

ESQUEMA DE CERTIFICAÇÃO QNRCS 2026

Versão Preliminar

Índice

Sumário 4

1. Contexto do Esquema de Certificação QNRCS 6

Quadro Nacional de Referência para a Cibersegurança 6

Um esquema de certificação da cibersegurança para as entidades nacionais 6

2. Glossário do Esquema de Certificação QNRCS 7

3. Descrição e caracterização do Esquema de Certificação QNRCS 9

Conceitos 9

Dono do esquema e entidade supervisora 9

Caracterização e síntese descritiva 9

Perfis de Certificação 10

Destinatários 11

4. Regras de aplicação dos perfis do Esquema de Certificação QNRCS 11

Delimitação do contexto de atividade aplicável e decisão de exclusão de medidas do QNRCS 11

Declaração de Aplicabilidade 12

Alteração do âmbito 12

5. Objetivos do Esquema de Certificação QNRCS 12

6. Papéis, funções e responsabilidades no Esquema de Certificação QNRCS 13

7. Requisitos para os Organismos de Certificação 15

Requisitos de competência de auditores 15

8. Requisitos para os candidatos à certificação QNRCS 16

9. Níveis de garantia do EC QNRCS 17

Níveis do EC QNRCS 17

Progressividade 17

Cumulabilidade 17

Seleção de níveis de garantia da candidatura 18

Aumento do nível de garantia 18

Redução do nível de garantia 18

10. Ciclo de vida e processo de certificação do EC QNRCS 19

Ciclo de vida 19

Validade dos certificados 19

Manutenção da certificação 19

Renovação da certificação 19

Processo de certificação no EC QNRCS 19

Versão Preliminar

Estados dos certificados **21**
Transferência **22**
Anulação voluntária **22**
Incumprimento das regras do EC QNRCS **22**
11. Métodos de avaliação e critérios de auditoria ***22***
12. Regras para o tratamento de "Não Conformidades" ***23***
13. Regras para a gestão dos certificados de conformidade EC QNRCS ***24***
14. Política de divulgação dos certificados de conformidade EC QNRCS ***24***
15. Regras para acesso, arquivo e preservação de informações relativa à certificação ***24***
16. Supervisão do ciclo de vida dos certificados de conformidade QNRCS ***25***
17. Histórico de revisões ***26***

Versão Preliminar

Sumário

A elaboração, implementação, execução, avaliação e gestão de esquemas nacionais de certificação da cibersegurança são competências do Centro Nacional de Cibersegurança (CNCS), enquanto Autoridade Nacional de Certificação da Cibersegurança (ANCC), definidas no n.º 2 do Artigo 20.º do Regime Jurídico da Cibersegurança (RJC) aprovado em anexo ao Decreto-Lei n.º 125/2025, de 4 de dezembro, em aplicação do art.º 58 do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019., e concorrem para a implementação de um Quadro Nacional de Certificação da Cibersegurança (QNCC).

No prosseguimento da sua missão de capacitação em cibersegurança das organizações nacionais, o CNCS disponibiliza desde 2019 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, primeira versão lançada em 2021) visava valorizar aquelas organizações que já tinham por referência e implementavam 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.

O EC QNRCS inaugurou o QNCC e 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, I.P. (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.

Esta versão atualizada do EC QNRCS, para além de se destinar mais claramente às entidades abrangidas pelo RJC para as apoiar no seu cumprimento, introduz, como principal novidade, o conceito de perfis de certificação. Foi criado um perfil específico de certificação que visa avaliar a conformidade da implementação das medidas mínimas de cibersegurança aplicáveis às entidades abrangidas pelo RJC e demais requisitos legalmente exigíveis. Caso uma dada entidade abrangida pelo RJC se certifique num nível de garantia de certificação equivalente ao nível de conformidade que lhe é legalmente exigido no contexto do RJC, tal entidade beneficiará de presunção de cumprimento com as medidas de cibersegurança ao Regulamento n.º 756/2026, tal como previsto no Artigo 27.º.

O presente documento descreve as regras gerais aplicáveis ao EC QNRCS, sem prejuízo da especificação de regras diferenciadas em cada perfil de certificação que se publique, 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 aos OC e a candidatos à certificação, os níveis de garantia, o ciclo de vida e o processo de certificação, 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, o documento referente ao "Perfil de Certificação RJC" que descreve as regras específicas aplicáveis às entidades que se pretendam certificar neste perfil, incluindo os requisitos de implementação das medidas do RJC para cada

Versão Preliminar

nível, bem como as evidências que deverão ser disponibilizadas aos OC em sede de auditoria para verificação do cumprimento dos requisitos.
O EC QNRCS, ao exigir transparência e clareza mas dias disposições, proporciona as condições para os processo de certificação 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.

Versão Preliminar

1. Contexto do Esquema de Certificação QNRCS

Quadro Nacional de Referência para a Cibersegurança

O Quadro Nacional de Referência para a Cibersegurança (QNRCS), aprovado pelo Centro Nacional de Cibersegurança (CNCS), constitui o principal referencial nacional para a identificação e adoção de normas, padrões e boas práticas aplicáveis às organizações públicas e privadas. O seu objetivo é apoiar as organizações na redução do risco associado a ciberameaças, disponibilizando uma abordagem estruturada para a proteção das redes e sistemas de informação, que sistematiza e orienta a implementação de controlos e medidas de cibersegurança.

A primeira versão do QNRCS, publicada em 2019, estabeleceu um conjunto de orientações destinadas a apoiar as organizações na definição da sua estratégia interna de cibersegurança, de forma homogénea e alinhada com as melhores práticas internacionais, promovendo simultaneamente uma resposta nacional mais harmonizada face às crescentes ciberameaças.

Com a entrada em vigor do novo Regime Jurídico da Cibersegurança (RJC), aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro, o QNRCS viu reforçada a sua relevância enquanto instrumento estruturante da segurança do ciberespaço nacional, passando a constituir um referencial reconhecido para a implementação de medidas técnicas, operacionais e organizativas de cibersegurança pelas organizações abrangidas pelo referido regime.

A segunda versão do QNRCS encontra-se alinhada com este novo enquadramento regulatório e com normas e boas práticas internacionais comummente utilizadas, representando uma evolução na abordagem à cibersegurança de uma organização. Encontra-se estruturado em seis objetivos fundamentais de cibersegurança, Governar, Identificar, Proteger, Detetar, Responder e Recuperar. Estes objetivos integram um conjunto de categorias, controlos e medidas destinados a reforçar a resiliência das organizações face aos riscos e incidentes de cibersegurança.

À sua antiga estrutura foi acrescentado um novo objetivo, Governar, com o propósito de incluir controlos e medidas que reflitam as condições transversais que as organizações devem implementar para garantir o cumprimento dos restantes objetivos.

Assim, esta nova versão do QNRCS procura refletir uma nova realidade e ambiente de cibersegurança que está em constante mudança. Incorpora novos referenciais, novos controlos e medidas de cibersegurança que pretendem refletir uma realidade complexa e heterogénea, resultado de uma análise dos incidentes mais relevantes em Portugal nos últimos anos. Esta versão inclui ainda uma nova estrutura procurando tornar mais ágil a sua evolução e adaptação a novas realidades e contextos. Neste sentido, são criados perfis de certificação com objetivos diferenciados e porventura enquadramentos regulatórios ou outros, complementares.

Um esquema de certificação da cibersegurança para as entidades nacionais

O Decreto-Lei n.º 125/2025, de 4 de dezembro, aprovou o Regime Jurídico da Cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União Europeia. Este regime é aplicável às entidades essenciais, importantes e públicas relevantes, nos termos e com os limites nele previstos.

No âmbito da operacionalização deste regime, foi publicado o Regulamento n.º 756/2026 que estabelece os termos da aplicação de diversas disposições do RJC, prevendo, nomeadamente, a possibilidade das entidades importantes e essenciais recorrerem à certificação para comprovar a implementação das medidas técnicas, operacionais e organizativas adequadas e proporcionadas para gerir os riscos de segurança dos sistemas de rede e informação utilizados nas respetivas operações ou prestação de serviços (n.º 3 do Artigo 34.º).

Versão Preliminar

Neste contexto, o referido regulamento, através da alínea a), nº 3 do Artigo 27.º, nomeia especificamente o presente Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança (EC QNRCS) como uma das certificações passíveis para atestar o cumprimento das medidas de cibersegurança previstas no artigo 30.º do Regulamento n.º 756/2026.

Esta evolução legislativa e regulamentar reforçou a relevância da certificação da cibersegurança, criando a necessidade do desenvolvimento de uma nova versão do EC QNRCS que desse resposta aos novos requisitos legais e regulamentares em vigor.

Ao mesmo tempo que a certificação no EC QNRCS - Perfil de Certificação RJC, de natureza voluntária, poderá conferir a presunção do cumprimento das medidas de cibersegurança do RJC a uma entidade por aquele abrangida, desde que observadas determinadas condições, possibilita também que qualquer entidade que se encontre fora do âmbito do RJC demonstre o cumprimento com os requisitos aplicáveis, promovendo uma adesão voluntária às medidas de cibersegurança, convertidas em requisitos de conformidade no presente EC.

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 EC QNRCS. Pode, cada perfil de certificação, adicionar termos ou conceitos específicos, os quais serão apresentados na sua própria estrutura.

Termo ou Conceito	Abreviatura	Definição	Notas adicionais
Auditoria de certificação		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 9000:2026)	
Avaliação do risco	AR	Processo sistematizado de identificação, análise e avaliação da probabilidade de uma ocorrência e do seu potencial impacto para o funcionamento de uma dada organização.	
Conformidade		Cumprimento dos requisitos dos critérios de certificação (Normas, regulamentos, etc.).	
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	Resultados da avaliação das evidências de auditoria recolhidas face aos critérios de auditoria (ISO 9000:2026).	
Esquema de Certificação	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.	
Perfil de Certificação do EC QNRCS	Perfil de Certificação ou Perfil	Conjunto de requisitos, medidas de cibersegurança e respetivas regras de avaliação, desenvolvido para responder às	

		características, necessidades ou obrigações específicas de um determinado grupo de organizações ou contexto regulatório.	
Evidências de auditoria	Evidências	Registos, afirmações factuais ou outra informação, que sejam relevantes para os critérios de auditoria e verificáveis (ISO 9000:2026).	
Medidas de cibersegurança	Medidas	Medidas de âmbito técnico, operacional e organizacional que visam apoiar as organizações na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações ou na prestação dos seus serviços, bem como impedir ou minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros serviços	No contexto do esquema de certificação tornam-se requisitos de conformidade em auditorias de certificação.
Medidas de cibersegurança passíveis de exclusão		Trata-se de medidas de cibersegurança dos perfis do EC 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.	Nem todos os perfis de certificação do EC QNRCS admitem a exclusão de implementação de medidas de cibersegurança.
Não conformidade Maior	NC Maior	A medida de cibersegurança não se encontra implementada ou, se implementada, encontra-se totalmente desalinhada dos objetivos da medida de segurança.	No enquadramento de auditoria de certificação, corresponde ao não cumprimento de um requisito. Pode impedir a certificação ou a manutenção do certificado até ser corrigida.
Não conformidade Menor	NC Menor	A medida de cibersegurança encontra-se implementada, mas não consegue demonstrar totalmente que cumpre os respetivos objetivos.	Normalmente não impede a certificação, desde que exista um plano de ações corretivas aceite.
Nível de Garantia		Grupo de requisitos e medidas definidos para um dado nível. Os níveis de garantia são definidos de forma progressiva, correspondendo cada nível ao cumprimento de um conjunto específico de requisitos e medidas, cumulativo relativamente aos níveis inferiores, sendo que a passagem para um nível superior pressupõe o cumprimento dos requisitos e medidas previstas nos níveis precedentes.	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	Oportunidade de atuação identificada para melhorar o desempenho da organização e reforçar a sua capacidade de adaptação às mudanças internas e externas.	
Requisitos de conformidade	Requisitos	Obrigações, necessidades ou expectativas especificadas e obrigatórias que um produto, serviço, processo ou organização deve satisfazer para alcançar a conformidade.	

3. Descrição e caracterização do Esquema de Certificação QNRCS

O Esquema de Certificação QNRCS visa ser um instrumento que permita às organizações atestar, através de uma certificação independente e eficaz, a implementação e cumprimento de medidas de cibersegurança, promovendo um aumento de resiliência, maturidade em cibersegurança e confiança das organizações nacionais.

Embora concebido para responder às necessidades das organizações abrangidas pelo RJC, o esquema pretende igualmente ser aplicável a outras organizações que pretendam melhorar a sua cibersegurança e demonstrá-lo através da obtenção da certificação. Nesta perspetiva, serão desenvolvidos perfis de certificação diferenciados, ajustados ao tipo, dimensão e contexto das organizações que pretendam certificar-se.

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).

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.

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.

Como dono do esquema, o CNCS zela pela manutenção e atualização do esquema face à evolução do contexto de cibersegurança, e procura garantir que as evoluções tidas por necessárias mantêm o esquema alinhado com os objetivos de política pública que estão na sua génese.

Caracterização e síntese descritiva

O Esquema de Certificação QNRCS define o modelo e os princípios orientadores da certificação da cibersegurança das organizações, estabelecendo os requisitos, processos e mecanismos necessários à avaliação da conformidade e à emissão dos respetivos certificados.

O presente documento define os princípios, regras, requisitos e procedimentos que enquadram a implementação e funcionamento do EC QNRCS. Neste âmbito, são descritos o objeto e o âmbito de aplicação do esquema, os seus objetivos e destinatários, os perfis de certificação aplicáveis aos diferentes tipos de organizações, as partes interessadas e os respetivos papéis, os métodos e critérios de avaliação da conformidade, os requisitos aplicáveis aos organismos de certificação e às organizações candidatas, bem como o processo e o ciclo de vida da certificação. O documento estabelece ainda as responsabilidades associadas à governação, supervisão e melhoria contínua do esquema, de forma a assegurar a sua eficácia, credibilidade e adequação às necessidades das organizações que pretendam obter certificação.

O EC QNRCS apresenta as seguintes características genéricas:

- A certificação da conformidade no EC QNRCS é voluntária, salvo se expressamente determinado em legislação própria;

Versão Preliminar

- Os requisitos para a certificação, critérios e evidências de auditoria para a decisão de certificação constam no corpo do presente esquema e no anexo referente ao perfil de certificação específico ao qual as organizações se candidatam. Independentemente do perfil a que se candidatem, as organizações que se encontram ao abrigo do RJC devem ainda cumprir os diplomas legais a que estão vinculadas por essa via, nomeadamente o respetivo regulamento e todas as instruções técnicas que lhe são anexas e vierem a ser publicadas, exceto nos casos em que não lhes seja expressamente aplicável;
- 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 EC QNRCS;
- O EC QNRCS prevê a existência de níveis de garantia . Estes níveis são incrementais, significando que, a acrescentar à aplicação de medidas dos níveis de garantia superior (por exemplo, Substancial e Elevado), as organizações devem assegurar, ainda, a aplicação das medidas de cibersegurança dos níveis de garantia respetivamente inferiores;
- A avaliação da conformidade para com um (ou mais) dos perfis de certificação do presente EC exige que o processo seja conduzido por um organismo de certificação, enquanto entidade externa e independente à organização candidata devidamente acreditada;
- 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 âmbito do 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)[1] 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 técnicas e 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;
- 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 do presente documento e respetivos anexos, sempre que se revele necessário e/ou pertinente.

Perfis de Certificação

Para efeitos do EC QNRCS, um perfil de certificação corresponde a um conjunto de requisitos, medidas e controlos de cibersegurança derivados do QNRCS, aos quais podem ainda ser acrescentados requisitos legais e de cibersegurança originários do RJC ou de outras leis e regulamentos de cibersegurança, que, sem prejuízo da natureza aberta e voluntária da certificação, se destinam a ser principalmente aplicados por uma determinada tipologia de organizações, definida em função de fatores como a sua dimensão, natureza da atividade, exposição ao risco, criticidade dos serviços prestados e enquadramento regulamentar.

[1] O IPAC é o organismo nacional de acreditação.

Versão Preliminar

A definição de perfis de certificação visa assegurar que os requisitos do esquema são adequados e proporcionais às características e necessidades das diferentes organizações, e para atender aos objetivos de políticas públicas em cibersegurança definidos para lidar com as necessidades de cibersegurança de contextos diversos, acrescentando ao esquema propriedades de flexibilidade e de simplificação para a abordagem a realidades distintas. Não obstante o cumprimento dos requisitos gerais definidos no esquema e aplicáveis a todos os perfis de certificação, cada perfil estabelece os requisitos obrigatórios específicos a cumprir para a obtenção e manutenção da certificação, bem como os critérios de auditoria e mecanismos específicos utilizados para a avaliação da conformidade.

Destaca-se que, para todas as certificações do EC QNRCS e independentemente do perfil de certificação selecionado pela organização candidata, são aplicáveis todas as regras gerais do EC QNRCS definidas no presente documento, exceto se expressamente disposto de forma diversa no perfil específico de certificação, sujeitas às devidas adaptações.

Destinatários

O presente esquema, e respetivos perfis de certificação, é de caráter voluntário e aplica-se a todas as organizações que pretendam obter a respetiva certificação, independentemente da sua tipologia ou dimensão, desde que se encontrem estabelecidas em território nacional e que cumpram os requisitos legais aplicáveis.

No entanto, o esquema, e em particular o Perfil de Certificação RJC, foi concebido tendo especialmente em consideração as entidades abrangidas pelo RJC, podendo a certificação nele prevista constituir um meio de demonstração e evidência da conformidade com os requisitos legais e regulamentares que lhes sejam aplicáveis.

4. Regras de aplicação dos perfis do Esquema de Certificação QNRCS

O EC QNRCS possibilita a certificação acreditada das práticas de cibersegurança das organizações nacionais, sendo, para isso, necessário observar um conjunto de regras comuns aplicáveis aos diversos perfis de certificação que o integram.

Sem prejuízo das disposições particulares definidas em cada um dos perfis de certificação, aplicam-se as regras gerais abaixo previstas.

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

Como princípio geral do presente EC, a seleção e aplicação de controlos e medidas de cibersegurança do QNRCS, cuja conformidade de implementação deve ser avaliada de acordo com os critério do EC QNRCS, deve principalmente resultar de um processo de gestão dos riscos para fins do seu tratamento, mas também pode resultar de critérios como, por exemplo, decisão estratégica, ou outro, salvo se for pretendida a presunção de cumprimento com as medidas do RJC ou outro regulamentação.

A organização candidata seleciona o conjunto das suas atividades que pretende incluir no âmbito da certificação. Recomenda-se que sejam incluídas as atividades mais relevantes para a prestação dos serviços considerados essenciais para a organização.

Haverá perfis de certificação, nomeadamente o Perfil de Certificação RJC, onde o âmbito das atividades ao qual as medidas são aplicadas, assim como as medidas obrigatórias a aplicar, é determinado pelo enquadramento da organização no RJC. Neste sentido, caso a organização se enquadre na referida lei, o nível de garantia a assegurar e as atividades a incluir no âmbito da certificação deve coincidir com a qualificação da organização no âmbito do RJC, para fins de presunção de cumprimento.

Versão Preliminar

Efetuada esta delimitação, e caso se observe que alguma das medidas de cibersegurança definidas no perfil de certificação como passíveis de exclusão (caso existam) 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.

O descrito não dispensa a consulta das regras específicas de cada um dos perfis de certificação.

Declaração de Aplicabilidade

A definição do contexto de atividade da organização aplicável à certificação, e as medidas do perfil de certificação passíveis de exclusão que a organização decidir não aplicar, deverão ser descritas no documento designado "Declaração de Aplicabilidade", a entregar no momento da candidatura, sendo igualmente justificada a sua exclusão ou não aplicabilidade.

As medidas de cibersegurança, 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 da organização candidata. A matéria auditável em contexto de auditoria será, assim, o grau e qualidade de implementação destas medidas de cibersegurança.

As condições para exclusão de medidas de cibersegurança são definidas nos anexos correspondentes a cada um dos perfis de certificação, sendo que, em alguns destes, é expectável que todos os requisitos sejam de caráter obrigatório devido ao seu objetivo, por exemplo, presunção de cumprimento para com o RJC.

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[2], ou por decisão estratégica da organização para alargar ou diminuir este âmbito, 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 o pedido de alteração ao âmbito da certificação, durante uma auditoria extraordinária ou na auditoria do ciclo.

As auditorias extraordinárias devem servir para avaliar pedidos de alteração de âmbito, não substituindo as auditorias do ciclo de certificação.

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.

5. Objetivos do Esquema de Certificação QNRCS

O EC QNRCS tem por objetivo promover o aumento do nível de cibersegurança, resiliência e maturidade das organizações que operam no ciberespaço nacional, através da disponibilização de um mecanismo de certificação independente que permita avaliar e demonstrar a implementação de requisitos, medidas e controlos de cibersegurança.

[2] Incluindo a mudança de uma atividade principal para outra

Versão Preliminar

O EC QNRCS destina-se a entidades públicas e privadas, independentemente da sua dimensão ou setor de atividade, podendo ser utilizado para demonstrar a conformidade com requisitos regulamentares ou outros requisitos específicos definidos para determinadas tipologias de entidades.

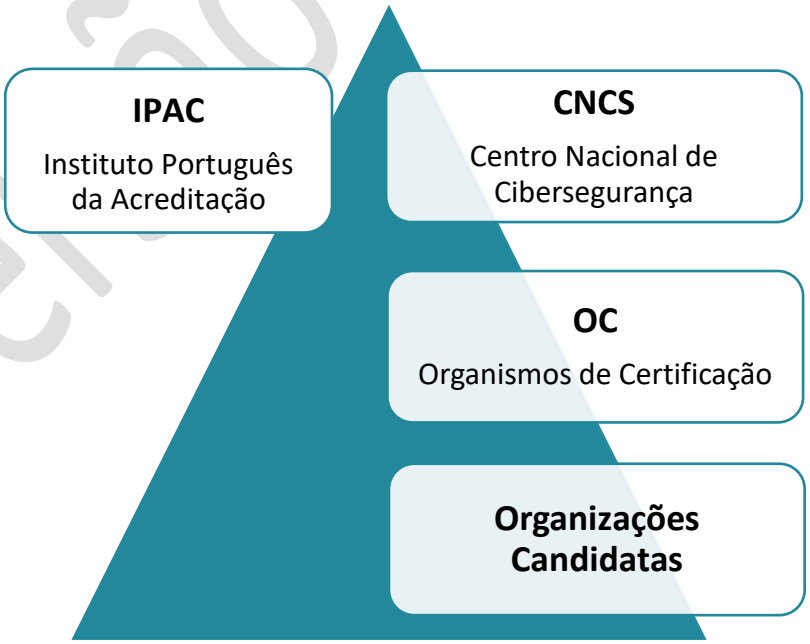
Para esse efeito, o EC QNRCS adota uma estrutura assente em perfis de certificação, entendidos como conjuntos de requisitos, medidas e controlos de cibersegurança desenvolvidos para responder às características, necessidades, níveis de risco ou obrigações regulamentares aplicáveis a um determinado grupo de organizações ou contexto específico. Esta abordagem permite assegurar uma aplicação proporcional e adequada dos requisitos de certificação, promovendo simultaneamente a flexibilidade, a simplicidade de adoção e a evolução contínua do EC.

Entre os objetivos do EC QNRCS destacam-se:

- promover uma gestão integrada da cibersegurança com base na nova versão do QNRCS;
- apoiar as organizações na implementação e melhoria contínua das suas capacidades de cibersegurança;
- promover a adoção de práticas organizacionais, processuais, tecnológicas e humanas alinhadas com referenciais reconhecidos de cibersegurança;
- fornecer mecanismos credíveis e independentes para a demonstração da conformidade com requisitos legais, em particular o RJC, regulamentares, setoriais ou normativos;
- promover uma gestão sistematizada dos riscos de cibersegurança;
- contribuir para a prevenção, deteção, resposta e recuperação face a incidentes de cibersegurança;
- reforçar a resiliência operacional das organizações e a continuidade da prestação dos seus serviços;
- promover relações de confiança entre organizações, clientes, utilizadores, parceiros, fornecedores, reguladores e demais partes interessadas.

6. 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:



Versão Preliminar

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	• Prestar serviços de acreditação aos OC para execução do processo de certificação no EC QNRCS; • Tratar reclamações sobre os OC em articulação com o CNCS se necessário; • Articular com o CNCS o processo de supervisão; • 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; • 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 a página QNCC para publicação dos certificados do EC QNRCS. • Estabelecer-se como ponto de contacto para a cooperação internacional no plano da certificação europeia em cibersegurança.
OC	Organismos de certificação	• Obter e manter a acreditação pelo IPAC; • Receber e validar as candidaturas à certificação no EC QNRCS; • Executar o processo de certificação; • Proferir a decisão de certificação; • Emitir os certificados 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	• Cumprir com as obrigações legais a que está sujeita, em especial as alusivas à sua situação de cibersegurança; • Efetuar o procedimento de análise e gestão dos riscos alusivo à sua situação de cibersegurança (apenas nos casos em que é aplicável); • Implementar todas as medidas de cibersegurança previstas no perfil de certificação do EC QNRCS ao qual se candidatam, exceto as medidas passíveis de exclusão que tenha decidido não aplicar em função da justificação na respetiva Declaração de Aplicabilidade (válido apenas para os perfis que contêm medidas passiveis de exclusão e mediante os resultados da análise dos riscos apresentada); • Executar a candidatura a um nível de garantia associado ao perfil de certificação do EC QNRCS escolhido;

Versão Preliminar

		• Disponibilizar evidências de implementação das medidas de cibersegurança; • 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.

7. 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.
- 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.

Requisitos de competência de auditores

O pessoal do OC com influência no processo de certificação tem de possuir os requisitos mínimos de competência estabelecidos abaixo.

A equipa auditora, no seu todo, deve demonstrar possuir os conhecimentos e aptidões para realizar auditorias e auditar os requisitos de certificação estabelecidos para cada nível a que estão qualificados. Tal inclui o conhecimento das medidas de cibersegurança listadas nos diferentes perfis de certificação do EC QNRCS para

Versão Preliminar

o nível correspondente de certificação. Considera-se que esse conhecimento deve ser obtido através das duas fontes abaixo:

- Habilitação escolar ou universitária cobrindo as medidas citadas e experiência profissional mínima:
  - 12.º ano + 7 ou mais anos de experiência profissional comprovada no setor das tecnologias de informação e comunicação, 3 dos quais na área da segurança da informação ou cibersegurança OU
  - Curso profissional ou curso técnico-profissional, na área das Tecnologias de Informação e Comunicação, Ciências Informáticas ou similares + 5 ou mais anos de experiência profissional comprovada no setor das tecnologias de informação e comunicação, 2 dos quais na área da segurança da informação ou cibersegurança OU
  - Licenciatura em Engenharia Informática ou similares + 3 ou mais anos de experiência profissional comprovada no setor das tecnologias de informação e comunicação, 1 dos quais na área da segurança da informação ou cibersegurança.
- Formação profissional específica nas medidas citadas:
  - Certificado de participação em curso de Auditor ISO 27001, E
  - Certificado de aproveitamento em prova de avaliação de conhecimentos a efetuar pelo CNCS
    - São considerado os auditores que já se encontrem com aproveitamento na prova de avaliação de conhecimentos referente à versão anterior do EC QNRCS.

As equipas auditoras devem ainda ter, pelo menos, um auditor familiarizado com a norma ISO/IEC 27005, o qual deve evidenciar conhecê-la e compreendê-la.

8. 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, designadamente as de cibersegurança;
- exceto se expressamente dispensado no perfil específico de certificação a que a organização se candidata:
  - 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[3]
  - ter determinado a circunscrição de atividades da organização a que a certificação se irá aplicar;
  - 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 cibersegurança passíveis de exclusão que não serão implementadas (onde aplicável);
- ter procedido à seleção do nível de garantia do correspondente perfil de cerificação;
- ter implementadas todas as medidas de cibersegurança para o nível de garantia a que se candidatam, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de riscos (sempre que aplicável);

[3] 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

Versão Preliminar

- ter registadas as evidências da implementação de tais medidas de cibersegurança, descritas no anexo do correspondente perfil de certificação do presente EC;
- disponibilizar e garantir a veracidade das informações e os contactos solicitados no formulário de candidatura;
- 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 de informação abrangidos no âmbito de certificação QNRCS da organização e que, por isso, possa comprometer a certificação.

Os requisitos para os candidatos à certificação pelo EC QNRCS devem ser analisados pelos OC, após a receção do respetivo formulário de candidatura à certificação, acompanhado pela Declaração de Aplicabilidade (sempre que aplicável).

O formulário de candidatura está disponível no **Anexo XX,** através de uma hiperligação.

9. Níveis de garantia do EC QNRCS

Níveis do EC QNRCS

O EC QNRCS prevê níveis diferentes de garantia, tal como tem sido utilizado no contexto de certificação a nível europeu.

A atribuição do nível de garantia adequado tem como objetivo assegurar uma aplicação proporcional dos requisitos do esquema.

Recomenda-se que a determinação do nível de garantia assente numa análise dos riscos, realizada de acordo com uma metodologia adequada à natureza da organização. Esta análise deverá considerar, entre outros aspetos, os ativos a proteger, as ameaças e vulnerabilidades relevantes, os impactos potenciais decorrentes de incidentes de cibersegurança e o contexto interno e externo da organização. O resultado desta avaliação permite enquadrar a organização no nível de garantia mais adequado, assegurando que os requisitos e medidas de certificação são proporcionais para mitigar os riscos identificados.

Cada perfil de certificação poderá definir procedimentos ligeiramente diferenciados para a aferição do nível de garantia a selecionar pelas entidades candidatas, a fim de se atingirem determinados objetivos, como a presunção de cumprimento com as medidas mínimas de cibersegurança previstas no Regime Jurídico de Cibersegurança.

Progressividade

A progressividade dos níveis de garantia do EC QNRCS redunda numa escalada de exigência nos requisitos de implementação das medidas 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 nos anexos 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”, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de riscos (apenas nos casos aplicáveis);

Versão Preliminar

- se a organização pretender ser certificada no nível “Substancial”, deverá ter implementadas todas as medidas previstas para os níveis “Básico” e “Substancial”, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de riscos (apenas nos casos aplicáveis);
- se a organização pretender ser certificada no nível “Elevado”, deverá ter implementadas todas as medidas previstas para os níveis “Básico”, “Substancial” e “Elevado”, com possível exceção das medidas passíveis de exclusão, identificadas em consequência do seu processo específico de análise e gestão de riscos (apenas nos casos aplicáveis);

Excetuam-se deste principio casos em que uma medida prevista num nível Superior substitua funcionalmente uma medida de nível inferior, desde que assegure, de forma evidenciável, os mesmos objetivos de segurança e proporcione um nível de proteção igual ou superior. Nestes casos, a não implementação da medida do nível inferior deve ser fundamentada pela organização e validada pelo OC no âmbito da certificação.

Procura-se desta forma proporcionar às organizações destinatárias uma via de crescimento e de progressão em cibersegurança compatível com as suas capacidades e necessidades.

Seleção de níveis de garantia da candidatura

As organizações candidatam-se a um nível de garantia formalizando-o no formulário disponível no **Anexo XX** através de uma hiperligação.

O nível de garantia selecionado pela organização deverá ter em conta o seu contexto e ter por base, entre outros, as capacidades e as necessidades de cibersegurança, inferidas do processo de análise e gestão dos riscos, acrescido do esforço, do custo de efetivação das medidas, da repercussão a atingir com a certificação, bem como outros fatores que lhe possam ser exclusivos. Todas as organizações candidatas deverão também considerar eventuais requisitos legais adicionais a que estejam obrigadas em matéria de cibersegurança.

No caso específico do Perfil de Certificação RJC, para que as entidades em âmbito do Regime Jurídico da Cibersegurança possam beneficiar da presunção do seu cumprimento através da certificação, a escolha do nível de garantia deverá ter por base o nível determinado pelo processo de qualificação de entidades, descrito no artigo 9.º do Regulamento n.º 756/2026, conforme descrito no respetivo Anexo.

O OC escolhido pela organização candidata deve avaliar os elementos submetidos na candidatura e concluir se se encontram reunidas as condições para a marcação de auditoria de concessão. Em caso negativo, deve solicitar esclarecimentos adicionais que permitam suportar a decisão favorável de aceitação da candidatura para o nível de garantia solicitado.

Aumento do nível de garantia

Se a proposta de alteração do nível da garantia 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 garantia

Se a proposta de alteração do nível de garantia 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.

Versão Preliminar

Os perfis específicos de certificação poderão conter disposições diferenciadas.

10. Ciclo de vida e processo de certificação do EC QNRCS

Entende-se por "ciclo de vida da certificação do EC 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 até um ano e com uma variação máxima de 30 dias de calendário em relação ao mês e finalização da auditoria de concessão e uma segunda auditoria de acompanhamento até dois anos e com uma variação máxima de 30 dias de calendário em relação ao mês e finalização da auditoria de concessão.

Compete ao OC agendar as auditorias, tendo em atenção os prazos acima 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, a qual deve ser realizada até 30 dias de calendário anteriores ao término da data de validade do certificado do EC QNRCS em vigor.

Processo de certificação no EC QNRCS

O processo genérico de certificação num dos perfis de certificação do EC QNRCS, sempre que no perfil não existam disposições específicas para este fim, pode-se resumir através do seguinte encadeamento de etapas e prazos associados:

1. Candidatura da organização à certificação num dos perfis de certificação que correspondam aos seus objetivos, 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 desde a aceitação da candidatura;
    - é verificada a implementação dos requisitos exigidos, considerando o nível de garantia manifestado na candidatura, através dos critérios de auditoria e evidências determinados pelo perfil de certificação específico;
    - caso sejam detetadas não conformidades, dever-se-ão encetar os passos detalhados no **Capítulo 13**;
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 os requisitos de cibersegurança associadas ao nível de garantia pretendido, com possível exceção das medidas passíveis de exclusão;
6. Emissão de certificado pelo OC:

Versão Preliminar

- com um período de validade de 3 anos não podendo a data de entrada em vigor do mesmo ser anterior à data de decisão;

7. Publicação dos certificados do EC QNRCS pelas organizações certificadas, 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 XX**), e contendo a informação definida pelo **Modelo de Certificados do EC QNRCS** (ver **Anexo XX**);
8. Realização da auditoria de acompanhamento anual[4]
   - deve ter uma variação máxima de 30 dias de calendário em relação ao mês e finalização da auditoria de concessão e uma segunda auditoria de acompanhamento até dois anos e com 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 no EC QNRCS / início de novo ciclo[5]
   - deve ser realizada até 30 dias de calendário anteriores ao término da data de validade do certificado em vigor;
10. Realização de auditorias extraordinárias
    - sempre que:
      i. após a certificação, ocorram alterações significativas[6] na organização certificada e que sejam consideradas no âmbito de certificação no EC QNRCS ou que tenham consequências na definição desse âmbito[7];
      ii. o OC o determine, para verificação de uma situação de incumprimento chegada ao seu conhecimento;
      iii. determinadas pelo CNCS na sua qualidade de ANCC.
    - 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 da certificação da organização e que, por isso, afete a validade do certificado.
11. Realização de auditorias de seguimento:
    - sempre que 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
12. Revogação de certificados pelos OC
    - no caso de não cumprimento pelas organizações candidatas das regras definidas pelo EC QNRCS;

Versão Preliminar

[4] A iniciativa de marcar as auditorias previstas no ciclo de acompanhamento ou de renovação é da responsabilidade do OC

[5] Ver comentário anterior

[6] Entende-se por alterações significativas alterações internas ou externas de natureza tecnológica, organizacional, operacional, relacionadas com a cadeia de fornecimento ou com o contexto de risco, que tenham potencial para afetar de forma relevante o contexto da organização, os seus resultados pretendidos ou a validade da certificação.

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

- 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 do EC QNRCS emitidos pelo OC podem estar associados aos seguintes estados:

- Atribuído – quando da decisão positiva de certificação da conformidade com o EC QNRCS pelo OC.
- Suspenso – pode ocorrer a necessidade de suspensão de um certificado, pelo menos nas seguintes circunstâncias, entre outras:
  - Execução não eficaz de um Plano de Ações Corretivas pela organização certificada;
  - 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 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 organização certificada não pode fazer qualquer referência ao estatuto de organização 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 organização certificada, bem como não pode fazer qualquer utilização do certificado de conformidade e da marca e/ou etiqueta de certificação.
- Expirado – quando o certificado atingiu o final do seu prazo de validade, sem que tenha havido lugar à sua renovação.

A notificação pelo OC ao CNCS da alteração de estado de um certificado 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.

Versão Preliminar

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 estarem devidamente acreditados para este esquema.

Deve ser solicitado ao OC que originalmente emitiu o certificado uma declaração em como as auditorias previstas do presente ciclo, à data da transferência da certificação, se encontram 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 emissor do certificado deve ainda disponibilizar informação sobre o programa de auditorias para o ciclo que se encontra a decorrer.

O OC recetor do pedido de transferência da certificação deve solicitar à organização que realizou o pedido de transferência a documentação considerada necessária para realizar uma análise documental e fundamentar a decisão de aceitação do pedido de transferência. A documentação a solicitar deve, no mínimo, incluir:

- relatório da auditoria de concessão ou o último relatório da auditoria de renovação, conforme aplicável;
- relatórios das auditorias de acompanhamento que tenham decorrido desde a auditoria de concessão ou da última auditoria de renovação, conforme aplicável;
- reclamações recebidas e as ações tomadas, no âmbito da certificação;

O resultado da análise documental e a respetiva decisão devem ser registados.

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

O novo certificado deve dar continuidade à validade do certificado do OC anterior.

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.

No caso de não estarem cumpridos os requisitos para uma decisão de transferência, o OC recetor do pedido deve tratar a organização como um novo cliente.

Anulação voluntária

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

Incumprimento das regras do EC QNRCS

Em cumprimento do disposto pelo Art.º 63 do DL n.º 125/2025, a organização certificada estará sujeita a sanções no caso de incorrer nas infrações nele previstas, sendo o CNCS, na qualidade de Autoridade Nacional de Cibersegurança (Art.º 19 do DL n.º 125/2025), a organização responsável pela sua aplicação.

11. 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.

Versão Preliminar

Esta decisão é alcançada através da análise de evidências recolhidas durante os atos de auditoria, comparando com os critérios de auditoria associados ao perfil de certificação escolhido, referentes à aplicação das medidas do QNRCS, e outras que vierem a ser definidas, elencadas no respetivo anexo.

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 perfil, exceto as medidas passíveis de exclusão que são particulares à organização, conforme Declaração de Aplicabilidade).

Nos anexos referentes a cada um dos perfis de certificação que vierem a ser elaborados, são identificadas 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.

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

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

- **Não conformidade Maior** – Ocorre nos casos em que a medida de cibersegurança não se encontra implementada ou, se implementada, encontra-se totalmente desalinhada dos objetivos da medida de cibersegurança, 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 cibersegurança se encontra implementada, mas não consegue demonstrar totalmente que cumpre os respetivos objetivos;
- **Oportunidade de Melhoria** – Ocorre nos casos em que a medida de cibersegurança se encontra 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.

Tanto as não conformidades (maior ou menor) como as oportunidades de melhoria, devem ser registadas e devidamente enquadradas no Relatório de Auditoria, produzido pelo OC e entregue à organização auditada.

12. Regras para o tratamento de "Não Conformidades"

No seguimento do disposto pelo **Capítulo 11** 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:
    - Deve ocorrer num prazo de 30 dias de calendário desde a apresentação do relatório de auditoria, identificando, para cada não conformidade registada, as causas, as correções e/ou as ações corretivas e o prazo de implementação;
3. Avaliação do PAC pelo OC:

Versão Preliminar

- Se o PAC for aceite, cabe ao OC avaliar a necessidade de solicitar envio de evidências de implementação das ações para resolução das não conformidades registadas. No caso de haver lugar ao envio de evidências, o prazo não deve ultrapassar 60 dias de calendário desde a entrega do relatório da auditoria. Ressalva-se que, no caso de ter havido lugar ao registo de não conformidades maiores, o OC deve solicitar evidências da implementação das ações para resolução destas não conformidades, num prazo de 15 dias de calendário desde a comunicação da aceitação do PAC;
- Se o PAC não for aceite, o OC deve comunicar à organização a necessidade de reformulação do PAC, tendo a organização o prazo de 15 dias de calendário desde a comunicação da não aceitação para o seu reenvio;
- No caso do registo de não conformidades maiores, por princípio, o OC deve desencadear a realização de auditoria de seguimento para o seu encerramento, excetuando-se nas situações em que é possível avaliar a adequabilidade e implementação das ações e a sua eficácia de forma documental.

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.

13. Regras para a gestão dos certificados de conformidade EC QNRCS

Os certificados de conformidade com o EC QNRCS devem ser emitidos pelo OC de acordo com as regras definidas pelo **Anexo XX** do EC QNRCS.

14. Política de divulgação dos certificados de conformidade EC 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 encontra-se refletido no **Anexo XX**.

15. 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.5.33 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 organização 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.

A obrigação de garantia total de confidencialidade sobre todos os assuntos envolvidos na certificação é extensível a todas as partes envolvidas, incluindo colaboradores ou terceiros cuja intervenção tenha sido considerada

Versão Preliminar

necessária. Esta obrigação recai sobre toda a informação e documentação técnica e não técnica, comercial ou outra, relativa à organização candidata à certificação, de que possam ter conhecimento ao abrigo ou em relação ao processo de certificação pelo EC 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 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 Regulamento Geral sobre a 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.5.33 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 organização certificada.

16. Supervisão do ciclo de vida dos certificados de conformidade QNRCS

Com a publicação e entrada em vigor do Decreto-Lei n.º 125/2025, de 4 de dezembro, foi confirmado e clarificado o papel do Centro Nacional de Cibersegurança como Autoridade Nacional de Certificação de Cibersegurança. Com efeito, o art.º 19 do referido diploma estabelece as competências do CNCS neste domínio, em conformidade com o disposto no art.º 58 do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019.

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

- Gestão da publicação dos certificados de conformidade numa página QNCC;
- 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;

Versão Preliminar

- 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.

17. Histórico de revisões

Versão	Data	Modificação	Notas adicionais
VERSÃO 1.1	22/12/2021	Criação	Versão inicial para revisão
VERSÃO 1.5	28/12/2021	Integração de resultados de revisões	Versão entregue para publicação
VERSÃO 1.8	30/12/2021	Integração de resultados de revisões	Versão aprovada para publicação
VERSÃO 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	
VERSÃO 1.11	20/01/2022	Diversas alterações	
VERSÃO 1.12	24/01/2022	Alterações produzidas pela revisão do Anexo 5	
VERSÃO 1.13	26/01/2022	Correções diversas	NC Grave passou a NC Maior
VERSÃO 1.14.3	22/05/2022	Reformulação geral do Esquema	Integração de alterações motivadas pela revisão do Anexo 5
VERSÃO 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.
VERSÃO 2.1	26/08/2022	Revisão geral	Introdução de informação sobre análises de riscos de cibersegurança setoriais e clarificação da atuação do CNCS em sede de supervisão, e de alguns deveres dos OC
VERSÃO 2.3	07/12/2022	Revisão final	Revisão 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

Versão Preliminar

			como propósito a sua validação formal
Versão 3.0	29/09/2026	Revisão geral inicial do EC QNRCS, tendo em vista a sua adaptação e atualização em relação ao novo Regime Jurídico de Cibersegurança e ao novo Quadro Nacional de Referência para a Cibersegurança.	Introdução do conceito de perfil de certificação. Elaboração do Perfil de Certificação RJC como instrumento para a presunção de cumprimento das medidas de cibersegurança do RJC. Introdução do conceito de reconhecimento (presunção) do cumprimento das medidas do RJC por uma organização que se certifique de acordo com o Perfil de Certificação RJC, no nível de garantia correspondente ao nível que lhe seja exigido pelo RJC.

Versão Preliminar