as Obrigações de Segurança constantes no Anexo V, 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).

**Nota: Qualquer referência, nas peças deste procedimento, a fabricantes ou proveniências determinadas, processos de fabrico específicos, marcas, patentes ou modelos e a uma dada origem ou produção, considera-se acompanhada da menção “ou equivalente”.**



**ANEXO I**  
**ESPECIFICAÇÕES TÉCNICAS**  
**ELABORAÇÃO DE ESQUEMA DE CERTIFICAÇÃO DA CONFORMIDADE COM O**  
**QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA**

**ENQUADRAMENTO**

Para efeitos de cumprimento do disposto no **Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril**, relativo à certificação da cibersegurança das tecnologias da informação e no **Decreto-Lei n.º 65/2021, de 30 de julho**, que define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881, e considerando ainda a **Lei n.º 46/2018, de 13 de agosto**, que estabelece o regime jurídico da segurança do ciberespaço, a **Resolução do Conselho de Ministros n.º 55/2020, de 31 de julho**, que aprova a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, a **Resolução do Conselho de Ministros n.º 131/2021, de 10 de Setembro**, que aprova a Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o respetivo Plano de Ação Transversal para a legislatura e, por fim, os esquemas europeus de certificação da cibersegurança finalizado - ***Common Criteria based European candidate cybersecurity certification scheme*** (EUCC), **de 18 de maio de 2021** - e em elaboração - ***European Cybersecurity Certification Scheme for Cloud Services*** (EUCS) - o Centro Nacional de Cibersegurança (CNCS) pretende adquirir um pacote de bens e serviços projetado para dotar o CNCS das capacidades iniciais necessárias para o exercício das atribuições e responsabilidades da Autoridade Nacional de Certificação da Cibersegurança (ANCC) e implementação por esta de um quadro nacional de certificação da cibersegurança, no seguimento da designação do CNCS enquanto ANCC.

O serviço respeitante a **ELABORAÇÃO DE ESQUEMA DE CERTIFICAÇÃO DA CONFORMIDADE COM O QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA** consiste na elaboração de um esquema nacional de certificação da conformidade com Quadro Nacional de Referência para a Cibersegurança (QNRCS), publicado em 2019, de acordo com a metodologia estabelecida no Quadro de Avaliação de Capacidades de Cibersegurança, publicado em janeiro de 2020.

Tem como objetivo estabelecer o QNRCS de modo análogo ao de uma norma certificável, tendo em vista:



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

- harmonizar e elevar a cibersegurança das organizações nacionais, promovendo a implementação de medidas de identificação, proteção, deteção, resposta e recuperação contra as ameaças que possam colocar em causa a segurança das suas redes e sistemas de informação e do ciberespaço, através da obtenção de certificados específicos que serão aplicáveis em Portugal;
- instituir o Esquema de Certificação da conformidade com o QNRCS como primeiro esquema do quadro nacional de certificação da cibersegurança;
- contribuir determinantemente para atingir a Meta para 2023 de “80 % dos organismos TIC da Administração Pública com certificação de conformidade com o Quadro Nacional de Referência em Cibersegurança” descrita na Medida 8.4 – “Reforçar os níveis de cibersegurança dos organismos da Administração Pública, através do Quadro Nacional de Referência para a Cibersegurança” da Resolução do Conselho de Ministros n.º 55/2020 de 31 de julho de 2020, que aprova a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023;
- executar até ao 4.º trimestre de 2022 a submedida 6.1.1 — “Criar o ecossistema de certificação para o QNRCS no âmbito do Quadro Nacional de Certificação em Cibersegurança” da Medida 6.1 “Conformidade com o Quadro Nacional de Referência para Cibersegurança (QNRCS)” contida no Plano de Ação Transversal para a Transformação Digital da Administração Pública 2021-2023 (até final da presente legislatura), associado à Estratégia para a Transformação Digital da Administração Pública 2021-2026 aprovada pela Resolução do Conselho de Ministros n.º 131/2021, de 10 de Setembro, tendo em vista o alcance da meta de 80 % de entidades TIC da Administração Pública certificadas no QNRCS até ao 4.º trimestre de 2024 definida para o objetivo estratégico “6.1 — Promover a certificação das entidades da AP no Quadro Nacional de Referência em Cibersegurança (QNRCS)” da Linha Estratégica VI: Segurança e Confiança da referida Estratégia.

## **DEFINIÇÕES**

No âmbito do presente documento consideram-se relevantes as definições contidas no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril, relativo à certificação da cibersegurança das tecnologias da informação, designadamente as estabelecidas no seu art.º 2.º com as diferenças que seguidamente se descrevem:





PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

- no contexto do presente Caderno de Encargos os conceitos de «esquema europeu de certificação da cibersegurança» e de «esquema nacional de certificação da cibersegurança» correspondem às definições contidas nos pontos 9 e 10 do referido artigo, alusivas a «Sistema europeu de certificação da cibersegurança» e a «Sistema nacional de certificação da cibersegurança», respetivamente<sup>1</sup>.

Consideram-se, também, relevantes as definições contidas no artigo 3.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, bem como as estabelecidas no Quadro Nacional de Referência para a Cibersegurança.

São também relevantes as definições comumente constantes na literatura técnica e normativa no âmbito da certificação da cibersegurança das tecnologias da informação, tal como as contempladas nas normas internacionais ou nos esquemas europeus de certificação da cibersegurança aludidos ao longo deste documento.

Como padrão, todas as normas serão mencionadas sem indicação do ano de publicação, significando que todas as normas citadas se referem às versões em vigor, ou últimas versões publicadas, exceto quando especificamente assinalado.

## **OBJETO CONTRATUAL**

É objeto do presente caderno de encargos a aquisição do serviço de elaboração do **ESQUEMA DE CERTIFICAÇÃO DA CONFORMIDADE COM O QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA**, nos termos mencionados no Enquadramento e contemplados nos Requisitos.

---

<sup>1</sup> A opção por esta nomenclatura diverge da tradução oficial do documento da União Europeia, mas é fundada nas práticas comuns vigentes no meio da certificação, tendo sido validada através de consultas informais junto de entidades relevantes do meio.



## **REQUISITOS**

### **R1. Sobre a execução do serviço**

1. Os concorrentes deverão apresentar uma proposta que refira os custos parciais e totais para o fornecimento dos objetos inframencionados, detalhando a forma de abordagem e tempo a afetar para a resposta a todos e a cada um dos requisitos identificados.
2. Os concorrentes deverão ainda incluir na proposta, para cada RH a alocar ao desenvolvimento dos objetos, o respetivo Curriculum Vitae que indique e ateste a experiência profissional, projetos e estudos de referência anteriores (caso haja) e áreas de conhecimento especializado, aplicáveis às necessidades identificadas para a execução da proposta.
3. Serão aceites as propostas de outras considerações pertinentes apresentadas pelos concorrentes sobre cada um dos requisitos.
4. Na proposta deverão ser incluídos todos os serviços necessários à boa prossecução dos objetos referidos.
5. Todos os conteúdos produzidos devem respeitar as regras, os logotipos, as normas gráficas de comunicação escrita e formatos de apresentação do CNCS.
6. Os documentos a desenvolver no âmbito do presente procedimento devem ser entregues em formato editável e nas suas versões finais em língua Portuguesa.
7. Os documentos acima referidos deverão também ser entregues em formato editável e nas suas versões finais em língua Inglesa (UK), sempre que solicitado pelo CNCS.
8. A propriedade de todos os documentos, dados utilizados<sup>2</sup> para a sua elaboração, e demais materiais e conteúdos produzidos no âmbito do presente procedimento, incluindo as ferramentas operacionais e sistemas de informação, é exclusiva do CNCS.
9. Até 7 dias após a 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.
10. A entidade adjudicatária deverá informar o CNCS, semanalmente e através de correio eletrónico, do desenvolvimento do seu trabalho, para validação do bom andamento do projeto.

---

<sup>2</sup> Por dados utilizados entendem-se todos os dados primários utilizados para a realização dos documentos, 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



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

11. 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 no horário e local que seja definido e acordado por ambas as partes.
12. Caso se verifique ser necessário o agendamento de reuniões de trabalho para além das referidas, e de forma presencial, as mesmas deverão ser objeto de informação prévia ao CNCS, para efeitos de agendamento e acompanhamento.
13. A necessidade das reuniões de trabalho referidas poderá ser suscitada pela entidade adjudicatária ou pelo CNCS.
14. Nos serviços a desenvolver e proposta a apresentar não devem ser considerados custos com materiais e equipamentos de suporte à execução.

## **R2. Gerais do Objeto Contratual**

1. O objeto do presente caderno de encargos visa a execução da submedida 6.1.1 — **“Criar o ecossistema de certificação para o QNRCS no âmbito do Quadro Nacional de Certificação em Cibersegurança”** da Medida 6.1 “Conformidade com o Quadro Nacional de Referência para Cibersegurança (QNRCS)” contida no **Plano de Ação Transversal para a Transformação Digital da Administração Pública 2021-2023** (até final da presente legislatura), associado à **Estratégia para a Transformação Digital da Administração Pública 2021-2026 aprovada pela Resolução do Conselho de Ministros n.º 131/2021, de 10 de Setembro**.
2. A elaboração do **Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança** deve considerar, como documento enquadrador legislativo, o **Decreto-Lei n.º 65/2021, de 30 de julho**, que define as obrigações em matéria de certificação da cibersegurança em execução do **Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019**, assim como este último, no que concerne à certificação da cibersegurança das tecnologias da informação e comunicação e respetivos esquemas europeus de certificação de cibersegurança.
3. Deve ainda considerar, como documento enquadrador, a **Resolução do Conselho de Ministros n.º 55/2020 de 31 de julho de 2020, que aprova a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023** cuja Medida 8.4 – “Reforçar os níveis de cibersegurança dos organismos da Administração Pública,



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

através do Quadro Nacional de Referência para a Cibersegurança” inclui a Meta para 2023 de “80 % dos organismos TIC da Administração Pública com certificação de conformidade com o Quadro Nacional de Referência em Cibersegurança.”

4. O Centro Nacional de Cibersegurança (CNCS) é a **Autoridade Nacional de Certificação da Cibersegurança (ANCC)** designadamente para efeitos do disposto no artigo 58.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, gozando para este efeito de independência técnica, conforme estabelecido no **n.º1 do Artigo 20.º do Decreto-Lei n.º 65/2021, de 30 de julho**.
5. Enquanto Autoridade Nacional de Certificação de Cibersegurança, o CNCS pretende assim implementar um **Quadro Nacional de Certificação da Cibersegurança (QNCC)**, estabelecendo as disposições necessárias à elaboração, implementação e execução dos esquemas de certificação nacionais, aos quais são aplicáveis, com as necessárias adaptações, as disposições constantes do título III do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019.
6. O **Quadro Nacional de Referência para a Cibersegurança (QNRCS)** permite às organizações reduzir o risco associado às ciberameaças, definindo as bases para que qualquer entidade possa cumprir os requisitos mínimos de segurança das redes e sistemas de informação. Este documento desenvolvido pelo CNCS e disponível em <https://www.cncs.gov.pt/docs/cncs-qnracs-2019.pdf> permite que as organizações respondam à necessidade de implementar medidas de **Identificação, Proteção, Detecção, Resposta e Recuperação** contra ameaças que coloquem **em causa a segurança do ciberespaço**. O **Quadro de avaliação de capacidades de cibersegurança** é um produto complementar ao QNRCS, que define três níveis de capacidade (Inicial, Intermédio e Avançado) para cada uma das medidas de cibersegurança inscritas no QNRCS, para que as organizações consigam cumprir os cinco objetivos de Cibersegurança - identificar, proteger, detetar, responder e recuperar - tendo em consideração o seu contexto e dimensão. Este documento foi desenvolvido pelo CNCS e está disponível em <https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf>.
7. Neste contexto, pretende-se que a entidade adjudicatária proceda à elaboração do **Esquema de Certificação da conformidade com o QNRCS** enquanto primeiro esquema do QNCC, tendo em vista a sua implementação, adoção e execução no contexto da realidade organizacional (pública e privada) portuguesa.
8. Deve ser assegurada a confidencialidade de toda a informação tratada no âmbito do objeto contratual e o tratamento de informação classificada de acordo com a Resolução do Conselho de Ministros n.º 50/88, de 3 de dezembro, que aprova as instruções para a segurança nacional,



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

salvaguarda e defesa das matérias classificadas (SEGNAC 1), bem como a proteção de dados pessoais nos termos da legislação europeia e nacional aplicável.

9. Após aprovação da versão definitiva do documento, deverão ser produzidas em papel (capa flexível) 100 cópias do esquema em língua Portuguesa e 20 cópias do esquema em língua inglesa (UK).

### **R3. Específicos do Objeto Contratual**

1. O esquema de certificação da conformidade com o QNRCS tem como objetivo harmonizar e garantir uma abordagem comum aos níveis de cibersegurança das organizações portuguesas, no que diz respeito à implementação de medidas de identificação, proteção, deteção, resposta e recuperação contra as ameaças que possam colocar em causa a segurança das suas redes e sistemas de informação e do ciberespaço, através de certificados específicos que serão aplicáveis em Portugal.
2. Devem ser considerados os seguintes requisitos e diretrizes para a elaboração do esquema de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança:
  - a) O esquema de certificação a elaborar deve estar de acordo com as disposições constantes do título III do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, garantindo o devido enquadramento e adaptação nacional. Destaca-se a importância do Artigo 54.º no que concerne aos elementos dos sistemas europeus de certificação da cibersegurança;
  - b) O esquema de certificação da conformidade com o QNRCS é voluntário, podendo as diversas organizações recorrer à certificação de forma voluntária, independentemente da sua dimensão, natureza (pública ou privada), criticidade ou orientação tecnológica, salvo eventuais disposições futuras em contrário;
  - c) O Esquema de Certificação da conformidade com o QNRCS deve considerar a sua aplicabilidade a todo o tipo de organizações públicas e privadas nacionais, nomeadamente:
    - i. Administração Pública;
    - ii. Operadores de Infraestruturas Críticas;
    - iii. Operadores de Serviços Essenciais;
    - iv. Prestadores de Serviços Digitais;
    - v. Quaisquer outras organizações que utilizem redes e sistemas de informação.



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

- d) Devem ser descritas as vantagens de adesão para os destinatários do esquema de certificação da conformidade com o QNRCS, referindo, nomeadamente, a possibilidade de comprovar o nível de segurança organizacional, a análise e avaliação do nível de segurança organizacional através de uma certificação externa independente, e o reconhecimento de segurança através de um certificado que trará benefícios de ordem reputacional, permitindo alargar a base de clientes e/ou melhorar a confiança dos utilizadores;
- e) Os níveis de garantia de segurança a estabelecer devem estar em concordância com os níveis de capacidade - Inicial, Intermédio e Avançado – e respetivas evidências descritas no Quadro de Avaliação de Capacidades de Cibersegurança enquanto ferramenta complementar ao QRNCS. Com este requisito, pretende-se garantir a uniformização e coerência entre referências e ferramentas de apoio disponibilizadas pelo CNCS;
- f) Os requisitos de segurança definidos em cada um dos níveis de garantia devem seguir uma lógica sequencial e evolutiva, que permite que as entidades candidatas aumentem gradualmente as suas capacidades de cibersegurança à medida que cumpram com sucesso os requisitos de segurança exigidos em cada um dos níveis de garantia;
- g) A especificação dos diferentes níveis de garantia e correspondentes medidas de segurança associadas deve ir ao encontro dos requisitos específicos deste esquema de certificação e atender às características específicas e definidoras do tecido social e económico do país;
- h) O Instituto Português da Qualidade, I. P. (IPQ) é o organismo nacional de normalização em Portugal, de acordo com a designação legalmente definida para este efeito, tal como mencionado no Decreto-Lei n.º 65/2021, de 30 de julho;
- i) O Instituto Português de Acreditação, I.P. (IPAC) é o organismo nacional de acreditação em Portugal, de acordo com a designação legalmente definida para este efeito, tal como mencionado no Decreto-Lei n.º 65/2021, de 30 de julho;
- j) As atividades de avaliação da conformidade com o esquema e de emissão de certificados poderão ser efetuadas por entidades privadas e públicas que estejam devidamente acreditadas pelo IPAC como organismo de avaliação de conformidade (OAC) no contexto do esquema em apreço;
- k) As disposições do esquema devem prever e procurar garantir a independência na relação entre o organismo nacional de acreditação, a Autoridade Nacional de Certificação da Cibersegurança, na sua vertente de supervisão, e os organismos de avaliação de conformidade;
- l) O papel de supervisão do esquema de certificação é desempenhado pela Autoridade Nacional de Certificação da Cibersegurança;



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

m) Todas as alusões e citações a outros documentos devem ser devidamente referenciadas.

3. A entidade adjudicatária deverá efetuar uma análise e propor uma decisão, acompanhada do relatório de análise e parecer fundamentado, respeitante à admissibilidade de atividades de autoavaliação para fins de emissão de declarações de conformidade, ou como etapa preliminar do processo de certificação a validar por um OAC, tendo em conta o panorama organizacional nacional e o âmbito do esquema.
4. A entidade adjudicatária deverá efetuar uma análise e propor uma decisão, acompanhada do relatório de análise e parecer fundamentado, respeitante à possibilidade de entidades detentoras de certificações ISO/IEC 27001 ou outras normas relevantes poderem obter, no âmbito do esquema de certificação em apreço, reconhecimento de equivalências com determinados requisitos de segurança constantes do QNRCS, ponderados os eventuais fundamentos comuns, e quais os moldes da sua operacionalização.
5. A entidade adjudicatária deverá efetuar uma análise e propor uma decisão, acompanhada do relatório de análise e parecer fundamentado, respeitante à possibilidade dos OAC acreditados para a certificação da norma ISO/IEC 27001 serem considerados aptos e obterem a acreditação para certificar a conformidade com o QNRCS, sem necessidade de estabelecimento e cumprimento de requisitos específicos adicionais. Caso se conclua negativamente, deverá ser proposta uma definição de tais requisitos específicos adicionais, conforme prevista em VII.  
**Requisitos específicos aplicáveis aos organismos de avaliação de conformidade**, da estrutura para o esquema sugerida no requisito específico 7, descrita mais abaixo.
6. A entidade adjudicatária deverá efetuar o desenvolvimento de proposta de marca, rótulo e/ou etiqueta, e identidade gráfica associada, para o presente esquema de certificação, a incluir em anexo ao esquema. A identidade gráfica a desenvolver e respetivos materiais deverão respeitar as condições associadas à identidade gráfica desenvolvida pelo CNCS para o Quadro Nacional de Certificação da Cibersegurança (contexto nacional de certificação em que se desenvolvem os esquemas específicos, como o do QNRCS ora em apreço), e deverá ser validada pelo CNCS.
7. Sugere-se a seguinte estrutura para o entregável final (admitindo-se variações após proposta do adjudicatário e posterior aprovação pelo CNCS), em concordância com a ordenação de elementos dos esquemas europeus de certificação constantes no art.º 54 do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019:

**I. Introdução**, abrangendo e indicando, por exemplo:

- Síntese do conteúdo do documento;
- A forma como o documento está estruturado e deve ser interpretado;
- Destinatários;



- Definições e glossário;
- Significado da iconografia (se aplicável).

## **II. Objeto e Âmbito de Aplicação**

- A entidade adjudicatária deverá efetuar análise sobre o eventual objeto a certificar e o âmbito de aplicação do esquema, efetuando proposta consentânea fundamentada, a validar pelo CNCS.

## **III. Objetivo do Esquema**, indicando, por exemplo:

- Modo como as normas, os métodos de avaliação e os níveis de garantia selecionados correspondem às necessidades estratégicas dos promotores do esquema e específicas dos utilizadores a que se destinam.

## **IV. Uso de Normas de Referência**, indicando, por exemplo:

- Referências às normas internacionais, europeias ou nacionais aplicadas na avaliação como:
  - i. Controlos de Segurança usados no esquema de certificação
    - Quadro Nacional de Referência para a Cibersegurança e respetivos referenciais (CIS CSC 7.0, COBIT 5, ISO/IEC 27001:2013, NIST SP-800-53 Rev4);
  - ii. Métodos e padrões de avaliação de segurança
    - Quadro de Avaliação de Capacidades de Cibersegurança;
    - Norma internacional ISO/IEC 27006;
    - Normas internacionais de auditoria ISAE3402 e ISAE3000;
  - iii. Acreditação dos organismos de avaliação da conformidade que realizam as atividades de avaliação e certificação
    - Norma internacional ISO/IEC 17021 e ISO/IEC 17065;
  - iv. entre outras que se considerem relevantes para o âmbito e objeto contratual.

## **V. Níveis de Garantia**

## **VI. Autoavaliação**, indicando, por exemplo:

- Se a autoavaliação da conformidade é autorizada no âmbito do esquema de certificação. De referir que a autoavaliação da conformidade, a existir, deverá ser permitida apenas para o nível de garantia "Inicial".

## **VII. Requisitos específicos aplicáveis aos organismos de avaliação de conformidade**





PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

- Se aplicável, os requisitos específicos ou adicionais a que estão sujeitos os organismos de avaliação da conformidade [i.e., para além da acreditação pela norma internacional ISO/IEC 17021 e/ou ISO/IEC 17065, nos termos do Regulamento (CE) n.º 765/2008], a fim de garantir a sua competência técnica para avaliar os requisitos de cibersegurança;
- Pendente da análise e proposta previstos em requisitos R3. Específicos do Objeto Contratual, n.º 5, do presente Anexo.

#### **VIII. Métodos e Critérios de Avaliação**

- Tipos de avaliação a utilizar para demonstrar que são alcançados os objetivos de segurança específicos do esquema;
- Esta secção deve obrigatoriamente compreender as evidências de implementação e metodologias de avaliação definidas no documento referencial Quadro de Avaliação de Capacidades de Cibersegurança.

#### **IX. Informações necessárias para a Certificação**

- As informações necessárias para a certificação e que os requerentes devem fornecer ou, por qualquer outro modo, pôr à disposição dos organismos de avaliação da conformidade. Para este fim, propõe-se a estruturação da informação a fornecer através de um *Formulário de candidatura/notificação de alterações*<sup>3</sup>.

#### **X. Marcas e Rótulos**

- As condições de utilização de marcas ou rótulos, caso estes estejam previstos pelo esquema de certificação;
- Devem ser concordantes com as disposições a conter em anexo ao esquema com proposta de imagem e identidade gráfica, prevista em requisitos R3. Específicos do Objeto Contratual, n.º 6, do presente Anexo.

#### **XI. Monitorização do cumprimento**

- As regras para a monitorização do cumprimento pelas organizações dos requisitos de cibersegurança do esquema de conformidade com o QNRCS, incluindo mecanismos para demonstrar a conformidade permanente com os requisitos de cibersegurança especificados.

#### **XII. Processo de certificação e Gestão de Certificados**

---

<sup>3</sup> O formulário deve respeitar as disposições a conter em anexo ao esquema com proposta de imagem e identidade gráfica, prevista em requisitos R3. Específicos do Objeto Contratual, n.º 6, do presente Anexo.



- Descrição das várias fases do processo de certificação, tais como a fase de candidatura, a fase de auditoria e a fase de decisão, e dos procedimentos a seguir em cada uma;
- As condições para a emissão, manutenção, continuação e renovação do certificado de cibersegurança, bem como as condições para o alargamento ou a redução do âmbito da certificação.

**XIII. Regras referentes a incumprimentos**

- As regras relativas às consequências para os detentores de certificados que se encontrem em situação de incumprimento em relação aos requisitos do esquema.

**XIV. Conservação de registos pelos organismos de certificação**

- As regras relativas à conservação de registos por parte dos organismos de avaliação da conformidade.

**XV. Esquemas Relacionados**

- Se aplicável, a identificação dos esquemas nacionais ou internacionais de certificação da cibersegurança que tenham ou abranjam objetivos, requisitos de segurança, critérios e métodos de avaliação e níveis de garantia similares.

**XVI. Conteúdo e Formato do Certificado**

- O conteúdo e formato do certificado de cibersegurança a emitir;
- Devem ser concordantes com as disposições a conter em anexo ao esquema com proposta de imagem e identidade gráfica, prevista em requisitos R3. Específicos do Objeto Contratual, n.º 6, do presente Anexo.

**XVII. Disponibilização de Informação**

- O período de disponibilidade da documentação técnica e de todas as outras informações relevantes a disponibilizar pelo detentor do certificado.

**XVIII. Validade dos Certificados**

- O prazo máximo de validade dos certificados de cibersegurança emitidos ao abrigo do esquema.

**XIX. Política de divulgação dos certificados**

- A política de divulgação dos certificados de cibersegurança emitidos, alterados e retirados ao abrigo do esquema.

**XX. Referências**

**Referências de suporte**



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

Poderão ser referências de suporte para o desenvolvimento do **Esquema de Certificação da Conformidade com o Quadro Nacional de Referência em Cibersegurança**, entre outras, as seguintes:

**i. Esquemas Europeus de Cibersegurança**

- *EUCS (European Cybersecurity Certification Scheme for Cloud Services), a candidate cybersecurity certification scheme for cloud services.*
  - <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>
- *EUCC (Common Criteria based European candidate cybersecurity certification scheme), a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS.*
  - <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>

**ii. Esquemas de Certificação Nacionais**

- *Selo Digital – Cibersegurança (quando disponível)*
- *Cyber essentials* (Reino Unido):
  - <https://www.ncsc.gov.uk/cyberessentials/overview>
- *Die Beschleunigte Sicherheitszertifizierung - BSZ* (Alemanha):
  - [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Beschleunigte-Sicherheitszertifizierung/beschleunigte-sicherheitszertifizierung\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Beschleunigte-Sicherheitszertifizierung/beschleunigte-sicherheitszertifizierung_node.html)

**R4. Níveis de serviço**

1. Primeira versão do Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança até 12 de dezembro de 2021;
2. Versão final do Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança aprovados até 20 de dezembro de 2021.

**R5. Documentação e Entregáveis**



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

A entidade adjudicatária deverá entregar à entidade adjudicante, conforme faseamento dos trabalhos, no mínimo, a seguinte documentação e entregáveis em suporte digital:

- a) Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança na versão final aprovada;
- b) Anexo ao Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança contendo proposta de marca, rótulo e/ou etiqueta, e identidade gráfica associada, para o presente esquema de certificação, na versão final aprovada;
- c) Prospeto com uma síntese descritiva do Esquema de Certificação da conformidade com o QNRCS;
- d) Material de divulgação necessários à implementação do esquema (i.e., apresentações .pptx, infografias, entre outros);
- e) Material para treino e formação sobre o Esquema de certificação da conformidade com o QNRCS (i.e., manual de implementação, entre outros);
- f) Documentação elaborada no âmbito das atividades prestadas;
- g) Formação e passagem de conhecimento à(s) equipa(s) do CNCS envolvidas;
- h) Especificações técnicas e documentação anexa de referência;
- i) Metodologia de gestão de projeto e dados utilizados<sup>4</sup>;
- j) Plano e calendário de ações para realização do objeto do caderno de encargos.

## **R6. Perfis técnicos dos recursos a afetar aos serviços**

1. A Entidade Adjudicatária deverá afetar à implementação uma equipa de trabalho de acordo com a apresentada 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 de acordo com a sua proposta, deverá disponibilizar uma equipa com a dimensão adequada ao projeto, onde devem constar pelo menos dois recursos, com os seguintes

---

<sup>4</sup> Por dados utilizados entendem-se todos os dados primários utilizados, 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



perfis e requisitos mínimos para execução do contrato, os quais serão integrados em equipa de projeto:

- 5 ou mais anos de experiência profissional em funções similares ou que se verifiquem revelantes para o exercício da atividade do objeto contratual;
- 3 ou mais anos de experiência profissional em projetos de certificação de tecnologias de informação e comunicação;
- Conhecimento do enquadramento legal de certificação e cibersegurança na União Europeia e em Portugal;
- Formação comprovada em matérias de segurança da informação e cibersegurança nomeadamente no âmbito da norma NP ISO/IEC 27001 (Tecnologia de Informação — Técnicas de segurança — Sistemas de Gestão de Segurança da Informação — Requisitos);
- Valoriza-se a certificação ISO 27001 *Lead Implementer* ou ISO 27001 *Lead Auditor*.

4. O currículo a apresentar para efeitos do número anterior não pode ser objeto de substituição durante a fase de execução de contrato exceto em situação de força maior a comprovar pelo adjudicatário e cuja justificação deverá ser expressamente aceite pela entidade adjudicante.

## **R7. Metodologia de Gestão de Projeto**

1. 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.<sup>[1]</sup><sub>SEP</sub>
2. Deverá ser indicada e descrita a metodologia a utilizar para todas as fases de execução do projeto, de forma a garantir a entrega do esquema e documentação com a qualidade necessárias. Devem ser claramente indicadas as dependências entre as várias fases do projeto. Deverá existir um responsável pelo Plano de Trabalhos e por reportar a sua evolução à entidade adjudicante, bem como a manutenção da gestão de riscos e de incidentes.
3. A entidade adjudicatária deverá indicar os recursos que pretende alocar, bem como a sua experiência profissional nessa área, de acordo com a metodologia e planos apresentados.



## **ANEXO II**

### **OBRIGAÇÕES DE SEGURANÇA**

#### **ELABORAÇÃO DE ESQUEMA DE CERTIFICAÇÃO DA CONFORMIDADE COM O QUADRO NACIONAL DE REFERÊNCIA PARA A 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 ele subcontratadas ou pessoas que com ele colaborem no âmbito do procedimento, encontram-se obrigados 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 obrigado 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.



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

- 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, associado 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. Todas as entidades ou pessoas subcontratadas, que colaborem com a entidade adjudicatária no âmbito do presente procedimento, encontram-se obrigados 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.



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

4. À entidade adjudicatária não é permitido, a todo o tempo e sem para tal estar autorizado, 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.
5. À entidade adjudicatária não é permitido 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.
6. Não será utilizado qualquer sistema ou instalação física que não obedeça aos requisitos de certificação e segurança associados à classificação de segurança do procedimento.
7. À 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.
8. 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.
9. A entidade adjudicatária reconhece, aceita e compreende todas as obrigações e requisitos de segurança constantes nas presentes Obrigações de Segurança.

Pela Entidade Adjudicatária

\_\_\_\_\_

Pela Entidade Adjudicante

\_\_\_\_\_

Data: \_\_ / \_\_\_\_ / \_\_\_\_\_