

A complex network diagram with numerous nodes and connecting lines, rendered in a light teal color against a darker teal background. The nodes vary in size, and the lines are thin and interconnected, creating a dense web of connections.

**CNCS**



Centro Nacional  
de Cibersegurança  
PORTUGAL

ESQUEMA DE CERTIFICAÇÃO QNRCS

## Índice

<b>Sumário</b> .....	<b>4</b>
<b>1. Contexto do Esquema de Certificação QNRCS</b> .....	<b>5</b>
Autoridade Nacional de Certificação da Cibersegurança .....	5
Quadro Nacional de Referência para a Cibersegurança, referenciais e ferramentas associados .....	5
Um esquema de certificação da cibersegurança para as organizações nacionais .....	6
<b>2. Glossário do Esquema de Certificação QNRCS</b> .....	<b>6</b>
<b>3. Descrição e caracterização do Esquema de Certificação QNRCS</b> .....	<b>8</b>
<b>Conceitos</b> .....	<b>8</b>
Dono do esquema e entidade supervisora.....	8
<b>Caracterização e síntese descritiva</b> .....	<b>8</b>
Destinatários .....	10
<b>4. Objeto e âmbito de aplicação do Esquema de Certificação QNRCS</b> .....	<b>10</b>
Âmbito de aplicação .....	10
Delimitação do contexto de atividade aplicável e decisão de exclusão de medidas do QNRCS .....	10
Declaração de Aplicabilidade.....	11
Alteração do âmbito .....	11
Redução do âmbito.....	11
Exclusões .....	11
<b>5. Referências legais, normativas e regulamentares</b> .....	<b>12</b>
<b>6. Objetivos do Esquema de Certificação QNRCS</b> .....	<b>12</b>
<b>7. Papéis, funções e responsabilidades no Esquema de Certificação QNRCS</b> .....	<b>14</b>
<b>8. Requisitos para os Organismos de Certificação</b> .....	<b>15</b>
<b>9. Requisitos para os candidatos à certificação QNRCS</b> .....	<b>16</b>
<b>10. Níveis de capacidade versus níveis de garantia do EC QNRCS</b> .....	<b>17</b>
Níveis do EC QNRCS .....	17
Diferenciação de níveis .....	17
Básico .....	17
Substancial .....	17
Elevado.....	17
Progressividade .....	18
Cumulabilidade.....	18
Níveis de capacidade versus níveis de garantia .....	18

Seleção de níveis de capacidade e candidatura .....	18
Validação do nível selecionado.....	19
Aumento do nível de capacidade .....	19
Redução do nível de capacidade .....	19
<b>11. Ciclo de vida e processo de certificação QNRCS .....</b>	<b>19</b>
<b>Ciclo de vida .....</b>	<b>19</b>
Validade dos certificados.....	19
Manutenção da certificação .....	19
Renovação da certificação .....	19
<b>Processo de certificação QNRCS .....</b>	<b>20</b>
<b>Estados dos certificados .....</b>	<b>21</b>
<b>Transferência.....</b>	<b>22</b>
<b>Anulação voluntária.....</b>	<b>22</b>
<b>Incumprimento das regras do EC QNRCS.....</b>	<b>23</b>
<b>12. Análise e gestão do risco .....</b>	<b>23</b>
Aceitação do uso de metodologias estabelecidas .....	23
Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança .....	23
Elementos essenciais para o processo de análise e gestão de risco .....	24
Validação pelos OC dos documentos de análise de risco.....	24
<b>13. Métodos de avaliação e critérios de auditoria.....</b>	<b>24</b>
<b>14. Regras para o tratamento de “Não Conformidades” .....</b>	<b>25</b>
<b>15. Regras para a gestão dos certificados de conformidade QNRCS .....</b>	<b>26</b>
<b>16. Política de divulgação dos certificados de conformidade QNRCS .....</b>	<b>26</b>
<b>17. Regras para acesso, arquivo e preservação de informações relativa à certificação .....</b>	<b>26</b>
<b>18. Supervisão do ciclo de vida dos certificados de conformidade QNRCS.....</b>	<b>27</b>
<b>19. Histórico de revisões .....</b>	<b>28</b>
<b>20. ANEXOS .....</b>	<b>28</b>
<b>Anexo 1 – Lista de critérios de auditoria.....</b>	<b>28</b>
<b>Anexo 2 – Lista de referências legais, normativas e regulamentares .....</b>	<b>28</b>
<b>Anexo 3 – Formulário de candidatura à certificação .....</b>	<b>29</b>
<b>Anexo 4 – Modelo e marcas dos certificados QNRCS.....</b>	<b>29</b>
<b>Anexo 5 – Política de divulgação dos certificados QNRCS .....</b>	<b>29</b>

## Sumário

Compete ao Centro Nacional de Cibersegurança (CNCS), enquanto Autoridade Nacional de Certificação da Cibersegurança (ANCC), estabelecida de acordo com o art.º 20 do Decreto-Lei n.º 65/2021, de 30 de julho, em aplicação do art.º 58 do Regulamento (UE) 2019/88, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, a elaboração, implementação e gestão de esquemas nacionais de certificação da cibersegurança.

No prosseguimento da sua missão de capacitação em cibersegurança das organizações nacionais, o CNCS disponibiliza desde 2020 o Quadro Nacional de Referência para a Cibersegurança (QNRCS), um referencial que orienta e apoia as organizações na adoção de uma cultura e práticas de cibersegurança, e a sua gestão contínua. Desde a sua publicação, o QNRCS tem-se afirmado como um modelo, amplamente reconhecido e utilizado, para o desenvolvimento e o aperfeiçoamento das capacidades de cibersegurança das organizações nacionais.

A aposta do CNCS na elaboração de um esquema de certificação da conformidade com o QNRCS (EC QNRCS) visa valorizar aquelas organizações que já têm por referência e implementam o QNRCS na gestão das suas Tecnologias de Informação e Comunicação, permitindo-lhes obter um certificado que assim o ateste e sinalize perante as partes interessadas que lhe são relevantes. Aspira ainda incentivar a adoção do QNRCS por aquelas que ainda não o fizeram, e o aperfeiçoamento e aprofundamento da implementação do QNRCS pelas que o adotaram de forma incipiente.

A constituição de uma bolsa de organizações certificadas na conformidade com o QNRCS poderá ainda atender a necessidades de política pública em cibersegurança, quando é preciso que as entidades que respondem a certos fins ou oferecem determinados serviços garantam um nível definido de cibersegurança, e é imperativo recorrer a um método idóneo, como a certificação, que as permita diferenciar nesse capítulo.

O EC QNRCS foi desenvolvido tendo por inspiração os esquemas europeus elaborados no contexto do Enquadramento Europeu de Certificação da Cibersegurança, possibilitando a obtenção da certificação em um de três níveis de garantia, designados *Básico*, *Substancial* e *Elevado*. O dono do esquema é o CNCS, na qualidade de ANCC, que elabora, gere e zela pela atualização e adequação do esquema, com a cooperação do Instituto Português da Qualidade, IP (IPQ) e do Instituto Português de Acreditação, I.P. (IPAC), e supervisiona a sua implementação. A atividade de certificação é efetuada por entidades terceiras independentes, os organismos de certificação (OC), que, para esse fim, devem obter e manter a acreditação junto do IPAC. Os destinatários da certificação da conformidade com o QNRCS são as organizações que tenham atividade e estejam estabelecidas em território nacional.

O presente documento descreve e define todos os componentes exigidos para a instituição de um esquema de certificação: o seu objeto e âmbito de aplicação, as referências legais que o balizam, os seus objetivos, as funções, papéis e responsabilidades dos seus intervenientes, os requisitos exigíveis a OC e a candidatos à certificação, os níveis de certificação, o ciclo de vida e o processo de certificação, o requisito específico de condução de um processo de análise e gestão de risco, os métodos de avaliação empregues e os critérios de auditoria, as regras para o tratamento de “Não Conformidades”, para a gestão dos certificados e para o acesso, arquivo e preservação de informações relativa à certificação, a política de divulgação dos certificados e, por fim, a supervisão do ciclo de vida dos certificados de conformidade QNRCS.

Em anexo são ainda disponibilizados, entre outros, o formulário de candidatura para a certificação, o modelo de certificado, em que são descritos os elementos constituintes e diferenciadores dos certificados, e, principalmente, no **Anexo 1, a Lista de critérios de auditoria**, que descreve os requisitos de implementação das medidas de segurança, para cada nível, bem como as evidências que deverão ser disponibilizadas aos OC em sede de auditoria para verificação do cumprimento dos requisitos.

O EC QNRCS proporciona, através da demanda de transparência e clareza nas suas disposições, condições para que as certificações decorram de forma isenta e consistente. Por via da reconhecida exigência nos seus requisitos, a certificação no EC QNRCS dirige-se a entidades com especiais responsabilidades em Cibersegurança e inaugura decisivamente o Quadro Nacional de Certificação da Cibersegurança.

**Centro Nacional de Cibersegurança**

## 1. Contexto do Esquema de Certificação QNRCS

### Autoridade Nacional de Certificação da Cibersegurança

Na sequência da publicação do Decreto-Lei n.º 65/2021<sup>1</sup>, de 30 de julho, foi o Centro Nacional de Cibersegurança (CNCS) designado Autoridade Nacional de Certificação da Cibersegurança (ANCC), conforme estabelece o art.º 20 daquele normativo, em aplicação do art.º 58 do Regulamento (UE) 2019/881<sup>2</sup>, do Parlamento Europeu e do Conselho, de 17 de abril de 2019.

O citado Decreto-Lei confere ao CNCS a possibilidade de desenvolver e implementar esquemas específicos de certificação da cibersegurança relativos a produtos, serviços e processos de tecnologias de informação e comunicação (TIC) que não sejam ainda abrangidos por um esquema europeu, sempre que a especificidade do objeto da certificação o justifique, no seio de um Quadro Nacional de Certificação da Cibersegurança (QNCC).

O QNCC pode ser assim descrito como o ecossistema nacional de certificação da cibersegurança no qual se constroem e operam os diferentes esquemas de certificação nacionais, para responder a exigências de políticas públicas de cibersegurança e outras, desde que não cubram âmbitos de aplicação que sejam objeto de esquema de certificação europeu.

O QNCC é inspirado no conceito de “enquadramento europeu para a certificação da cibersegurança” em toda a União Europeia para produtos, serviços e processos de TIC, introduzido no Regulamento (UE) 2019/881. Decorre desta determinação da UE o quadro normativo para a produção de esquemas europeus de certificação em cibersegurança específicos e baseados no risco, como o “*Common Criteria based European Cybersecurity Certification scheme*” (EUCC), o “*European Cybersecurity Certification Scheme for Cloud Services*” (EUCS), e o “*EU 5G candidate cybersecurity certification scheme*” (EU5G). Similarmente, as categorias de elementos que constituem os esquemas nacionais de certificação da cibersegurança correspondem, no que é aplicável, às categorias de elementos constituintes dos esquemas europeus estabelecidos no art.º 54 do Regulamento (UE) 2019/881.

### Quadro Nacional de Referência para a Cibersegurança, referenciais e ferramentas associados

O Quadro Nacional de Referência para a Cibersegurança (QNRCS) foi criado e disponibilizado pelo CNCS em abril de 2020 enquanto referencial para suporte das organizações à sua capacitação.

O QNRCS constitui um conjunto de recomendações para que as organizações possam definir uma estratégia de cibersegurança que envolva toda a sua estrutura. Pretende-se que as entidades o adotem de forma voluntária para assim beneficiar de uma abordagem homogénea e integral à sua conjuntura específica de cibersegurança, contribuindo, simultaneamente, para a promoção de uma resposta nacional às ciberameaças.

Procurando refletir a realidade organizacional portuguesa, o QNRCS disponibiliza as bases para que qualquer entidade possa cumprir os requisitos mínimos de segurança das redes e sistemas de informação por meio da implementação de medidas de Identificação, Proteção, Detecção, Resposta e Recuperação contra ameaças que colocam em causa a segurança do ciberespaço, reduzindo assim o risco associado.

Em complemento ao QNRCS, o CNCS elaborou o Quadro de Avaliação de Capacidades de Cibersegurança (QACC), como referencial que viabiliza a autoavaliação das organizações relativamente à implementação e operacionalização das medidas de segurança do QNRCS, considerando o seu contexto e dimensão, enquanto procuram cumprir os citados objetivos de cibersegurança – identificar, proteger, detetar, responder e recuperar – e que se traduzem em três diferentes níveis de capacidade – Inicial, Intermédio e Avançado.

Como ferramentas de suporte à implementação do QNRCS em contexto organizacional, o CNCS disponibiliza ainda, no seu sítio web, o CyberCheckUp e o Roteiro para as Capacidades Mínimas de Cibersegurança (RCMC).

<sup>1</sup> Doravante abreviado como Decreto-Lei n.º 65/2021

<sup>2</sup> Doravante abreviado como Regulamento (UE) 2019/881



O CyberCheckUp é uma ferramenta interativa em linha para apoiar o exercício de autoavaliação do QACC. Permite a uma organização aferir, por meio de um questionário correlativo ao QACC, o seu estado em termos de cibersegurança, considerando a adoção das medidas definidas no QNRCS. Os resultados do CyberCheckUp permitem situar o nível de capacidade da organização de acordo com a distribuição convencionada no QACC.

O RCMC é um modelo de capacitação em cibersegurança com enfoque especial em pequenas e médias empresas (PME). Apresenta um conjunto de ações divididas por cinco fases, de adaptação gradual, a implementar em cada organização, quer seja por meios próprios internos, ou mesmo recorrendo a subcontratação ou externalização de soluções. Este conjunto de ações, enquadradas no âmbito do QNRCS, procuram corresponder a um conceito das capacidades consideradas mínimas em cibersegurança.

## Um esquema de certificação da cibersegurança para as organizações nacionais

A dependência crescente das TIC por parte de organizações de todos os tipos e setores, e o reconhecimento de que a qualidade e a própria essência das suas prestações de serviços assentam cada vez mais em infraestruturas e processos de informação e comunicação que se situam e atuam no ciberespaço, tem vindo a formar a consciência, em decisores políticos e gestores de todos os quadrantes, da necessidade de dotar o país e as organizações que lideram de um nível de cibersegurança adequado face aos riscos que correm.

Os processos de certificação da cibersegurança representam um meio eficaz de desenvolvimento organizacional através da assimilação de práticas sistematizadas de cibersegurança e da apropriação de uma cultura de cibersegurança pelos membros de uma organização.

A certificação da cibersegurança e os esforços que a ela conduzem apresentam-se como uma resposta idónea à procura por informação, por formação e por processos e ferramentas de capacitação em cibersegurança.

No prosseguimento da missão última do CNCS de aumentar a segurança nacional no ciberespaço e tendo por orientação o QNRCS, surge como etapa natural na evolução das ações de capacitação das organizações nacionais e, por conseguinte, do país, a criação e a operacionalização de um esquema de certificação que permita atestar, por organismos terceiros independentes e devidamente acreditados, o nível alcançado pelas organizações nas suas implementações do QNRCS.

O alinhamento entre o QNRCS e o QACC é o ponto de partida para o CNCS, assumindo o seu papel de ANCC dentro da amplitude de atuação conferida pelo Decreto-Lei n.º 65/2021, desenvolver o presente Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança (**EC QNRCS**).

O EC QNRCS é, assim, concebido para permitir que as organizações públicas e privadas possam atestar a implementação das suas práticas de cibersegurança organizativas, processuais, tecnológicas e humanas, através da certificação, tendo como critério de referência o QNRCS e inspiração no QACC e no RCMC.

## 2. Glossário do Esquema de Certificação QNRCS

A tabela apresentada em seguida tem como objetivo permitir uma melhor compreensão dos termos ou conceitos utilizados no esquema de certificação QNRCS.

Em complemento, recomenda-se a consulta do capítulo 3.4 “Definições e Abreviaturas” do QNRCS.

Termo ou Conceito	Abreviatura	Definição	Notas adicionais
<b>Auditoria de certificação</b>		Processo sistemático, independente e documentado para obter evidência objetiva e respetiva avaliação objetiva com vista a determinar em que medida os requisitos das normas de certificação são cumpridos (ISO 9000:2015)	
<b>Análise do Risco</b>	AR	Avaliação da probabilidade de um perigo ocorrer e no cálculo do seu possível impacto na organização	
<b>Conformidade</b>	Conformidade	Cumprimento dos requisitos dos critérios de certificação (Normas, regulamentos, etc.)	
<b>Conformidade permanente</b>		Representa o esforço que a organização deverá empreender para assegurar a continuidade do nível de garantia de cibersegurança obtido na certificação	
<b>Constatações de auditoria</b>	Constatações	Resultados da avaliação das evidências de auditoria recolhidas face aos critérios da auditoria (ISO 9000:2015)	
<b>Esquema de Certificação</b>	EC	Conjunto de regras, práticas e procedimentos que a organização, à qual pertence o esquema, emite para que os organismos de certificação e as organizações auditadas entendam os compromissos que as partes devem aceitar, cumprir e fazer cumprir	
<b>Evidências de Auditoria</b>	Evidências	Registos, afirmações factuais ou outra informação, que sejam relevantes para os critérios da auditoria e verificáveis (ISSO 9000:2015)	
<b>Medidas de segurança</b>	Medidas	Trata-se de práticas que o QNRCS identifica para a implementação eficaz dos objetivos de segurança	No contexto do esquema de certificação tornam-se requisitos de conformidade em auditorias de certificação
<b>Medidas de segurança obrigatórias</b>		Trata-se de medidas de segurança definidas pelo QNRCS que são definidas como sendo de aplicação obrigatória pelo EC QNRCS por todos os candidatos à certificação	Ver Anexo 1 – Lista de critérios de auditoria
<b>Medidas de segurança passíveis de exclusão</b>		Trata-se de medidas de segurança do QNRCS passíveis de exclusão de implementação e que cada organização candidata identifica, através da sua análise do risco, como podendo não ser aplicáveis ao seu contexto específico para melhorar a sua cibersegurança	Ver Anexo 1 – Lista de critérios de auditoria
<b>Não conformidade Maior</b>	NC Maior	A medida de segurança não se encontra implementada ou, se implementada, encontra-se totalmente desalinhada dos objetivos da medida de segurança.	No enquadramento de auditoria de certificação, correspondente ao não cumprimento de um requisito

<b>Não conformidade Menor</b>	NC Menor	A medida de segurança encontra-se implementada, mas não consegue demonstrar totalmente que cumpre os respetivos objetivos	
<b>Nível de Capacidade</b>		Representa grupos cumulativos de medidas de segurança que a organização implementa, conferindo 3 níveis de execução efetiva: Básico, Substancial e Elevado	No contexto do esquema de certificação tornam-se em níveis de garantia de cibersegurança, comprovados como resultado de um processo de certificação.
<b>Oportunidade de Melhoria</b>	OM	Oportunidade de atuação identificada com foco no aumento do desempenho de uma organização e reação à mudança interna e externamente	
<b>Requisitos de conformidade</b>	Requisitos	Requisito relativo à qualidade e/ou segurança (ISO 9001:2015)	

### 3. Descrição e caracterização do Esquema de Certificação QNRCS

O Esquema de Certificação QNRCS está incluído no QNCC, sendo concebido para sustentar o objetivo de certificação da cibersegurança de organizações estabelecidas em território nacional, tendo como critério de conformidade o QNRCS.

#### Conceitos

Por “certificação” deve entender-se a declaração formal de comprovação do cumprimento de requisitos emitida por uma organização autorizada a realizar as atividades necessárias para produzir tal declaração, designada como “organismo de certificação” (OC<sup>3</sup>).

Por “dono do esquema” entende-se a entidade externa e independente do OC que define as regras, procedimentos e requisitos do esquema, e reconhece a certificação dentro do seu âmbito.

O “esquema de certificação” consiste num conjunto de regras, práticas e procedimentos que o dono do esquema especifica para que os organismos de certificação e as organizações auditadas entendam os compromissos que as partes devem aceitar, cumprir e fazer cumprir.

Para monitorização das atividades de certificação, é estipulada uma “entidade supervisora” que se encarrega de avaliar o desempenho do “esquema de certificação” e garantir que os seus requisitos são efetivados de acordo com o estabelecido e cumpridos por todas as partes.

#### Dono do esquema e entidade supervisora

O CNCS, na qualidade de Autoridade Nacional de Certificação para a Cibersegurança, é a entidade competente pelos esquemas nacionais de certificação da cibersegurança e é, assim, a entidade responsável pela elaboração e operacionalização do esquema de certificação da conformidade com o QNRCS, bem como pela sua supervisão.

#### Caracterização e síntese descritiva

O esquema de certificação QNRCS define e institui o ciclo de vida da certificação da conformidade com o QNRCS e dos respetivos certificados de conformidade, e tem por entidade supervisora o CNCS, sendo os requisitos para a certificação os que constam do seu **Anexo 1 – Lista de critérios de auditoria**.

O esquema de certificação da conformidade com o QNRCS é estabelecido neste documento, onde são definidas as suas regras, requisitos e procedimentos, incluindo o objeto e âmbito de aplicação do esquema, os objetivos e

<sup>3</sup> Organismos de certificação, por vezes também designados como organismos de avaliação de conformidade



destinatários, as partes interessadas e papéis associados, os métodos e critérios utilizados para a avaliação da conformidade, os requisitos para organismos de certificação e para os candidatos, o processo e ciclo de certificação, e as responsabilidades no domínio da supervisão do funcionamento do esquema, entre outras regras.

O EC QNRCS apresenta as seguintes características genéricas:

- A certificação da conformidade com o QNRCS é voluntária, salvo se expressamente determinado em legislação própria.
- Os requisitos para a certificação, critérios e evidências de auditoria para a decisão de certificação são definidos pelo **Anexo 1 – Lista de critérios de auditoria** do presente documento, baseados no QNRCS e inspirados no QACC e RCMC.
- A certificação obtida noutra esquema ou norma certificável não dá lugar a qualquer tipo de equivalência direta para a obtenção do certificado de conformidade com o QNRCS.
- A implementação das medidas previstas no EC QNRCS exige que a organização candidata efetue uma análise de risco que vise identificar o risco a que está sujeita e as medidas do QNRCS adequadas para o tratamento desse mesmo risco.
- O EC QNRCS prevê a implementação de todas as medidas de segurança do QNRCS por defeito. No entanto, poderão existir medidas de segurança passíveis de exclusão pelos candidatos, por não se aplicarem ao tratamento do seu risco específico. Podem assim ser distinguidas, de entre todas as medidas de segurança do QNRCS, dois tipos de medidas, que se classificam da seguinte forma:
  - medidas obrigatórias, que todos os candidatos à certificação deverão implementar;
  - medidas passíveis de exclusão, que os candidatos poderão optar por não implementar em função da análise de risco efetuada.

A classificação das medidas como obrigatórias ou passíveis de exclusão é indicada no **Anexo 1 – Lista de critérios de auditoria** deste EC QNRCS.

- O esquema de certificação QNRCS compreende a certificação da conformidade com o QNRCS em três níveis de garantia, que se distribuem por um nível “Básico”, um nível “Substancial” e um nível “Elevado”.
- Cabe à organização candidata declarar a que nível de garantia pretende a certificação.
- A certificação da conformidade com o QNRCS exige que o processo seja conduzido por uma entidade externa e independente à organização candidata, o organismo de certificação.
- Todas as atividades de avaliação da conformidade, incluindo as auditorias, e de decisão de certificação deverão ser executadas pelo organismo de certificação, não sendo admissíveis atividades de autoavaliação pela organização candidata para verificação da conformidade ou decisão de certificação no EC QNRCS.
- A organização deverá efetuar a candidatura à certificação diretamente junto de um organismo de certificação.
- Os organismos de certificação devem estar devidamente acreditados nessa qualidade pelo Instituto Português de Acreditação, I.P. (IPAC)<sup>4</sup> para poderem operar no contexto deste esquema.
- O organismo de certificação, após a aceitação da candidatura, deverá efetuar a verificação e avaliação da implementação dos requisitos de certificação pela organização candidata, por meio de auditorias e verificações documentais. O OC deverá, em seguida, efetuar uma revisão dos resultados das auditorias e proferir uma decisão acerca da certificação. Caso o processo seja concluído com sucesso, culminando numa decisão de certificação favorável, o OC emite o certificado, que passa a poder ser utilizado pela organização certificada.
- O certificado emitido tem uma validade de três anos desde a data da emissão.

---

<sup>4</sup> O IPAC é o organismo nacional de acreditação

- A organização certificada deverá cumprir com os requisitos de certificação durante o período de validade do certificado, incluindo a realização de auditorias de acompanhamento e as ações de preparação atempada do processo de renovação.
- A entidade supervisora verifica o cumprimento das regras e requisitos do esquema por todas as partes.
- O dono do esquema procede à atualização<sup>5</sup> do presente documento e respetivos anexos, sempre que se revele necessário e/ou pertinente.

## Destinatários

A certificação no esquema de certificação da conformidade com o QNRCS tem por destinatárias as organizações nacionais de todas as dimensões, tipologias e áreas de atividade, desde que estejam estabelecidas em território nacional.

O esquema de certificação QNRCS foi desenvolvido tendo como principais destinatários finais as organizações da Administração Pública (AP) central e local, operadores de infraestruturas críticas, operadores de serviços essenciais<sup>6</sup>, prestadores de serviços digitais<sup>7</sup>, empresas e outro tipo de organizações privadas e não-governamentais, com ou sem fins lucrativos, que exibam, necessitem ou queiram alcançar um nível de maturidade em cibersegurança reconhecido como meritório entre pares, no mercado em que operam ou na sociedade em geral, para propiciar confiança na sua segurança e na dos serviços que prestam às partes interessadas com quem se relacionam.

## 4. Objeto e âmbito de aplicação do Esquema de Certificação QNRCS

O esquema de certificação QNRCS possibilita a certificação acreditada das práticas de cibersegurança das organizações nacionais, genericamente consideradas, de acordo com os métodos e critérios referidos no **Capítulo 13 – Métodos de avaliação e critérios de auditoria** e definidos no **Anexo 1 – Lista de critérios de auditoria** do presente documento.

### Âmbito de aplicação

O EC QNRCS tem por âmbito de aplicação a implementação das medidas de segurança do QNRCS especificadas no **Anexo 1 – Lista de critérios de auditoria** do presente esquema, dentro de um determinado contexto de atividade em cada organização. Tal contexto de atividade aplicável é determinado pela organização candidata em função do processo de análise e gestão de risco, e é estabelecido na “Declaração de Aplicabilidade”.

### Delimitação do contexto de atividade aplicável e decisão de exclusão de medidas do QNRCS

A caracterização do risco da organização e a determinação do nível de risco aceitável são efetuadas por meio de uma análise de risco que deverá reger-se pelos princípios referidos no **Capítulo 12 – Análise e gestão do risco** do presente esquema. Executada a análise de risco e conforme a avaliação do risco específico à sua esfera de atuação, a organização candidata determina o conjunto das suas atividades ao qual se deverão aplicar as medidas de segurança do QNRCS, isto é, estipula se estas se devem aplicar a todas as atividades e a toda a

---

<sup>5</sup> E, eventualmente, à sua extinção

<sup>6</sup> Conforme definição da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço, da Diretiva (UE) 2016/1148 e designação pelo CNCS

<sup>7</sup> Idem, no que for aplicável

organização ou se se aplicam apenas às suas atividades significativas, definidas como as que são essenciais para a prestação dos respetivos serviços, identificando-as.

Efetuada esta delimitação, e caso se observe que alguma das medidas do QNRCS definidas no presente esquema como passíveis de exclusão não se aplica ao seu contexto de atividade ou para tratamento do seu risco específico, a organização poderá eleger não aplicá-la. Tal exclusão não deverá, no entanto, colocar em causa o tratamento adequado do risco em que a organização incorre, no sentido de reduzir a sua exposição e trazer o risco para um patamar tido por aceitável.

## Declaração de Aplicabilidade

A definição do contexto de atividade da organização aplicável à certificação, e as medidas do QNRCS passíveis de exclusão que a organização decidir não aplicar, deverão ser descritas no documento designado “Declaração de Aplicabilidade”, a entregar no momento da candidatura.

As medidas de segurança do QNRCS, exceto as medidas passíveis de exclusão que a organização declare optar por excluir, dentro dos limites de atividade que a organização candidata determine, conforme conste na “Declaração de Aplicabilidade”, constituem, após validação pelo organismo de certificação, o âmbito de aplicação do esquema de certificação da conformidade com o QNRCS na organização candidata. A matéria auditável em contexto de auditoria será, assim, o grau e qualidade de implementação destas medidas de segurança.

## Alteração do âmbito

Após a organização estar certificada, qualquer alteração na organização que possa interferir com a delimitação do âmbito da certificação, sobretudo qualquer alteração à sua atividade principal<sup>8</sup>, deverá ser vertida num pedido de alteração de âmbito a solicitar ao OC e ser por este aprovado.

Dependendo do teor da alteração, poderá ser necessário acrescentar tempo adicional para auditar quaisquer atividades que tiverem sido acrescentadas ao âmbito da certificação, durante uma auditoria extraordinária ou na auditoria do ciclo.

Durante a auditoria extraordinária, o auditor poderá verificar apenas as atividades que foram adicionadas ao âmbito, desde que não interfiram com o estado de conformidade associado a outras atividades previamente auditadas.

## Redução do âmbito

A redução do âmbito de certificação de uma organização certificada pode ser efetuada administrativamente, salvo se existir algum motivo não previsto que possa ser lícito.

## Exclusões

Exclui-se do âmbito de aplicação da presente versão do esquema de certificação QNRCS:

- cibersegurança da cadeia de abastecimento para os prestadores de serviços nas organizações candidatas (exceto quanto às medidas específicas definidas no QNRCS que se referem à relação da organização candidata com as partes interessadas externas e/ou quanto à gestão de risco da cadeia logística)<sup>9</sup>;
- cibersegurança dos prestadores de serviços de computação na nuvem.

---

<sup>8</sup> Incluindo a mudança de uma atividade principal para outra

<sup>9</sup> Esclarece-se, a título interpretativo, que o EC QNRCS não inclui a certificação das entidades integrantes da cadeia de abastecimento. Contudo, avalia e certifica a conformidade da entidade candidata e/ou certificada quanto às medidas de gestão de risco da cadeia logística

## 5. Referências legais, normativas e regulamentares

O esquema de certificação QNRCS está definido em função dos requisitos e orientações estabelecidas nos diplomas legais nacionais e europeus aplicáveis, em normas e referenciais de boas práticas disponibilizados pelo CNCS, ou ainda em fontes internacionalmente reconhecidas:

- O EC QNRCS está contido no Quadro Nacional de Certificação da Cibersegurança, conforme previsto no Decreto-Lei n.º 65/2021, sendo desenvolvido ao abrigo do n.º2 do art.º 20 daquele diploma legal;
- Os elementos constituintes do EC QNRCS regem-se, com as necessárias adaptações, pelas disposições constantes do título III do Regulamento (UE) 2019/881, seguindo, em particular, tanto quanto possível e aplicável, os elementos definidos no art.º 54 daquele normativo;
  - Por conseguinte, a estrutura e conteúdos dos esquemas europeus EUCC e EUCS também serviram de inspiração para o EC QNRCS;
- A estrutura do esquema de certificação contido no DNP TS 4577-1 Maturidade digital – Selo digital, Parte 1: Cibersegurança, parcialmente desenvolvido pelo CNCS, foi outra fonte de inspiração do presente esquema;
- A terminologia utilizada no EC QNRCS tem por referência a terminologia e definições da ISO/IEC 27001;
- A norma ISO/IEC 17065 é o padrão internacional para a acreditação<sup>10</sup> dos organismos de avaliação de conformidade no âmbito do EC QNRCS;
- A secção alusiva à gestão de risco que informa as decisões quanto às medidas do QNRCS a aplicar foi baseada nas orientações decorrentes do Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança (à data, pendente de publicação);
- Os requisitos de implementação de medidas para fins de certificação no âmbito do presente esquema, bem como as evidências de verificação associadas, estão definidos no **Anexo 1 – Lista de critérios de auditoria** deste EC QNRCS e operacionalizam as medidas de segurança estabelecidas no Quadro Nacional de Referência para a Cibersegurança, tendo por inspiração o Quadro de Avaliação de Capacidades de Cibersegurança e fazendo uso, tanto quanto possível, da terminologia e critérios de auditoria em uso na ISO/IEC 27001;
- O leque de medidas definidas como sendo de aplicação obrigatória no contexto do presente esquema é inspirado nas ações previstas e objetivos propostos no Roteiro para as Capacidades Mínimas de Cibersegurança.

A lista comentada das referências utilizadas, acima listadas, e de outros documentos que lhes servem de matriz, é disponibilizada, através de hiperligação, no **Anexo 2 – Lista de referências legais, normativas e regulamentares**.

## 6. Objetivos do Esquema de Certificação QNRCS

O Esquema de Certificação QNRCS tem por objetivo elevar o nível de cibersegurança das organizações nacionais, em particular as organizações às quais são exigíveis particulares responsabilidades de cibersegurança atentas as funções que desempenham, a natureza ou essencialidade dos serviços que prestam para a sociedade, ou dos bens que produzem, e o grau de dependência das TIC, ou de integração no ciberespaço, que evidenciam.

Como destinatários especiais, incluem-se nestas categorias as organizações abrangidas pela Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço, nomeadamente organizações

---

<sup>10</sup> Independentemente de eventuais requisitos adicionais que vierem a ser definidos pelo CNCS e pelo IPAC

da Administração Pública, central e local, sobretudo os seus organismos TIC, os operadores de infraestruturas críticas, operadores de serviços essenciais e os prestadores de serviços digitais.

Um dos principais objetivos para o EC QNRCS é assim o de, através da concretização das ações inerentes a um processo de certificação, auxiliar as organizações abrangidas pelo Regime Jurídico da Segurança do Ciberespaço a cumprir com as exigências legais que sobre elas impendem, a capacitá-las para prevenir e evitar incidentes de cibersegurança, e a revesti-las de mecanismos de resiliência indispensáveis à continuidade da prestação dos seus serviços ou da produção dos seus bens, na eventualidade de ocorrência dos incidentes.

O EC QNRCS poderá também ser genericamente utilizado como instrumento para sustentar políticas públicas de cibersegurança, através da sua utilização por reguladores, organismos de supervisão e outro tipo de organismos públicos, que entendam exigir a determinadas categorias de entidades sob a sua esfera de atuação, a certificação neste esquema para prossecução de objetivos específicos de cibersegurança, principalmente os de continuidade de serviço e de proteção do público em geral.

Para além destas, as empresas e outro tipo de organizações privadas e não-governamentais, com ou sem fins lucrativos, que dediquem especial atenção à sua cibersegurança, exibindo um nível de maturidade incomum ou que pretendam atingir um patamar de cibersegurança notável, são outros dos destinatários preferenciais deste esquema.

Através da certificação no EC QNRCS, tais entidades aspiram à criação de vínculos de confiança na sua relação com os seus utilizadores, clientes e/ou consumidores e outras partes interessadas externas, ao desenvolvimento e solidificação de valores reputacionais e à promoção da diferenciação favorável da imagem da entidade e das suas ofertas.

Por seu turno, um objetivo suplementar aos acima listados será o de propiciar a tais partes interessadas externas, sobretudo clientes e consumidores, um dispositivo que lhes permita adquirir uma representação do estado da cibersegurança das entidades às quais se pretendem associar, suscitando comparações e alicerçando as suas decisões e escolhas.

O EC QNRCS distingue-se assim de outras ofertas de certificação no mercado, dirigidas a entidades com preocupações de cibersegurança elementares e, portanto, com menor grau de exigência na obtenção dos certificados.

O EC QNRCS tem, por último, como objetivo contribuir para a execução da Resolução do Conselho de Ministros n.º 55/2020, que aprova a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, e da Resolução do Conselho de Ministros n.º 131/2021, que aprova a Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o atinente Plano de Ação Transversal para a legislatura, promovendo as devidas condições para a certificação de entidades da Administração Pública no QNRCS.

Resumem-se alguns benefícios e objetivos genéricos para as organizações certificadas no EC QNRCS:

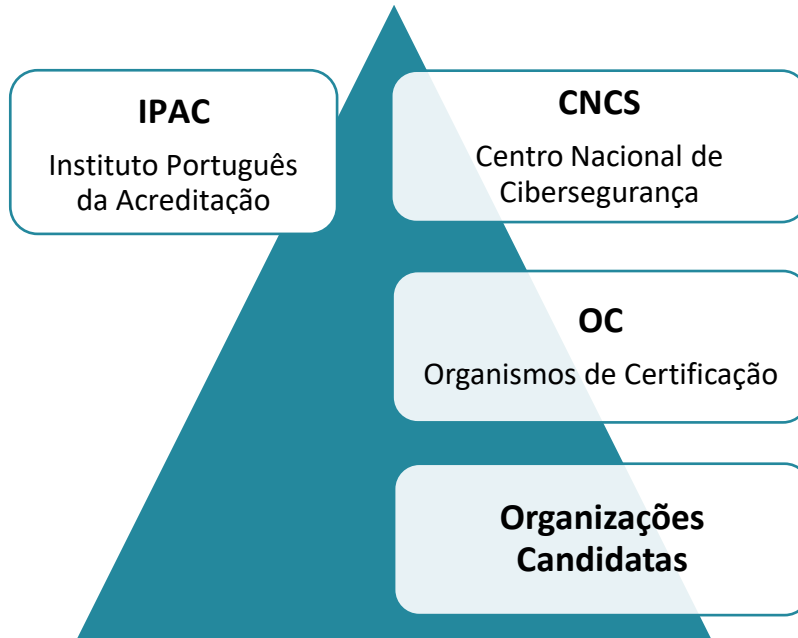
- Otimizar a aposta das organizações na gestão do risco, promovendo a melhoria contínua dos controlos de segurança em função dos níveis do risco percecionado que resulta das auditorias de certificação;
- Maior confiança dos utilizadores, fornecedores, clientes e parceiros;
- Melhorar o seu desempenho e eficácia operacional;
- Demonstrar o compromisso e a maturidade em matérias de cibersegurança e segurança da informação;
- Demonstrar a conformidade com requisitos legais e regulamentares de cibersegurança;
- Promover um diferencial competitivo no mercado em que se insere.

**Centro Nacional de Cibersegurança**



## 7. Papéis, funções e responsabilidades no Esquema de Certificação QNRCS

O modelo de governação do EC QNRCS está estruturado com base em 4 atores e/ou categorias de atores principais e correspondentes papéis:



Os papéis, funções e responsabilidades de cada um destes atores no EC QNRCS são apresentados na tabela seguinte:

Entidade(s) / siglas	Papéis	Funções e Responsabilidades
<b>IPAC</b>	Organismo nacional de acreditação	<ul style="list-style-type: none"> <li>• Prestar serviços de acreditação aos OC para execução do processo de certificação QNRCS</li> <li>• Tratar reclamações sobre os OC em articulação com o CNCS se necessário</li> <li>• Articular com o CNCS o processo de supervisão</li> <li>• Elaborar e publicar o esquema de acreditação dos OC para fins de certificação no EC QNRCS</li> </ul>
<b>CNCS</b>	Autoridade Nacional de Certificação da Cibersegurança	<ul style="list-style-type: none"> <li>• Elaborar, gerir, manter, atualizar e publicitar o Esquema de Certificação QNRCS</li> <li>• Disponibilizar uma proposta de metodologia para a gestão e análise do risco</li> <li>• Supervisionar os certificados emitidos e as organizações certificadas</li> <li>• Apoiar o IPAC na supervisão dos OC</li> <li>• Apoiar o IPAC na elaboração do esquema de acreditação dos OC para fins de certificação no EC QNRCS</li> <li>• Emitir os códigos QR a constar nos certificados</li> <li>• Gerir a página web para publicação dos certificados QNRCS</li> </ul>

		<ul style="list-style-type: none"> <li>Estabelecer-se como ponto de contacto para a cooperação internacional no plano da certificação europeia em cibersegurança</li> </ul>
<b>OC</b>	Organismos de certificação	<ul style="list-style-type: none"> <li>Obter e manter a acreditação pelo IPAC</li> <li>Receber e validar as candidaturas à certificação no EC QNRCS</li> <li>Executar o processo de certificação QNRCS</li> <li>Proferir a decisão de certificação QNRCS</li> <li>Emitir os certificados QNRCS e gerir os respetivos ciclos de vida</li> <li>Cumprir e fazer cumprir as regras e requisitos do EC QNRCS, incluindo a Política de divulgação dos certificados QNRCS</li> </ul>
<b>Organizações Candidatas</b>	Entidades públicas ou privadas candidatas à certificação QNRCS	<ul style="list-style-type: none"> <li>Cumprir com as obrigações legais a que está sujeita, em especial as alusivas à sua situação de cibersegurança</li> <li>Efetuar o procedimento de análise e gestão de risco alusiva à sua situação de cibersegurança</li> <li>Implementar todas as medidas de segurança previstas no EC QNRCS, exceto as medidas passíveis de exclusão que tenha decidido não aplicar em função da sua análise de risco</li> <li>Executar a candidatura a um nível de capacidade QNRCS</li> <li>Disponibilizar evidências de execução das medidas de segurança</li> <li>Cumprir as regras e requisitos do EC QNRCS, incluindo a Política de divulgação dos certificados QNRCS e as notificações de incidentes de cibersegurança</li> </ul>

## 8. Requisitos para os Organismos de Certificação

Um Organismo de Certificação (OC) deve ser uma organização acreditada pelo IPAC na norma ISO/IEC 17065 *Conformity assessment — Requirements for bodies certifying products, processes and services* para a execução do processo de certificação QNRCS.

Em complemento aos requisitos próprios da acreditação na norma ISO/IEC 17065, os OC devem assegurar o cumprimento dos seguintes requisitos específicos para a devida acreditação para a certificação no EC QNRCS:

- requisitos adicionais que venham eventualmente a ser definidos pelo CNCS e/ou pelo IPAC no âmbito do esquema de acreditação do EC QNRCS;
- assegurar a qualificação de auditores de certificação e de auditores peritos com as credenciais adequadas para a condução de auditorias EC QNRCS, a definir pelo CNCS e/ou pelo IPAC no âmbito do esquema de acreditação do EC QNRCS.

É obrigação dos OC observar as seguintes regras gerais do EC QNRCS:

- tratar a informação recebida das organizações candidatas com confidencialidade, assegurando o respetivo tratamento interno no estrito cumprimento das práticas de gestão da segurança da informação associada, nomeadamente em termos de controlo de acessos e de partilha com terceiras partes;
- cumprir os procedimentos de comunicação com o CNCS estabelecidos no âmbito do EC QNRCS;
- cumprir com todos os demais requisitos definidos no EC QNRCS para os OC, incluindo a Política de divulgação dos certificados QNRCS;
- participar nas atividades de supervisão do EC QNRCS pelo CNCS, sempre que solicitados nos casos aplicáveis.

- investigar e atuar diligentemente sobre situações de não conformidade detetadas em certificados por si emitidos, ou de incumprimento de regras do EC QNRCS por parte de organizações por si certificadas, comunicadas pelo CNCS ou por qualquer outra via chegadas ao seu conhecimento, tendo em vista o rápido restabelecimento da situação de conformidade dos certificados ou de cumprimento dos demais requisitos do esquema.

Os requisitos e regras a que os organismos de certificação estão assim sujeitos procuram garantir a sua qualificação e proficiência nas normas e procedimentos estabelecidos e amplamente reconhecidos em matérias de certificação e de cibersegurança, bem como a sua idoneidade, isenção e imparcialidade na condução dos processos de certificação. Como consequência, os certificados por estes emitidos beneficiam de credibilidade e de legitimidade nos mais diversos contextos de utilização, inclusive internacionais.

## 9. Requisitos para os candidatos à certificação QNRCS

As organizações candidatas à certificação no EC QNRCS devem:

- ter atividade e serem estabelecidas em território nacional;
- corresponder a uma única entidade legal;
- estar em situação de cumprimento para com as obrigações legais que sobre si impendem, especialmente as de cibersegurança, e, sobretudo, caso se trate de uma entidade abrangida pelo Regime Jurídico da Segurança do Ciberespaço;
- ter procedido a um levantamento de todas as atividades prosseguidas pela organização suportadas por Tecnologias de Informação e de Comunicação, à data da candidatura, com clara indicação da(s) atividade(s) principal(is), e fazer entrega do documento resultante ao OC<sup>11</sup>
- ter procedido à análise de risco requerida no QNRCS e determinar, como seu corolário:
  - a circunscrição de atividades da organização a que a certificação se irá aplicar;
  - as medidas de segurança do QNRCS designadas como passíveis de exclusão, definidas no **Anexo 1 – Lista de critérios de auditoria** deste documento, que não serão aplicáveis como medidas de tratamento dos riscos identificados;
- elaborar uma "Declaração de Aplicabilidade" nos moldes previstos no **Capítulo 4 – Objeto e âmbito de aplicação do Esquema de Certificação QNRCS**, em que estabeleça o conjunto das suas atividades que serão objeto da certificação, assim como as medidas de segurança passíveis de exclusão que não serão implementadas;
- eleger um nível de capacidade, apropriado às suas necessidades e capacidades de cibersegurança, para o qual pretendem atingir a certificação;
- ter implementadas todas as medidas de segurança QNRCS para o nível de capacidade a que se candidatam, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de risco;
- ter registadas as evidências da implementação de tais medidas de segurança, descritas no **Anexo 1 – Lista de critérios de auditoria** do esquema de certificação;
- disponibilizar e garantir a veracidade das informações e os contactos solicitados no formulário de candidatura, que deverá ser entregue a um OC;
- comprometer-se a comunicar ao OC qualquer incidente de cibersegurança que provoque impactos no que respeite à confidencialidade, integridade e disponibilidade da segurança das redes e dos sistemas

---

<sup>11</sup> Este documento ajudará o OC na análise e validação da "Declaração de Aplicabilidade", permitindo-lhe aferir se as atividades nucleares da organização estão corretamente identificadas, e se a análise de risco e a "Declaração de Aplicabilidade" são adequadas à realidade organizacional

de informação abrangidos no âmbito de certificação QNRCS da organização e que, por isso, afete a validade do certificado.

Os requisitos para os candidatos à certificação QNRCS devem ser analisados pelos OC, após a receção do respetivo formulário de candidatura à certificação QNRCS, acompanhado pela Declaração de Aplicabilidade.

O formulário de candidatura a enviar aos OC está disponível no **Anexo 3 – Formulário de candidatura à certificação**, através de uma hiperligação.

## 10. Níveis de capacidade versus níveis de garantia do EC QNRCS

### Níveis do EC QNRCS

O QACC distingue em três níveis de capacidade a implementação dos requisitos do QNRCS.

O EC QNRCS parte do conceito de níveis de implementação do QNRCS propostos no QACC e revê o grau de exigência no QACC das medidas atribuídas para cada um dos níveis, intensificando-o, tendo em consideração os destinatários principais deste esquema. Exige-se a implementação efetiva das medidas de segurança definidas pelo QNRCS e que serão matéria auditável, para geração de evidências de auditoria e posterior constatação de conformidade ou da sua ausência.

Os três diferentes níveis do EC QNRCS seguem a nomenclatura usada no enquadramento europeu de certificação da cibersegurança, denominando-se respetivamente “**Básico**” – “**Substancial**” – “**Elevado**”.

### Diferenciação de níveis

#### Básico

O nível de capacidade “Básico” deverá ser considerado como ponto de partida na jornada da cibersegurança, contemplando o estabelecimento de medidas e procedimentos de segurança introdutivos, embora robustos, para as entidades com um historial de cibersegurança incipiente ou que se iniciam nesta senda mediante a certificação QNRCS. Sublinhe-se o carácter vigoroso das medidas de segurança concebidas desde o nível “Básico”, pertinente às características dos candidatos destinatários preferenciais da certificação QNRCS e do papel central que ocupam na sociedade.

O alcance da certificação QNRCS mesmo no nível “Básico” configura uma capacitação em cibersegurança digna e relevante, apta à proteção da organização, das suas partes interessadas externas, sobretudo clientes, consumidores e utilizadores finais, a um ponto significativo para o panorama geral de segurança do ciberespaço nacional.

#### Substancial

As medidas de segurança do nível de capacidade “Substancial” densificam as medidas do nível “Básico” tendo por destinatários as organizações que já obtiveram a certificação nesse nível, que dispõem de certificações em outros esquemas de cibersegurança ou em normas certificáveis da segurança da informação (como a ISO 27001) ou que já têm instituídas e solidificadas as práticas e procedimentos de cibersegurança nucleares.

#### Elevado

O nível de capacidade “Elevado” contempla medidas que acrescentam substrato notável às medidas definidas para os níveis anteriores, traduzindo-se num destacado aperfeiçoamento das práticas de cibersegurança da organização. Destina-se por isso a organizações com dedicação de importantes recursos à cibersegurança, que têm excecionais necessidades de cibersegurança ou para quem a cibersegurança é um fator diferenciador ou

decisivo, inclusive para as suas partes interessadas externas. Considera-se que as entidades que obtenham a certificação do EC QNRCS a um nível “Elevado” demonstram capacidades de facto avançadas em cibersegurança.

## Progressividade

A progressividade dos níveis de capacidade do EC QNRCS redonda numa escalada de exigência nos requisitos de implementação das medidas do QNRCS de nível para nível, a que necessariamente corresponde uma escalada de exigência respeitante às evidências associadas às implementações que devem ser apresentadas perante os OC.

Este atributo é demonstrado nas diferenças entre níveis dos requisitos de implementação das medidas e das evidências solicitadas, contidas no **Anexo 1 – Lista de critérios de auditoria** do EC QNRCS.

## Cumulabilidade

Os níveis são complementares e cumulativos, o que significa que:

- se a organização pretender ser certificada no nível “Básico”, deverá ter implementadas todas as medidas previstas para o nível “Básico” conforme definidas no **Anexo 1 – Lista de critérios de auditoria**, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de risco;
- se a organização pretender ser certificada no nível “Substancial”, deverá ter implementadas todas as medidas previstas para os níveis “Básico” e “Substancial”, conforme definidas no **Anexo 1 – Lista de critérios de auditoria**, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de risco;
- se a organização pretender ser certificada no nível “Elevado”, deverá ter implementadas todas as medidas previstas para os níveis “Básico”, “Substancial” e “Elevado”, conforme definidas no **Anexo 1 – Lista de critérios de auditoria**, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de risco.

Procura-se desta forma proporcionar às organizações destinatárias uma via de crescimento e de progressão em cibersegurança, compatível com as suas capacidades e necessidades, e da qual consigam gerir o ritmo de evolução, ao mesmo tempo que robustecem as práticas já adquiridas.

## Níveis de capacidade versus níveis de garantia

No contexto do EC QNRCS, cada organização deve identificar e seleccionar o nível de capacidade para o qual pretende atingir a sua certificação.

Quando o resultado de auditoria comprova que a organização está em conformidade com os requisitos de um determinado nível e apta para receber o devido certificado de conformidade, este nível passa a ser identificado como “nível de garantia em cibersegurança”.

## Seleção de níveis de capacidade e candidatura

As organizações candidatam-se a um nível de capacidade através de um formulário disponível por meio de uma hiperligação no **Anexo 3 – Formulário de candidatura à certificação**, que deve ser entregue junto de um OC.

O nível de candidatura seleccionado pela organização deverá, fundamentalmente, ter em conta as suas capacidades de cibersegurança, as suas necessidades de cibersegurança, inferidas do processo de análise e gestão de risco, e os eventuais requisitos legais a que esteja obrigada, mais o esforço, incluindo o custo, de



efetivação das medidas do QNRCS, a imagem que tenciona transmitir como consequência da certificação, e outros fatores que lhe possam ser exclusivos.

O OC escolhido pela organização candidata analisa a candidatura, podendo, em condições normais, aceitar o nível proposto, ou informar a organização candidata da eventual inexistência de condições para obtenção da certificação no nível pretendido, caso as informações patentes nos documentos de candidatura desde logo fortemente o indiquem.

## Validação do nível selecionado

Durante as auditorias descritas no **Capítulo 11 – Ciclo de vida e processo de certificação QNRCS** do presente documento, integrantes do ciclo de vida da certificação, a equipa auditora, em representação do OC, pode confirmar que a organização tem condições para atingir o nível de capacidade selecionado, ou, se for o caso, deverá informar a organização candidata e o OC que a análise das evidências recolhidas é consistente com o enquadramento num outro nível de capacidade. A organização candidata poderá então solicitar a obtenção da certificação num nível diverso do originalmente declarado, evitando o insucesso na certificação.

## Aumento do nível de capacidade

Se a proposta de alteração do nível da capacidade se traduzir num aumento de nível em relação ao qual a organização originalmente se candidatou, a organização poderá ter de completar a candidatura no que seja aplicável ao novo nível.

## Redução do nível de capacidade

Se a proposta de alteração do nível da capacidade se traduzir numa redução de nível em relação ao qual a organização originalmente se candidatou, o processo poderá decorrer normalmente.

Se a organização, após estar certificada, solicitar uma redução do nível de garantia do certificado, a alteração poderá ser feita administrativamente, salvo se existir algum motivo não previsto que possa ser lícito.

## 11. Ciclo de vida e processo de certificação QNRCS

Entende-se por “ciclo de vida da certificação QNRCS” a execução do EC QNRCS na sua globalidade.

### Ciclo de vida

#### Validade dos certificados

O período de validade dos certificados de conformidade com o QNRCS é de três anos após a emissão, salvo motivo superveniente que conduza à sua anulação antes daquele prazo.

#### Manutenção da certificação

A manutenção da validade do certificado requer a realização de uma auditoria de acompanhamento transcorrido cada ano, ou seja, deverá ser efetuada uma primeira auditoria de acompanhamento passado um ano da auditoria de concessão e uma segunda auditoria de acompanhamento passados dois anos.

Compete ao OC agendar as auditorias, tendo em atenção os prazos abaixo estipulados e a organização certificada deverá cooperar no sentido de se manter disponível e assegurar o bom curso das auditorias.

#### Renovação da certificação

O ciclo de certificação renova-se ao terceiro ano, por meio de uma auditoria de renovação, à qual são aplicáveis os requisitos acima descritos.

## Processo de certificação QNRCS

O processo de certificação QNRCS pode-se resumir através do seguinte encadeamento de etapas e prazos associados:

1. Candidatura da organização à certificação QNRCS junto do OC
2. Análise e validação da candidatura pelo OC
  - o OC tem um prazo de 15 dias úteis para confirmar, ou não, a aceitação de uma candidatura;
3. Realização da auditoria de concessão pelo OC
  - deve ser iniciada num prazo previamente acordado entre as partes, mas que não deve ultrapassar 90 dias de calendário;
  - é verificada a implementação das medidas exigidas, considerando o nível de capacidade manifestado na candidatura, através dos critérios e evidências definidos no **Anexo 1 – Lista de critérios de auditoria**;
  - caso sejam detetadas não conformidades, dever-se-ão encetar os passos detalhados no **Capítulo 14 – Regras para o tratamento de "Não Conformidades"**;
4. Análise e revisão do relatório de auditoria e das evidências apuradas por parte do OC
5. Decisão de certificação pelo OC
  - quando demonstrada a conformidade em todas as medidas de segurança associadas ao nível de capacidade pretendido, com possível exceção das medidas passíveis de exclusão;
6. Emissão de certificado pelo OC
  - com um período de validade de 3 anos;
7. Publicação dos certificados QNRCS pelas organizações candidatas, OC e CNCS
  - num prazo máximo de 5 dias úteis após a emissão do certificado de conformidade;
  - de acordo com as práticas definidas pela **Política de divulgação dos certificados QNRCS** (ver **Anexo 5**), e contendo a informação definida pelo documento **Modelo e marcas dos certificados QNRCS** (ver **Anexo 4**);
8. Realização da auditoria de acompanhamento anual<sup>12</sup>
  - deve ter uma variação máxima de 30 dias de calendário em relação ao mês e finalização da auditoria de concessão;
9. Realização da auditoria de renovação da certificação QNRCS / início de novo ciclo<sup>13</sup>
  - deve ser realizada até 30 dias de calendário anteriores ao término da data de validade do certificado QNRCS em vigor;
10. Realização de auditorias extraordinárias
  - sempre que
    - i. após a certificação, ocorram alterações significativas na organização certificada e que sejam consideradas no âmbito de certificação QNRCS ou que tenham consequências na definição desse âmbito<sup>14</sup>;
    - ii. no seguimento de auditorias prévias de concessão, de renovação ou de acompanhamento, para a confirmação da execução com eficácia de um Plano de Ações Corretivas
    - iii. o OC o determine, para verificação de uma situação de incumprimento chegada ao seu conhecimento;
    - iv. determinadas pelo CNCS na sua qualidade de ANCC.

<sup>12</sup> A iniciativa de marcar as auditorias previstas no ciclo – de acompanhamento ou de renovação – é da responsabilidade do OC

<sup>13</sup> Ver comentário anterior

<sup>14</sup> Exceto se se tratar de uma redução geral do âmbito sem concurso de acréscimo de atividades

As auditorias extraordinárias são utilizadas quando a organização certificada quer alterar os pressupostos iniciais da certificação (mudança de instalações, fusão, extensão do âmbito, entre outras). Estas auditorias podem ser efetuadas em qualquer momento entre as auditorias planeadas.

As auditorias extraordinárias podem ainda ocorrer, por decisão do OC, na sequência de uma notificação pela organização certificada de um incidente de cibersegurança que provoque impactos no que respeita à confidencialidade, integridade e disponibilidade da segurança das redes e dos sistemas de informação abrangidos no âmbito de certificação QNRCS da organização e que, por isso, afete a validade do certificado.

## 11. Revogação de certificados QNRCS pelos OC

- no caso de não cumprimento pelas organizações candidatas das regras definidas pelo EC QNRCS;
- a decisão de revogação deve ser comunicada à organização certificada e ao CNCS no prazo máximo de 5 dias úteis.

## Estados dos certificados

Os certificados QNRCS emitidos pelo OC podem estar associados aos seguintes estados:

- Atribuído – quando da decisão positiva de certificação da conformidade com o QNRCS pelo OC.
- Suspenso – pode ocorrer a necessidade de suspensão de um certificado QNRCS, pelo menos nas seguintes circunstâncias, entre outras:
  - Execução não eficaz de um Plano de Ações Corretivas pela organização candidata;
  - Pedido de alteração do âmbito de aplicação QNRCS pela organização certificada (exceto se se tratar de uma redução do âmbito);
  - Identificação de não conformidades associadas ao certificado ou de incumprimentos das regras do EC QNRCS por parte da organização certificada, através da comunicação pelo CNCS ao OC das irregularidades detetadas durante as atividades de supervisão do EC QNRCS, ou por qualquer outra via chegadas ao seu conhecimento.

O prazo de suspensão de um certificado QNRCS não pode ultrapassar 6 meses.

A suspensão da certificação deve ser levantada quando se demonstrar que a causa que esteve na origem da suspensão da certificação já não existe. O levantamento da suspensão da certificação pode ser feito através da análise de evidências documentais, quando suficiente, ou através de auditorias que não substituem as auditorias previstas do ciclo de certificação.

Durante o período de suspensão da certificação, a entidade certificada não pode fazer qualquer referência ao estatuto de entidade certificada e fica impossibilitada de utilizar a marca de certificação.

Após o levantamento da suspensão, o ciclo de certificação é retomado, mantendo-se a data de validade original do certificado de conformidade, não havendo lugar a qualquer prorrogação do seu prazo de validade.

- Revogado – quando o OC identifica ou é informado de situações de não cumprimento do EC QNRCS por parte da organização certificada, inclusive através de comunicação pelo CNCS no seguimento das suas atividades de supervisão do EC QNRCS, e designadamente nos casos em que, estando o certificado suspenso, não há pela organização certificada a observância do disposto pelo OC para restabelecimento da conformidade e levantamento da suspensão. É ainda aplicada nas situações de encerramento da organização (falência ou deslocação para outra zona geográfica), e/ou no caso de compra por, ou fusão com, outra organização não certificada.

Neste caso, a organização não pode fazer qualquer referência ao estatuto de entidade certificada, bem como não pode fazer qualquer utilização do certificado de conformidade e da marca e/ou rótulo de certificação.

- Expirado – quando o certificado QNRCS atingiu o final do seu prazo de validade.

A notificação pelo OC ao CNCS da alteração de estado de um certificado QNRCS deve ocorrer no prazo máximo de 5 dias úteis.

A publicação, pelas partes respeitantes, das informações referentes à alteração do estado de um certificado deve ser efetuada o mais brevemente possível desde a data de ocorrência da alteração ou do recebimento da respetiva notificação, consoante se aplique, mas não deverá ultrapassar o prazo de 10 dias úteis desde a data de ocorrência da alteração de estado.

## Transferência

O EC QNRCS admite a transferência da certificação entre OC pela organização certificada mediante as seguintes condições:

- o certificado estar dentro de prazo de validade;
- ambos os OC envolvidos no procedimento de transferência devem estar devidamente acreditados para este esquema.

Deve ser solicitado ao OC que originalmente emitiu o certificado uma declaração em como as auditorias do presente ciclo se encontram todas realizadas e as não conformidades encerradas, e de que não existem incidências pendentes com a organização a transferir (por exemplo, reclamações ou dívidas).

O OC que emitiu originalmente o certificado não poderá anular o certificado antes de todas as atividades de transferência estarem concluídas.

Na eventualidade do certificado atingir o termo da validade durante as atividades de transferência, o certificado a emitir pelo novo OC apresentará um intervalo entre a data de validade do certificado anterior e a data de emissão do novo.

A auditoria de transferência deve ser efetuada antes do termo de validade do certificado.

A transferência pode ser efetuada em qualquer altura do ciclo de certificação, no entanto a auditoria de transferência deve ser equiparada a uma auditoria de recertificação, para que o novo OC e a respetiva equipa auditora possam fazer uma análise adequada da documentação e das práticas da organização transferida.

A auditoria de transferência inclui a análise dos relatórios do ciclo anterior e o teor das não conformidades das auditorias, de modo a identificar e avaliar recorrências.

A auditoria decorrerá de acordo com o estipulado para as restantes auditorias.

O novo certificado deve dar continuidade à validade do certificado do OC anterior, com um prazo de validade de 3 anos.

## Anulação voluntária

A qualquer altura do ciclo de certificação a organização poderá pedir a anulação do seu certificado, enviando um pedido para o OC, que comunicará essa decisão ao CNCS.

## Incumprimento das regras do EC QNRCS

Em cumprimento do disposto pelo Art.º 21º do Decreto-Lei n.º 65/2021, a organização certificada estará sujeita a sanções no caso de incorrer nas infrações nele previstas, sendo o CNCS, na qualidade de ANCC, a entidade responsável pela sua aplicação.

## 12. Análise e gestão do risco

O QNRCS compreende conjuntos de medidas de segurança tendentes ao prosseguimento dos seus cinco objetivos – Identificar, Proteger, Detetar, Responder e Recuperar.

A implementação das medidas do QNRCS para fins de certificação requer a condução de um processo de análise e gestão do risco.

Em particular, o **Anexo 1 – Lista de critérios de auditoria** do QNRCS consigna, de entre todas as medidas do QNRCS, a classificação destas como sendo de aplicação obrigatória, para todas as entidades e independentemente do risco a que estão sujeitas, ou como sendo medidas passíveis de exclusão, que a organização candidata, partindo de uma análise de risco e da perceção informada do risco que sobre ela incorre, identifica como não lhe sendo aplicáveis para o tratamento do seu risco específico, pelo que poderá optar por não as implementar.

A realização da análise e gestão de risco é assim uma pré-condição para a certificação QNRCS.

Existem diferentes metodologias de análise e gestão de risco, que implicam o emprego de diferentes técnicas ou sequências dos procedimentos para se atingir o mesmo fim ou se obter resultados igualmente válidos. Certas metodologias estão bastante bem estabelecidas e são reconhecidas como metodologias confiáveis para a obtenção de cenários factuais do risco associado à organização e do seu tratamento.

### Aceitação do uso de metodologias estabelecidas

Algumas organizações realizam regularmente procedimentos de gestão de risco, por vezes trabalhados com o apoio de entidades externas contratadas. A escolha da metodologia a adotar é feita em razão da sua adequação às características, como as capacidades, e os objetivos de segurança da organização.

Havendo tais procedimentos de análise e gestão de risco em uso na organização, e contendo estes os elementos essenciais que um processo fidedigno deve apresentar, conforme detalhado no Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança e no QNRCS, a organização deverá continuar a executar os procedimentos que já tem enraizados nas suas atividades de cibersegurança e que estarão adaptados às suas necessidades e realidade organizacional.

### Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança

Reconhece-se, no entanto, que muitas potenciais candidatas à certificação QNRCS poderão não ter tido ainda a experiência de realizar uma análise de risco, ou não ter tais práticas sedimentadas.

Para esses casos, recomenda-se a adoção de uma metodologia para a análise e gestão do risco definida pelo CNCS, disponibilizada através de um documento exógeno, mas complementar, ao EC QNRCS, o citado Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança, e que é congruente com os passos relatados no capítulo 3.5 do QNRCS.

A metodologia estruturada neste Guia determina um processo para gestão do risco, apresentando as regras e práticas admissíveis para a realização da análise do risco e para a realização da identificação das medidas para tratamento do risco.



## Elementos essenciais para o processo de análise e gestão de risco

Em súmula, menciona-se que a organização candidata tem de implementar:

- O processo para gestão do risco;
- O inventário dos ativos presentes nas atividades incluídas pela organização candidata no seu âmbito de certificação;
- A lista de ameaças, vulnerabilidades e riscos aplicáveis aos ativos inventariados;
- Os critérios para a avaliação e aceitação do risco, nomeadamente os níveis de probabilidade de ocorrência da ameaça e o nível de impacto nas atividades a proteger pelo âmbito de certificação;
- O relatório de análise do risco;
- Os tratamentos do risco que serão implementados para a redução do risco para um nível aceitável pela organização candidata.

A organização candidata executa a sua análise do risco em estrito cumprimento de uma metodologia que inclua os elementos acima listados, produzindo como resultado da sua aplicação o documento obrigatório designado por “Declaração de Aplicabilidade”, descrito no **Capítulo 4 – Objeto e âmbito de aplicação do Esquema de Certificação QNRCS**.

Este documento apresenta as decisões da organização em relação à aplicabilidade, ou não, das medidas de segurança para o nível de capacidade a que se candidata descritas no **Anexo 1 – Lista de critérios de auditoria** do EC QNRCS como passíveis de exclusão, assim como a respetiva justificação para cada decisão.

## Validação pelos OC dos documentos de análise de risco

Para efeitos de recorte da informação, ponderação e validação das análises de risco individualizadas executadas pelas organizações candidatas e, periodicamente, pelas organizações detentoras de certificados QNRCS, devem os OC consultar e ter em consideração os resultados das análises de risco da cibersegurança setoriais que o CNCS venha a publicar.

## 13. Métodos de avaliação e critérios de auditoria

A conformidade de uma organização candidata à certificação QNRCS resulta da decisão do OC, em função dos resultados obtidos na auditoria de certificação.

Esta decisão é alcançada através da análise de evidências recolhidas durante os atos de auditoria, comparando com os critérios elencados no **Anexo 1 – Lista de critérios de auditoria** deste EC QNRCS, referentes à aplicação das medidas do QNRCS.

Nas auditorias de concessão e de renovação deve ser verificada a implementação de todos os requisitos e devidas evidências.

Nas auditorias de acompanhamento anuais, o OC deverá selecionar quais as medidas a verificar entre a primeira e a segunda auditoria anual, sendo que no cômputo de ambas deverão ser verificadas todas as medidas exigidas para o seu nível de garantia que lhe são aplicáveis (i.e., todas as medidas do QNRCS, exceto as medidas passíveis de exclusão que são particulares à organização, conforme Declaração de Aplicabilidade).

O **Anexo 1 – Lista de critérios de auditoria** identifica as evidências de conformidade que a organização candidata deve apresentar, e que deverão ser confirmadas pelo OC no decurso da auditoria, sendo que poderão ser solicitadas evidências adicionais em função das características específicas dos produtos, sistemas, recursos, serviços, processos e procedimentos da organização.

Os critérios de auditoria de certificação correspondem às medidas de segurança e respetivas evidências definidas no **Anexo 1 – Lista de critérios de auditoria** do EC QNRCS para cada nível de capacidade.

Compete ao OC a análise do conjunto de evidências recolhidas e a produção de constatações de conformidade sustentadas, em cada medida de segurança analisada.

No entanto, da análise de cada medida de segurança, para além da conformidade, podem resultar outras constatações referidas abaixo:

- **Não conformidade Maior** – Ocorre nos casos em que a medida de segurança não se encontra implementada ou, se implementada, encontra-se totalmente desalinhada dos objetivos da medida de segurança, sendo que, de tais factos, decorre um impacto conducente à anulação de qualquer efeito ou garantia de segurança e/ou de proteção que a implementação de tal medida pretendesse proporcionar;
- **Não conformidade Menor** – Ocorre nos casos em que a medida de segurança encontra-se implementada, mas não consegue demonstrar totalmente que cumpre os respetivos objetivos;
- **Oportunidade de Melhoria** – Ocorre nos casos em que a medida de segurança encontra-se implementada, consegue demonstrar a obtenção dos respetivos objetivos, mas não o está a fazer da forma mais eficaz. Poderá ainda ser associada a situações em que a oportunidade de melhoria possa prevenir futuras não conformidades.

## 14. Regras para o tratamento de “Não Conformidades”

No seguimento do disposto pelo **Capítulo 13 – Métodos de avaliação e critérios de auditoria** do EC QNRCS, poderão ocorrer situações em que os resultados de auditoria identifiquem não conformidades.

As diligências para resolução de não conformidades devem exibir o seguinte encadeamento:

1. O OC informa a organização candidata sobre as não conformidades detetadas, identificando-as, e solicita a entrega de um Plano de Ações Corretivas (PAC)
2. Entrega ao OC do PAC pela organização candidata
3. Avaliação do PAC pelo OC
  - Se o PAC for aceite, é concedido um prazo para a organização candidata implementar as medidas corretivas do PAC dentro dos prazos e moldes previstos mais abaixo
  - Se o PAC contiver medidas para encerramento de não conformidades maiores e não for aceite pelo OC, este declara parecer negativo para certificação e o processo termina
4. No caso de se estarem a tratar não conformidades maiores, deverá ser efetuada uma auditoria de seguimento pelo OC para verificação da implementação das medidas antes da emissão da decisão e do certificado

Para encerrar as Não conformidades, a organização candidata deve proceder à criação e entrega ao OC, no prazo máximo de 30 dias de calendário desde a apresentação da Não Conformidade, de um Plano de Ações Corretivas (PAC) onde estabelece as ações a implementar, responsáveis e prazos de implementação.

O OC deve analisar a proposta de PAC, informando a organização candidata da sua aprovação ou não aprovação, no prazo máximo de 10 dias úteis.

Para encerramento de Não conformidades Maiores, e após aprovação do PAC pelo OC, a organização candidata deve apresentar as evidências de implementação dentro de um prazo máximo de 30 dias de calendário desde a apresentação da Não Conformidade.

Para encerramento das Não conformidades menores, a organização deverá produzir e enviar um PAC ao OC, implementando as ações nele constantes o mais rapidamente possível dentro de um prazo não superior a 60 dias

**Centro Nacional de Cibersegurança**

de calendário desde a apresentação da Não Conformidade. As evidências de implementação serão obrigatoriamente verificadas na próxima auditoria de acompanhamento.

O certificado só será emitido com todas as evidências de implementação das ações relativas às Não conformidades Maiores aceites pelo OC, e com o PAC aprovado pelo OC no caso de lhe terem sido identificadas Não conformidades menores.

## 15. Regras para a gestão dos certificados de conformidade QNRCS

Os certificados de conformidade QNRCS devem ser emitidos pelo OC de acordo com as regras definidas pelo **Anexo 4 – Modelo e marcas dos certificados QNRCS** do Esquema de Certificação QNRCS.

## 16. Política de divulgação dos certificados de conformidade QNRCS

A Política de divulgação dos certificados QNRCS tem como objetivo descrever as regras e práticas para a divulgação dos certificados emitidos pelos OC, no contexto do Esquema de Certificação do QNRCS. Este documento é acessível no **Anexo 5 – Política de divulgação dos certificados QNRCS**, através de uma hiperligação.

## 17. Regras para acesso, arquivo e preservação de informações relativa à certificação

Os OC devem manter um sistema de registos de acordo com os requisitos da norma de acreditação ISO/IEC 17065, que, no que diz respeito à respetiva segurança da informação, deve ser implementado e gerido tendo em conta as práticas definidas pelo controlo A.18.1.3 da norma ISO/IEC 27001.

Todos os documentos que resultam de, ou suportem as, atividades de certificação ao abrigo do presente Esquema de Certificação devem ser classificados como “Informação Confidencial”.

O respetivo acesso deve assim ser realizado através de controlos de segurança da informação que o permitam restringir apenas a colaboradores do CNCS, do IPAC, I.P. e de outras autoridades e organismos envolvidos que estejam formalmente autorizados por cada entidade a ter acesso aos documentos, utilizarem a informação neles contida para as suas tarefas de certificação e de supervisão, assim como para executarem os procedimentos de arquivo e preservação.

Para além de garantir a total confidencialidade sobre todos os assuntos envolvidos na certificação e tratar como confidencial toda a informação e documentação a que tenha acesso no âmbito da sua atuação, sendo esta obrigação extensível a todas as partes, incluindo colaboradores ou terceiros que as mesmas envolvam, todas as entidades envolvidas devem guardar sigilo sobre toda a informação e documentação técnica e não técnica, comercial ou outra, relativa à organização candidata à certificação, de que possa ter conhecimento ao abrigo ou em relação ao processo de certificação QNRCS.

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 das atividades decorrentes do processo de certificação.

Exclui-se do dever de sigilo previsto a informação e a documentação que forem comprovadamente do domínio público à data da respetiva obtenção pelo CNCS e/ou pelo OC, ou que estes sejam legalmente obrigados a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes. Salvo disposição em contrário neste esquema e sem prejuízo das disposições

**Centro Nacional de Cibersegurança**

vigentes em matéria de confidencialidade, todas as partes envolvidas na aplicação do presente esquema devem respeitar a confidencialidade das informações e dos dados obtidos no desempenho das suas tarefas, a fim de proteger:

- dados pessoais, de acordo com os requisitos do Regime Geral de Proteção de Dados - Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016;
- informações comerciais confidenciais e segredos comerciais de qualquer pessoa singular ou coletiva, incluindo direitos de propriedade intelectual, exceto quando, por motivo extraordinário e devidamente fundamentado, a divulgação for necessária para salvaguardar o interesse público, ou por ter sido ordenada judicialmente;
- informações necessárias para a implementação eficaz deste esquema, em particular para efeitos de colaboração eficaz entre as autoridades e organismos envolvidos e o tratamento das reclamações.

A preservação, pela organização certificada, de documentos e registos das informações disponibilizadas aquando do processo de certificação, seja em formato digital ou em papel, deve ser assegurada durante um prazo mínimo de 5 anos após o término da data de validade do certificado, sendo obrigatório manter as práticas de segurança da informação durante este período de tempo definidas pelo OC para o controlo A.18.1.3 da norma ISO/IEC 27001. Esses registos devem incluir toda a documentação e evidências disponibilizadas ao organismo de certificação durante a certificação, incluindo aquelas que foram disponibilizadas apenas de forma restrita, por tempo limitado ou apenas nas instalações da entidade certificada.

## 18. Supervisão do ciclo de vida dos certificados de conformidade QNRCS

Conforme exposto no **Capítulo 1 – Contexto do Esquema de Certificação QNRCS** deste EC QNRCS, o CNCS é a Autoridade Nacional de Certificação da Cibersegurança, atuando de acordo com as funções, atribuições, responsabilidades e competências inerentes a tal qualidade.

Neste contexto, as atividades de supervisão e gestão que o CNCS executa no contexto do Esquema de Certificação QNRCS são, entre outras, as seguintes:

- Gestão da publicação dos certificados de conformidade, em página web dedicada,;
- Monitorização dos certificados emitidos e das organizações que os titulam;
- Comunicação aos OC, para as diligências que devidamente lhes competem, de quaisquer não conformidades para com os requisitos de certificação dos certificados por aqueles emitidos, ou de qualquer incumprimento das regras do EC QNRCS cometido por organizações certificadas, detetados durante as ações de supervisão levadas a cabo pelo CNCS, ou por qualquer outra via chegados ao seu conhecimento;
- Apoio técnico ao IPAC, a seu pedido e mediante a sua coordenação, na supervisão das atividades dos OC e na resolução de divergências entre os OC e as organizações candidatas;
- Comunicação ao IPAC de qualquer incumprimento das regras do EC QNRCS cometido por organismos de certificação, incluindo a omissão de atuação que lhes fosse exigida, designadamente, para com as organizações por aqueles certificadas que se revelem em situação de incumprimento, detetada durante as ações de supervisão levadas a cabo pelo CNCS, ou por qualquer outra via chegada ao seu conhecimento;
- Aplicação de sanções e penalidades na sequência de incumprimentos do EC QNRCS;
- Incentivo às organizações certificadas para uma cultura de conformidade permanente e de melhoria contínua;
- Publicação de guias de esclarecimentos e boas práticas.

## 19. Histórico de revisões

Versão	Data	Modificação	Notas adicionais
<b>VERSÃO 1.1</b>	22/12/2021	Criação	Versão inicial para revisão
<b>VERSÃO 1.5</b>	28/12/2021	Integração de resultados de revisões	Versão entregue para publicação
<b>VERSÃO 1.8</b>	30/12/2021	Integração de resultados de revisões	Versão aprovada para publicação
<b>VERSÃO 1.10</b>	14/01/2022	Inclusão da existência de medidas obrigatórias e passíveis de exclusão em função da gestão do risco, definidas no Anexo 1	
<b>VERSÃO 1.11</b>	20/01/2022	Diversas alterações	
<b>VERSÃO 1.12</b>	24/01/2022	Alterações produzidas pela revisão do Anexo 1	
<b>VERSÃO 1.13</b>	26/01/2022	Correções diversas	NC Grave passou a NC Maior
<b>VERSÃO 1.14.3</b>	22/05/2022	Reformulação geral do Esquema. Integração de alterações motivadas pela revisão do Anexo 1	
<b>VERSÃO 2.0</b>	08/06/2022	Revisão geral. Integração de alterações motivadas pela revisão do esquema e do Anexo 1	Versão disponibilizada para a segunda consulta pública
<b>VERSÃO 2.1</b>	26/08/2022	Revisão geral. Introdução de informação sobre análises de risco de cibersegurança setoriais e clarificação da atuação do CNCS em sede de supervisão, e de alguns deveres dos OC.	
<b>VERSÃO 2.3</b>	07/12/2022	Revisão geral de carácter editorial. Reformulações e pequenos acrescentos ao esquema decorrentes das interações com o IPAC, I.P. e o IPQ, I.P., para o tornar mais explícito e tendo como propósito a sua validação formal.	
<b>VERSÃO 2.4</b>	29/12/2022	Pequenas revisões editoriais e ortográficas e alinhamento com nova numeração dos Anexos.	Versão para publicação pelo CNCS

## 20. ANEXOS

### Anexo 1 – Lista de critérios de auditoria

O documento que contém a lista de critérios aplicáveis ao EC QNRCS pode ser encontrado [aqui](#).

### Anexo 2 – Lista de referências legais, normativas e regulamentares

A lista de referências aplicáveis ao Esquema de Certificação do QNRCS pode ser encontrada [aqui](#).



## Anexo 3 – Formulário de candidatura à certificação

O formulário de candidatura das organizações à certificação QNRCS, para envio a um OC, pode ser encontrado [aqui](#).

## Anexo 4 – Modelo e marcas dos certificados QNRCS

O documento que descreve o modelo e marcas do certificado QNRCS pode ser encontrado [aqui](#).

## Anexo 5 – Política de divulgação dos certificados QNRCS

O documento que contém a política de divulgação dos certificados de conformidade QNRCS pode ser encontrado [aqui](#).