Índice

1. Enquadramento do Esquema de Certificação QNRCS

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*.

O QNCC é concebido em alinhamento com o Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que introduz o "enquadramento europeu para a certificação da cibersegurança" em toda a União Europeia para produtos, serviços e processos de tecnologias de informação e comunicação (TIC). 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 **EUCC,** que representa o "*Common Criteria based European Cybersecurity Certification scheme*" ou o **EUCS**, "*European Cybersecurity Certification Scheme for Cloud Services*", entre outros.

Correspondentemente, o QNCC é o ecossistema nacional de certificação da cibersegurança no qual se desenvolvem e operam os diferentes esquemas de certificação nacionais, prevendo a possibilidade da criação e implementação de vários esquemas de certificação em âmbitos de aplicação que não estejam abrangidos por um esquema de certificação europeu, e sempre que a especificidade do objeto da certificação o justifique.

Por sua vez o **QNRCS** – *Quadro Nacional de Referência para a Cibersegurança* foi criado e disponibilizado pelo CNCS 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. O seu propósito é que as entidades o adotem de forma voluntária para assim beneficiar de uma abordagem homogénea e integral à sua conjuntura específica de cibersegurança e que, simultaneamente, promova uma resposta nacional às ciberameaças.

Em complemento ao QNRCS, o CNCS elaborou o **QACC** – *Quadro de Avaliação de Capacidades de Cibersegurança*, enquanto referencial que define 3 (três) diferentes níveis de capacidade para a demonstração das práticas de segurança que as organizações implementam e operacionalizam no seu contexto.

Este alinhamento do QNRCS e do QACC permite ao CNCS, assumindo o seu papel de **ANCC** – *Autoridade Nacional de Certificação em Cibersegurança,* desenvolver o **EC QNRCS** – Esquema de Certificação para o Quadro Nacional de Referência para a Cibersegurança.

O EC QNRCS é, assim, concebido para permitir que as organizações públicas e privadas possam atestar a implementação das suas práticas de segurança organizativas, processuais, tecnológicas e humanas, através da certificação tendo como critério de referência o QNRCS e respetivo QACC.

2. Objetivos 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.

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".

Para monitorização das atividades de certificação, é nomeada uma "entidade supervisora" que se encarrega de avaliar o desempenho do "esquema de certificação" e garantir que os seus requisitos são cumpridos e são conformes com o estabelecido.

O “esquema de certificação” consiste num conjunto de regras, práticas e procedimentos que a entidade supervisora emite para que os organismos de certificação e as organizações auditadas entendam os compromissos que as partes devem aceitar, cumprir e fazer cumprir.

O presente documento descreve o Esquema de Certificação cuja entidade supervisora é o CNCS, na qualidade de Autoridade Nacional de Certificação em Cibersegurança, sendo os requisitos para a certificação os que constam do QNRCS e QACC, 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 QNRCS tem ainda 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 respetivo Plano de Ação Transversal para a legislatura, promovendo as devidas condições para a certificação de entidades da Administração Pública no QNRCS.

Salientam-se alguns benefícios para as organizações certificadas no EC QNRCS:

- 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.

3. Âmbito de aplicação do Esquema de Certificação QNRCS

O âmbito de aplicação do Esquema de Certificação QNRCS caracteriza-se por:

- Estar incluído no QNCC;
- Os critérios de auditoria para decisão de certificação serem definidos pelo QNRCS e pelo QACC;
- Serem destinatárias as organizações nacionais públicas ou privadas, sendo voluntárias na sua adesão à certificação QNRCS;
- As medidas para cada nível serem todas de implementação obrigatória, mas poderem ser aplicadas a toda a organização ou a partes significativas da atividade da organização.

Exclui-se do âmbito de aplicação da presente versão do Esquema de Certificação QNRCS:

- Qualquer tipo de equivalência da certificação com outro esquema de certificação fora do QNCC;
- Cibersegurança da cadeia de abastecimento para os prestadores de serviços nas organizações;
- Cibersegurança dos prestadores de serviços *Cloud*.

4. 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			
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
Não conformidade Grave	NC Grave		
Não conformidade Menor	NC Menor		
Nível de Capacidade		Representa grupos cumulativos de medidas de segurança que a organização implementa, conferindo 3 níveis de execução efetiva: Inicial, Intermédio e Avançado	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		

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 internacionalmente reconhecidos.

No **Anexo 1** pode ser encontrada a hiperligação para a lista comentada de referências utilizadas.

6. Níveis de capacidade versus garantia

O QACC apresenta 3 (três) níveis de capacidade para implementação dos requisitos do QNRCS.

São identificados como: “Inicial” – “Intermédio” – “Avançado”

Trata-se de níveis complementares e cumulativos, que exigem 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.

No contexto do EC QNRCS, cada organização deve identificar o nível de capacidade para o qual pretende atingir a sua certificação, de acordo com as regras definidas pelo **Capítulo 10** do presente documento.

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

As organizações candidatam-se a um nível de capacidade, através de um formulário disponível no **Anexo 2,** através de uma hiperligação.

O **OAC**[1] - *Organismo de Avaliação de Conformidade* escolhido pela organização candidata analisa a candidatura, podendo aceitar ou propor que o procedimento de certificação tenha por objetivo um outro nível de capacidade.

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

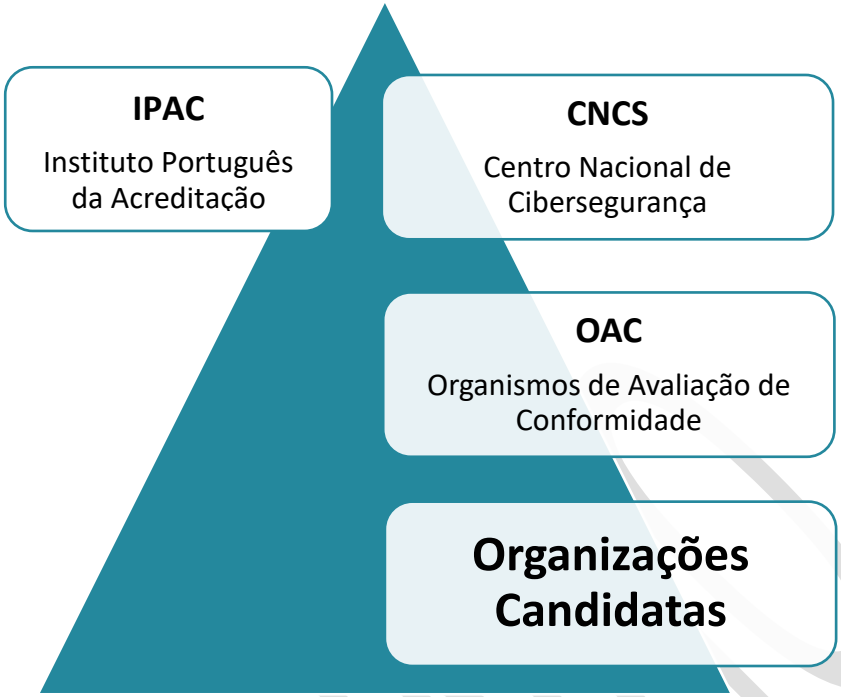
Qualquer alteração do âmbito de certificação ou do nível da capacidade ao qual se candidata, representa a necessidade de a organização voltar a submeter nova candidatura.

Havendo divergências de opinião entre a organização candidata e o OAC, compete a este a comunicação da situação ao organismo nacional de acreditação dos OAC, o **IPAC** – *Instituto Português de Acreditação* que, por sua vez, poderá solicitar parecer ao CNCS, em caso de necessidade de apoio técnico.

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:

[1] Organismos de avaliação de conformidade, muitas vezes conhecidos na sua sigla em língua inglesa como CAB (*Conformity assessment body*)



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

Entidade	Papéis	Funções e Responsabilidades
IPAC	Organismo nacional de acreditação	• Acreditar os OAC para execução do processo de certificação QNRCS • Resolução de divergências entre os OAC e as organizações certificadas ou candidatas • Supervisão dos OAC
CNCS	Autoridade Nacional de Certificação da Cibersegurança	• Gestão, manutenção/atualização e publicitação do Esquema de Certificação QNRCS • Supervisão dos certificados emitidos e das organizações certificadas • Apoio ao IPAC na supervisão dos OAC • Emissão dos códigos QR • Gestão do Portal QNCC para publicação dos certificados QNRCS • Ponto de contacto para a cooperação internacional
OAC	Entidades responsáveis pela execução do processo de certificação	• Assegurar a acreditação pelo IPAC • Executar o processo de certificação QNRCS • Decisão de certificação QNRCS • Emissão dos certificados QNRCS e gestão do respetivo ciclo 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	• 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.

8. Requisitos para os Organismos de Avaliação de Conformidade (OAC)

Um OAC deve ser uma organização acreditada pelo IPAC na norma ISO/IEC 17065:2012 *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 OAC devem assegurar o cumprimento dos seguintes requisitos específicos para a devida acreditação para a certificação no EC QNRCS:

- Assegurar o cumprimento de outros requisitos eventualmente a definir pelo CNCS e/ou pelo IPAC no âmbito do esquema de acreditação do EC QNRCS;
- Assegurar a qualificação de auditores de certificação e 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 OAC observar as seguintes regras gerais do EC QNRCS:

- Cumprir os procedimentos de comunicação com o CNCS estabelecidos no âmbito do EC QNRCS *(a defnir)*;
- Cumprir com todos os demais requisitos definidos no EC QNRCS para os OAC, 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.

9. Métodos de avaliação e critérios de auditoria

A conformidade de uma organização candidata à certificação QNRCS resulta da decisão do OAC, 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 estabelecidos no QNRCS e QACC.

O QACC identifica as evidências que a organização candidata deve apresentar, e que deverão ser confirmadas pelo OAC 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 pelo QNRCS e pelo QACC para cada nível de capacidade.

Compete ao OAC a análise do conjunto de evidências recolhidas e a produção de constatações sustentadas para a declaração de conformidade, ou de não conformidade, em cada medida de segurança analisada.

Para a análise de cada medida de segurança, podem resultar a identificação dos seguintes resultados de auditoria:

- **Não conformidade Grave** – 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.

10. Requisitos para os candidatos à certificação QNRCS

Os candidatos à certificação no EC QNRCS devem:

- ser organizações estabelecidas em território nacional;
- ter implementadas as medidas de segurança definidas no QNRCS para o nível de capacidade a que se candidatam;
- ter registadas as evidências da implementação de tais medidas de segurança, de acordo com os métodos e procedimentos definidos no QACC;
- disponibilizar e garantir a veracidade das informações e os contactos solicitados no formulário de candidatura.

Os requisitos para os candidatos à certificação QNRCS devem ser analisados pelos OAC, após a receção do respetivo formulário de candidatura à certificação QNRCS.

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

11. Ciclo de vida da certificação QNRCS

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

As etapas definidas neste ciclo de vida são as seguintes:

1) Candidatura da organização à certificação QNRCS e respetiva aprovação pelo OAC.
2) Realização da auditoria de concessão pelo OAC, que deve resultar na emissão de um certificado de conformidade QNRCS, quando demonstrada a conformidade em todas as medidas de segurança associadas ao nível de capacidade pretendido. O certificado deve ter a validade de 3 anos.
3) Realização da auditoria de acompanhamento anual.
4) Realização de auditorias de renovação da certificação QNRCS, que devem ser realizadas até 30 dias do término da data de validade do certificado QNRCS em vigor.
5) Realização de auditorias extraordinárias, sempre que ocorram alterações significativas na organização certificada e que sejam consideradas no âmbito de certificação QNRCS ou que tenham consequências na definição desse âmbito, ou se determinadas pelo CNCS na sua qualidade de ANCC, ou ainda para a confirmação da execução com eficácia de um **PAC** - Plano de Ações Corretivas.
   Estas auditorias extraordinárias podem ocorrer, por decisão do OAC 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.

6) Publicação dos certificados QNRCS pelas organizações candidatas, OAC e CNCS, 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**).
7) Revogação de certificados QNRCS pelos OAC, no caso de não cumprimento pelas organizações candidatas das regras definidas pelo EC QNRCS.

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

- Atribuído – quando da decisão positiva de certificação QNRCS pelo OAC
- Suspenso – pode ocorrer a necessidade de suspensão de um certificado QNRCS nas seguintes circunstâncias:
    - Execução não eficaz de um Plano de Ações Corretivas pela organização candidata;
    - Pedido de alteração do âmbito de aplicação QNRCS pela organização certificada;
    - Pedido de redução de nível de capacidade QNRCS pela organização certificada;
    - Decisão pelo CNCS no seguimento de atividades de supervisão do EC QNRCS, devido à deteção de não conformidades ou de incumprimentos das regras do presente EC QNRCS.

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

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

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

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

- Revogado – quando o OAC 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.

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

A notificação pelo OAC ao CNCS, utilizando o procedimento de comunicação estabelecido, da alteração de estado de um certificado QNRCS deve ocorrer no prazo máximo de 5 dias úteis.

Sempre que uma organização certificada pretenda alterar o seu âmbito de aplicação QNRCS ou o seu nível de capacidade, deve voltar a apresentar um novo formulário de candidatura ao OAC.

Em cumprimento do disposto pelo Artigo 21º do Decreto-Lei n.º 65/2021, de 30 de julho, 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. Regras para acesso, arquivo e preservação de informações das atividades de certificação

Os OAC devem manter um sistema de registos de acordo com os requisitos da norma de acreditação ISO / IEC 17065.

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 das 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 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. 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.

13. Regras para a gestão dos certificados de conformidade QNRCS

Os certificados de conformidade QNRCS devem ser emitidos pelo OAC de acordo com as regras definidas pelo **Anexo 3** do Esquema de Certificação QNRCS.

14. 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 OAC, no contexto do Esquema de Certificação do QNRCS. Este documento é acessível no **Anexo 4**, através de uma hiperligação.

15. Regras para o tratamento de "Não Conformidades"

No seguimento do disposto pelo **Capítulo 9** do EC QNRCS, poderão ocorrer situações em que os resultados de auditoria identifiquem não conformidades.

Sempre que tal aconteça, a organização candidata deve proceder à criação e entrega ao OAC de um **PAC** – Plano de Ações Corretivas, no prazo máximo de 30 dias.

O OAC deve analisar a proposta de PAC, informando a organização candidata da sua aprovação ou não aprovação, no prazo máximo de 5 dias úteis.

Os prazos máximos para a execução com eficácia do PAC são definidos em função do nível de capacidade em análise:

- Nível Inicial – 30 dias
- Nível Intermédio – 60 dias
- Nível Avançado – 90 dias

Em casos especiais, a organização candidata pode solicitar ao OAC uma extensão do prazo, que, no limite, poderá representar 1/3 do prazo máximo definido.

Nos casos em que o OAC entenda ser necessário, deverá enviar ao CNCS, através do procedimento de comunicação estabelecido *(a definir)*, um pedido de parecer fundamentado para a prorrogação deste prazo.

16. 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 as seguintes:

- Monitorização dos certificados emitidos e das organizações que os titulam;
- Gestão da publicação dos certificados de conformidade no portal QNCC;

- Decisão para a realização de auditorias extraordinárias em organizações certificadas, eventualmente com utilização de critérios de amostragem a definir caso a caso;
- Ratificação da decisão do OAC para a realização de auditorias extraordinárias no caso de a organização certificada ter efetuado uma notificação de um incidente de cibersegurança ao CNCS que seja considerado de impacto relevante ou substancial, ou que provoque impactos no que respeita à confidencialidade, integridade e disponibilidade da segurança das suas redes e dos seus sistemas de informação abrangidos no âmbito de certificação QNRCS;
- Apoio técnico ao IPAC, a seu pedido e mediante a sua coordenação, na supervisão das atividades dos OAC e na resolução de divergências entre os OAC 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.

17. 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

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.