CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

ESQUEMA DE CERTIFICAÇÃO QNRCS

POLÍTICA DE DIVULGAÇÃO DOS CERTIFICADOS QNRCS

Índice

1. Âmbito e objetivo da política de divulgação dos certificados QNRCS

A política de divulgação de certificados de conformidade com o Quadro Nacional de Referência para a Cibersegurança (QNRCS) tem como objetivo descrever as regras e práticas para a divulgação dos certificados emitidos pelos organismos de certificação (OC), no contexto do referido esquema.

2. Compromissos do CNCS para a aplicação da política

O Centro Nacional de Cibersegurança (CNCS) é a entidade supervisora do esquema de certificação de conformidade com o QNRCS (EC QNRCS), e, como tal, tem a seu cargo a gestão do ciclo de vida da política de divulgação de certificados emitidos ao abrigo deste esquema de certificação.

O ciclo de vida desta política inclui a sua criação, divulgação, publicação, revisão e atualização periódica por forma a assegurar a sua contínua aplicabilidade para o âmbito e objetivos descritos.

3. Regras e requisitos para a divulgação dos certificados QNRCS

São em seguida apresentadas as regras e requisitos que se aplicam à divulgação de certificados referentes ao EC QNRCS, organizados em função dos intervenientes neste esquema de certificação:

3.1. Aplicáveis ao CNCS

- Gerar o(s) "Código QR" solicitados pelos OC para constarem no certificado, sob a forma de uma hiperligação, publicada através da página web dedicada ao Quadro Nacional de Certificação da Cibersegurança, gerida pelo CNCS.
- Divulgar os certificados na referida página web, por um prazo correspondente ao período de validade do certificado.
- Publicar alterações aos estados dos certificados, em função das notificações dos OC.
- Atender aos prazos para a publicação do certificado e da eventual alteração do seu estado, conforme definido no **Capítulo 11** do EC QNRCS.
- Efetuar a relocalização da informação associada a um certificado que tenha expirado ou tenha sido revogado, e assim que essa condição se verifique, para uma página de arquivo, sob o título de "certificados não válidos", que ficará preservada durante, pelo menos, cinco (5) anos.

3.2. Aplicáveis ao OC

- Emitir os certificados QNRCS sempre que uma entidade candidata cumpra os requisitos de conformidade referentes ao nível de garantia a que se candidatou e que foi aprovado pelo OC.
- Emitir os certificados respeitando o definido no **Anexo 4** do EC QNRCS, nomeadamente o modelo e marcas a utilizar no certificado QNRCS.
- Proceder, em todos os momentos e obrigatoriamente, à clara identificação do estado do certificado, sempre que emitido ou alterado, tendo em conta as definições referentes aos diferentes estados constantes no **Capítulo 11** do EC QNRCS.
- Solicitar, conforme lhe compete, a geração de um "Código QR" ao CNCS.
- Os certificados podem ser divulgados pelos organismos de certificação emitentes nos seus sítios web, sendo publicados de acordo com as instruções emitidas pelo CNCS para essa finalidade.

- Comunicar ao CNCS qualquer alteração do estado de um certificado, tendo em atenção o prazo definido para este efeito no EC QNRCS.
- Compete ao OC a eventual decisão de "suspensão" para um certificado que ainda se encontra dentro do seu período de validade, de acordo com as regras previstas no EC QNRCS, sendo que nesta condição deve ser associada a esta declaração o motivo de suspensão e a data do fim do período de suspensão.

3.3. Aplicáveis à organização certificada

- As organizações certificadas podem usar certificados publicados na página web dedicada ao Quadro Nacional de Certificação da Cibersegurança, gerida pelo CNCS, para fins comerciais ou outros, mas não podem modificar o certificado e, em particular, devem sempre incluir uma hiperligação para o certificado original no sítio web do CNCS para permitir que os interessados verifiquem o estado atual do certificado.
- Apenas organizações detentoras de um certificado válido podem ser promovidas como organizações certificadas.
- As organizações certificadas não podem utilizar certificados suspensos, expirados ou definidos pelo OC como revogados, nas suas atividades de divulgação comercial ou de marketing.
- A utilização indevida de certificados conforme, mas não se limitando, aos usos descritos no ponto anterior constitui um incumprimento das regras do EC QNRCS, sujeito às sanções nele previstas, assim como às contraordenações estabelecidas no n.º 2 do art.º 21 do Decreto-Lei n.º 65/2021, de 30 de julho.

4. Funções e responsabilidades

Tendo em conta a segregação de regras práticas apresentadas pelo **Capítulo 3** da presente Política, identifica-se o seguinte quadro de funções e responsabilidades no seu âmbito de aplicação:

Entidade	Funções e Responsabilidades	Notas adicionais
CNCS	1. Gestão do ciclo de vida da política 2. Definição do modelo do certificado QNRCS, incluindo as marcas e rótulos 3. Geração do "Código QR" para inclusão nos certificados pelo OC 4. Publicação dos Certificados e das suas alterações em página web dedicada ao Quadro Nacional de Certificação da Cibersegurança, gerida pelo CNCS	1. Inclui ações de sensibilização e para incentivo da sua aplicação 2. Este modelo é identificado em detalhe no **Anexo 4** do Esquema de Certificação QNRCS 3. Os "Códigos QR" serão gerados tendo por base uma hiperligação para a página web dedicada ao Quadro Nacional de Certificação da Cibersegurança, gerida pelo CNCS, onde irá constar a informação relevante do certificado. 4. As alterações ao estado dos certificados são realizadas de acordo com as definições do EC QNRCS
OC	1. Emissão de certificados QNRCS 2. Solicitação ao CNCS do "Código QR"	1. De acordo com o modelo definido pelo CNCS 2. Os "Códigos QR" serão gerados tendo por base uma hiperligação para a página web dedicada ao Quadro Nacional de Certificação da

	3. Publicação do certificado no sítio web do OC (opcional) 4. Cumprir e fazer cumprir a presente política de divulgação	Cibersegurança, gerida pelo CNCS, onde irá constar a informação relevante do certificado. 4. Os OC incluem esta determinação aquando da formalização da aceitação da candidatura à certificação, com as organizações candidatas
Organização certificada	1. Utilizar o certificado emitido pelo OC de acordo com as regras e práticas da presente política	1. O incumprimento da presente política deverá ser considerado um incumprimento das regras do EC QNRCS, podendo ser aplicadas as sanções previstas

5. Documentos de referência

A política de divulgação dos certificados QNRCS tem por referência a lista de referências legais, normativas e regulamentares definida como **Anexo 2** do EC QNRCS.

6. Classificação da informação

A política de divulgação dos certificados QNRCS está classificada como **PÚBLICA**.

7. Divulgação e publicação

Tendo em conta a classificação deste documento, é permitida a sua divulgação não controlada através de qualquer meio de divulgação digital, verbal ou em papel.

A sua publicação será realizada em formato digital PDF, no portal do CNCS.

8. Revisão e atualização

A política de divulgação dos certificados QNRCS será revista e atualizada sempre que se entender relevante para a sua correta interpretação e aplicação.

9. Histórico de revisões

Versão	Data	Modificação	Notas adicionais
VERSÃO 1.1			Versão inicial para revisão.
VERSÃO 1.4			Versão pronta para publicação e recolha de contributos.
VERSÃO 1.6	07/12/2022	Alteração de nomenclaturas para alinhamento com a versão final do esquema de certificação da conformidade com o QNRCS e respetivos Anexos.	
VERSÃO 1.7	28/12/2022	Pequenas revisões editoriais e ortográficas e alinhamento com nova numeração dos Anexos.	Versão pronta para publicação pelo CNCS.