Índice

Sumário 3

1. Contexto histórico do Esquema de Certificação QNRCS 4

Quadro Nacional de Referência para a Cibersegurança e referenciais associados 4

Autoridade Nacional de Certificação da Cibersegurança 4

Um esquema de certificação da cibersegurança para as organizações nacionais 5

2. Glossário do Esquema de Certificação QNRCS 5

3. Descrição e caracterização do Esquema de Certificação QNRCS 6

Conceitos 7

Caracterização e síntese descritiva 7

Destinatários 8

Dono do esquema e entidade supervisora 9

4. Objeto e âmbito de aplicação do Esquema de Certificação QNRCS 9

Âmbito de aplicação 9

Delimitação do contexto de atividade aplicável e decisão de exclusão de medidas do QNRCS 9

Declaração de Aplicabilidade 9

Alteração do âmbito 10

Redução do âmbito 10

Exclusões 10

5. Referências legais, normativas e regulamentares 10

6. Objetivos do Esquema de Certificação QNRCS 11

7. Papéis, funções e responsabilidades no Esquema de Certificação QNRCS 12

8. Requisitos para os Organismos de Certificação 14

9. Requisitos para os candidatos à certificação QNRCS 14

10. Níveis de capacidade versus níveis de garantia do EC QNRCS 15

Níveis do EC QNRCS 15

Diferenciação de níveis 15

Básico 15

Substancial 16

Elevado 16

Progressividade 16

Cumulabilidade 16

Níveis de capacidade versus níveis de garantia **17**

Seleção de níveis de capacidade e candidatura **17**

Validação do nível selecionado **17**

Aumento do nível de capacidade 17

Redução do nível de capacidade 17

11. Ciclo de vida e processo de certificação QNRCS ***17***

Ciclo de vida **18**

Validade dos certificados 18

Manutenção da certificação 18

Renovação da certificação 18

Processo de certificação QNRCS **18**

Estados dos certificados **19**

Transferência **20**

Anulação voluntária **20**

Incumprimento das regras do EC QNRCS **21**

12. Análise e gestão do risco ***21***

Aceitação do uso de metodologias estabelecidas **21**

Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança **21**

Elementos essenciais para o processo de análise e gestão de risco **21**

13. Métodos de avaliação e critérios de auditoria ***22***

14. Regras para o tratamento de "Não Conformidades" ***23***

15. Regras para a gestão dos certificados de conformidade QNRCS ***24***

16. Política de divulgação dos certificados de conformidade QNRCS ***24***

17. Regras para acesso, arquivo e preservação de informações relativa à certificação ***24***

18. Supervisão do ciclo de vida dos certificados de conformidade QNRCS ***25***

19. Histórico de revisões ***25***

20. ANEXOS ***26***

Anexo 1 – Lista de referências legais, normativas e regulamentares **26**

Anexo 2 – Formulário de candidatura a certificação **26**

Anexo 3 – Modelo de certificado QNRCS **26**

Anexo 4 – Política de divulgação dos certificados de conformidade QNRCS **26**

Anexo 5 – Critérios de auditoria para o esquema de certificação QNRCS **26**

Sumário

A desenvolver…

*Na sequência da aplicação do art.º 58 do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, e do art.º 20 do Decreto-Lei n.º 65/2021, de 30 de julho, o **CNCS** – Centro Nacional de Cibersegurança foi designado **ANCC** – Autoridade Nacional de Certificação em Cibersegurança, tendo a seu cargo a definição e implementação do **QNCC** – Quadro Nacional de Certificação em Cibersegurança.*

1. Contexto histórico do Esquema de Certificação QNRCS

Quadro Nacional de Referência para a Cibersegurança e referenciais 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.

O QNRCS procura refletir a realidade organizacional portuguesa, disponibilizando 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, Deteção, 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), enquanto referencial que define três diferentes níveis de capacidade – Básico, Substancial e Elevado – para a autoavaliação da aquisição das práticas de segurança do QNRCS que as organizações implementam e operacionalizam, considerando o seu contexto e dimensão, procurando cumprir os citados objetivos de cibersegurança – identificar, proteger, detetar, responder e recuperar.
O CiberCheckUp,é uma ferramenta em linha disponibilizada pelo CNCS no seu sítio web 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 CiberCheckUp permitem situar a capacidade da organização de acordo com a distribuição convencionada no QACC.

O CNCS também faculta o Roteiro para as Capacidades Mínimas de Cibersegurança (RCMC), um modelo de capacitação em cibersegurança com enfoque especial em PME. O RCMC 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.

Autoridade Nacional de Certificação da Cibersegurança

Na sequência da publicação do Decreto-Lei n.º 65/2021[1], de 30 de julho, foi o Centro Nacional de Cibersegurança 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[2], 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.

[1] Doravante abreviado como Decreto-Lei n.º 65/2021
[2] Doravante abreviado como Regulamento (UE) 2019/881

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 ambiente de trabalho 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.

Um esquema de certificação da cibersegurança para as organizações nacionais

A dependência crescente das TIC por parte de organizações de todos os tipos 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 poderoso 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 para 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
Auditoria de certificação			
Análise do Risco	AR		

Conformidade	Conformidade		
Conformidade permanente		Representa o esforço que a organização deverá empreender para assegurar a continuidade do nível de garantia de cibersegurança obtido na certificação	
Constatações de auditoria	Constatações		
Esquema de Certificação	EC		
Evidências de Auditoria	Evidências		
Medidas de segurança	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
Medidas de segurança obrigatórias		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 5
Medidas de segurança passíveis de exclusão		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 5
Não conformidade Maior	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
Não conformidade Menor	NC Menor	A medida de segurança encontra-se implementada, mas não consegue demonstrar totalmente que cumpre os respetivos objetivos	
Nível de Capacidade		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.
Oportunidade de Melhoria	OM		
Requisitos de conformidade	Requisitos		

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, vulgo "organismo de certificação" (OC[3]).

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 no âmbito do esquema.

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 cumpridos por todas as partes e são conformes com o estabelecido.

Caracterização e síntese descritiva

O Esquema de Certificação para o QNRCS tem por entidade supervisora o CNCS, na qualidade de Autoridade Nacional de Certificação em Cibersegurança, sendo os requisitos para a certificação os que constam do seu **Anexo 5**, para cada nível de garantia, permitindo a definição do ciclo de vida da certificação QNRCS e dos respetivos certificados de conformidade.

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 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 de 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 5** do presente documento, baseados no QNRCS e inspirados no QACC e RCMC.
- A certificação obtida noutro esquema ou norma certificável não dá lugar a qualquer tipo de equivalência direta para a obtenção do certificado de conformidade com o QNRCS.
    - Poderá haver, porém, a aceitação de evidências de implementações de medidas específicas realizadas no âmbito de outros esquemas para efeitos de verificação de implementação de determinadas medidas do QNRCS, quando estas medidas sejam idênticas às dos outros esquemas, e essas equivalências estejam definidas e reguladas em sede do manual de auditoria do EC 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 do risco.
- O EC QNRCS prevê a implementação de todas as medidas de segurança do QNRCS por defeito. No entanto, poderão existir medidas passíveis de exclusão pelos candidatos por não se aplicarem ao

[3] Organismos de certificação ou organismos de avaliação de conformidade, muitas vezes designados e conhecidos na sua sigla em língua inglesa como CAB (*Conformity assessment body*)

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, por eventualmente não se adequarem ao tratamento do seu risco específico.

A classificação das medidas como obrigatórias ou passíveis de exclusão é indicada no **Anexo 5** deste EC QNRCS.

- O esquema de certificação para o 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 no 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 enquanto tal pelo Instituto Português de Acreditação, I.P. (IPAC)[4] 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 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 poderá ter uma validade máxima de três anos desde a data da emissão.
- 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[5] do presente documento sempre que se revele necessário e/ou pertinente.

Destinatários

A certificação no esquema de certificação 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

[4] O IPAC é o organismo nacional de acreditação

[5] E, eventualmente, à sua extinção

essenciais[6], prestadores de serviços digitais[7], 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.

Dono do esquema e entidade supervisora

O CNCS é a entidade responsável pela elaboração e operacionalização do esquema de certificação QNRCS, bem como pela sua supervisão.

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** e definidos no **Anexo 5** do presente documento.

Âmbito de aplicação

O EC QNRCS tem por âmbito de aplicação, em cada organização, a implementação das medidas de segurança do QNRCS especificadas no **Anexo 5** do presente esquema, dentro do contexto de atividade aplicável determinado pela organização candidata em função do processo de análise e gestão de risco e conforme fique 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 de nível de risco aceitável são efetuadas por meio de uma análise de risco que deverá reger-se pelos princípios referidos no capítulo 12 do presente esquema. Executada a análise de risco e conforme a avaliação do risco específico à sua esfera de atuação, a organização candidata define se as medidas de segurança do QNRCS se devem aplicar à atividade de toda a organização ou apenas a partes significativas da sua atividade, definidas como as que são essenciais para a prestação dos respetivos serviços, identificando-as.

Efetuada esta delimitação, e caso se verifique que alguma das medidas do QNRCS definidas no presente Esquema como passíveis de exclusão não se aplicam ao seu contexto de atividade ou para tratamento do seu risco específico, a organização poderá decidir não aplicá-la. Tal exclusão não deverá colocar em causa o tratamento adequado do risco em que a organização incorre, reduzindo a sua exposição e trazendo 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 descritos no documento designado "Declaração de Aplicabilidade", a entregar no momento da candidatura.

As medidas 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

[6] Conforme definição do Regime Jurídico da Segurança do Ciberespaço, da Diretiva (UE) 2016/1148 e designação pelo CNCS
[7] Idem, no que for aplicável

Aplicabilidade, constituem, após validação pelo organismo de certificação, o âmbito de aplicação do esquema de certificação do QNRCS na organização candidata e que serão a matéria auditável.

Alteração do âmbito

Após a organização estar certificada, qualquer alteração na organização que possa interferir com a delimitação do âmbito da certificação, 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 validar apenas as atividades que foram adicionadas ao âmbito, desde que não interfiram com a validade de outra atividades previamente auditadas.

Redução do âmbito

A redução de âmbito de certificação[8] 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);
- cibersegurança dos prestadores de serviços de computação na nuvem.

5. Referências legais, normativas e regulamentares

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

- O EC QNRCS está contido no quadro nacional de certificação da cibersegurança, cfr. previsto no Decreto-Lei n.º 65/2021, sendo desenvolvido ao abrigo do n.º2 do art.º 20 daquele diploma legal;
- A terminologia utilizada no EC QNRCS tem por referência a terminologia e definições da ISO/IEC 27001;
- 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 norma ISO/IEC 17065 é o padrão internacional para a acreditação[9] dos organismos de avaliação de conformidade no âmbito do EC QNRCS;

[8] Sempre que a redução geral das atividades que delimitam o âmbito da certificação não coincida com o acrescento de qualquer eventual atividade por auditar ao âmbito da certificação

[9] Independentemente de eventuais requisitos adicionais que vierem a ser definidos pelo CNCS e pelo IPAC

- 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, em processo de consulta pública no sítio Web do CNCS, para recolha de contributos, revisão e futura 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 5 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 1**.

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 para a sociedade dos serviços que prestam 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 pelo Regime Jurídico da Segurança do Ciberespaço, em cumprimento da Diretiva (UE) 2016/1148, nomeadamente organizações da Administração Pública, central e local, sobretudo os seus organismos TIC, os operadores de infraestruturas críticas, operadores de serviços essenciais[10] e os prestadores de serviços digitais[11].

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 acima identificadas 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 da sua ocorrência.

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.

[10] Conforme definição do Regime Jurídico da Segurança do Ciberespaço, da Diretiva (UE) 2016/1148 e designação pelo CNCS
[11] Idem, no que for aplicável

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.

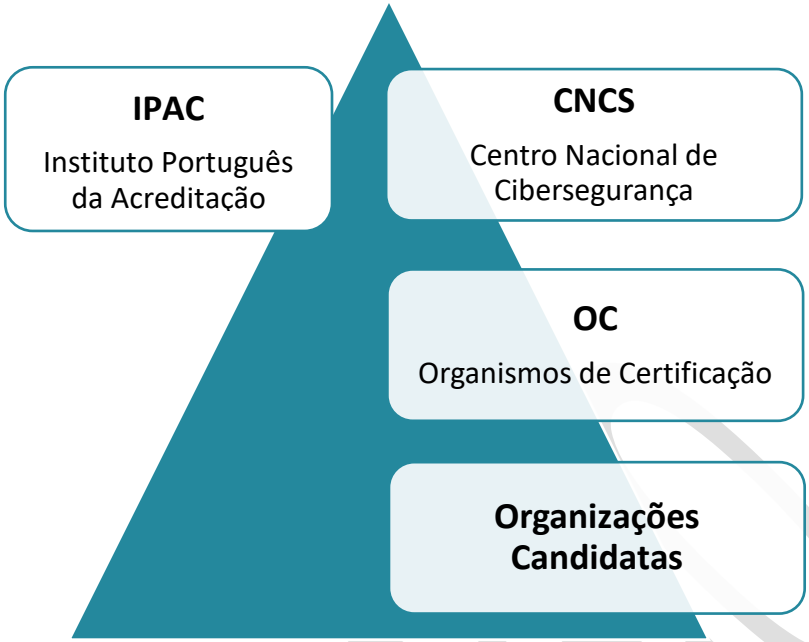
O EC QNRCS tem, por último, como objetivo contribuir para a execução da Resolução do Conselho de Ministros n.º 55/2020, que aprova a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, e da Resolução do Conselho de Ministros n.º 131/2021, que aprova a Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o atinente Plano de Acão 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 em resultado 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.

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

O modelo de governação do EC QNRCS está estruturado com base em 4 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
IPAC	Organismo nacional de acreditação	• Acreditar os OC para execução do processo de certificação QNRCS • Dirimir divergências entre os OC e as organizações certificadas ou candidatas • Supervisionar os OC • Elaborar e publicar o esquema de acreditação dos OC para fins de certificação no EC QNRCS
CNCS	Autoridade Nacional de Certificação da Cibersegurança	• Elaborar, gerir, manter, atualizar e publicitar o Esquema de Certificação QNRCS • Definir uma proposta de metodologia para a gestão e análise do risco • Supervisionar os certificados emitidos e as organizações certificadas • Apoiar o IPAC na supervisão dos OC • Apoiar o IPAC na elaboração do esquema de acreditação dos OC para fins de certificação no EC QNRCS • Emitir os códigos QR a constar nos certificados • Gerir o Portal QNCC para publicação dos certificados QNRCS • Estabelecer-se como ponto de contacto para a cooperação internacional no plano da certificação europeia
OC	Organismos de certificação	• Assegurar a acreditação pelo IPAC • Receber e validar as candidaturas à certificação no EC QNRCS • Executar o processo de certificação QNRCS • Proferir a decisão de certificação QNRCS • Emitir os certificados QNRCS e gerir os respetivos ciclos de vida

		• Cumprir e fazer cumprir as regras e requisitos do EC QNRCS, incluindo a Política de Divulgação de Certificados do EC QNRCS
Organizações Candidatas	Entidades públicas ou privadas candidatas à certificação QNRCS	• Efetuar o procedimento de análise e gestão de risco alusiva à sua situação de cibersegurança • 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 • Executar a candidatura a um nível de capacidade QNRCS • Disponibilizar evidências de execução das medidas de segurança • Cumprir as regras e requisitos do EC QNRCS, incluindo a Política de Divulgação de Certificados do EC QNRCS e as notificações de incidentes de cibersegurança

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 de Certificados do EC QNRCS;
- participar nas atividades de supervisão do EC QNRCS pelo CNCS, sempre que solicitados nos casos aplicáveis.

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:

- ser estabelecidas em território nacional;

- corresponder a uma única entidade legal;
- ter procedido à análise de risco requerida 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 5** deste documento, que não serão aplicáveis como medidas de tratamento dos riscos identificados;
- elaborar uma ”Declaração de Aplicabilidade” nos moldes previstos no capítulo 4, 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 5** do esquema de certificação;
- disponibilizar e garantir a veracidade das informações e os contactos solicitados no formulário de candidatura;
- comprometer-se a comunicar ao CNCS e ao OC qualquer incidente de cibersegurança com impacto relevante ou substancial nos termos dos artigos 15.º, 17.º e 19.º do Regime Jurídico de Segurança do Ciberespaço, ou, caso a organização não esteja abrangida pelo disposto no citado diploma legal, 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.

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 está disponível no **Anexo 2,** através de uma hiperligação.

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

Níveis do EC QNRCS

O QACC apresenta três níveis de capacidade para implementação dos requisitos do QNRCS, identificados como “**Básico**” – “**Substancial**” – “**Elevado**”.

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.

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 vigorosos, 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 segurança 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 redunda 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 5** 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 5, 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 5, 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 5, 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 maturação evolutiva 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 selecionar 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 no **Anexo 2,** através de uma hiperligação.

O nível de candidatura selecionado 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 aceitar ou propor que o procedimento de certificação tenha por objetivo um outro nível de capacidade.

Validação do nível selecionado

Durante as auditorias descritas no **Capítulo 11** do presente documento, integrantes do ciclo de vida da certificação, o auditor, em representação do OC, pode confirmar que a organização tem condições para atingir o nível de capacidade selecionado ou propor à organização candidata e ao OC um outro nível que seja consistente com a análise das evidências recolhidas.

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 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 o cumprimento 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 5 dias uteis 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 5;
    - caso sejam detetadas não conformidades, dever-se-ão encetar os passos detalhados no capítulo 14;
4. Se tudo estiver conforme, 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, determinadas em consequência do processo de análise e gestão de risco;
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 de Certificados QNRCS (ver Anexo 4), e contendo a informação definida pelo Modelo de Certificados QNRCS (ver Anexo 3);
8. Realização da auditoria de acompanhamento anual
    - terá 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
    - devem ser realizadas até 30 dias de calendário do 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[12];
        ii. ou se determinadas pelo CNCS na sua qualidade de ANCC;
        iii. ou ainda, 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.

    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). Podem ser efetuadas em qualquer momento entre as auditorias planeadas.
    As auditorias extraordinárias podem ainda ocorrer, por decisão do OC e ratificação do CNCS, na sequência de uma notificação pela organização certificada de um incidente de cibersegurança com impacto relevante ou substancial nos termos dos artigos 15.º, 17.º e 19.º do Regime Jurídico de Segurança do Ciberespaço, ou, caso a organização não esteja abrangida pelo disposto no citado diploma legal, 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.
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 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);

  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.

[12] Exceto se se tratar de uma redução geral do âmbito sem concurso de acrescento de atividades

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 situações de não cumprimento do EC QNRCS pela organização certificada ou mediante decisão do CNCS enquanto ANCC, por motivo de incumprimento das regras do presente EC QNRCS.
  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 etiqueta 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, utilizando o procedimento de comunicação estabelecido, deve ocorrer no prazo máximo de 5 dias úteis.

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.

A auditoria de transferência deve ser efetuada antes da caducidade 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 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 máximo de validade de 3 anos.

Os auditores que participaram nas auditorias do OC anterior só poderão voltar a efetuar auditorias à organização transferida após 3 anos da última auditoria.

Anulação voluntária

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

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 5 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 (anteriormente referido), condensado no capítulo 3.5 do QNRCS e resumido mais abaixo, a organização deverá continuar a executar os procedimentos que já tem enraizados nas suas atividades de cibersegurança e que estarão adaptados às necessidades da organização.

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 este tipo de experiências ou não ter tais práticas sedimentadas.

Para esses casos, recomenda-se vivamente a adoção de uma metodologia para a análise e gestão do risco definida pelo CNCS, que será apresentada por 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.

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 5 do EC QNRCS como passíveis de exclusão, assim como a respetiva justificação para cada decisão.

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 realizada através da análise de evidências recolhidas durante os atos de auditoria, comparando com os critérios elencados no Anexo 5 a este 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 5 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 especificas 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 5 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 existir 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;

- **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** 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, de um Plano de Ações Corretivas (PAC) onde estabelece as ações a implementar, responsáveis e prazos.

O OC deve analisar a proposta de PAC, informando a organização candidata da sua aprovação ou não aprovação, no prazo máximo de 5 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 dos prazos máximos estabelecidos por cada nível de capacidade.

O prazo máximo para a execução com eficácia do PAC para Não conformidades Maiores é de 30 dias.

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 de calendário. 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/ou com o plano de ações aprovado pelo OC no caso das 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 3** do Esquema de Certificação QNRCS.

16. Política de divulgação dos certificados de conformidade QNRCS

A política de divulgação de certificados do EC 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 4**, 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 contidas 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 organismo de certificação 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 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** do 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:
- Monitorização dos certificados emitidos e das organizações que os titulam;
- Gestão da publicação dos certificados de conformidade no portal QNCC;
- 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;
- 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
DRAFT 1.1	22/12/2021	Criação	Versão inicial para revisão
DRAFT 1.5	28/12/2021	Integração de resultados de revisões	Versão entregue para publicação
DRAFT 1.8	30/12/2021	Integração de resultados de revisões	Versão aprovada para publicação
DRAFT 1.10	14/01/2022	Inclusão da existência de medidas obrigatórias e passíveis de exclusão em função da gestão do risco, definidas no Anexo 5	
DRAFT 1.11	20/01/2022	Diversas alterações	
DRAFT 1.12	24/01/2022	Alterações produzidas pela revisão do Anexo 5	
DRAFT 1.13	26/01/2022	Correções diversas	NC Grave passou a NC Maior

DRAFT 1.14.3	22/05/2022	Reformulação geral do Esquema	Integração de alterações motivadas pela revisão do Anexo 5
DRAFT 2.0	08/06/2022	Revisão geral	Integração de alterações motivadas pela revisão do esquema e do Anexo 5. Versão disponibilizada para a segunda consulta pública.

20. ANEXOS

Anexo 1 – Lista de referências legais, normativas e regulamentares

A lista de referências aplicáveis ao Esquema de Certificação do QNRCS pode ser encontrada aqui.

Anexo 2 – Formulário de candidatura a certificação

O formulário para candidatura das organizações à certificação QNRCS pode ser encontrado aqui.

Anexo 3 – Modelo de certificado QNRCS

O documento que descreve o modelo e marcas do certificado QNRCS pode ser encontrado aqui.

Anexo 4 – Política de divulgação dos certificados de conformidade QNRCS

O documento que contém a política de divulgação dos certificados de conformidade QNRCS pode ser encontrado aqui.

Anexo 5 – Critérios de auditoria para o esquema de certificação QNRCS

O documento que contém a lista de critérios aplicáveis ao EC QNRCS pode ser encontrado aqui.