1 Objetivo

O presente documento tem como finalidade definir os requisitos específicos de acreditação para fins de certificação no âmbito do Esquema de Certificação (EC) da conformidade com o Quadro Nacional de Referência para a Cibersegurança (QNRCS) - https://www.cncs.gov.pt/pt/certificacao-nacional/.

2 Autoridade competente

O Centro Nacional de Cibersegurança (CNCS - https://www.cncs.gov.pt) é a autoridade competente na matéria de cibersegurança e o dono deste esquema de certificação regulamentar.

3 Norma de acreditação

Considerando o esquema de certificação em causa, este serviço está incluído no esquema de acreditação de Organismos de Certificação de Produtos, Processos e Serviços, cujo referencial de acreditação é a NP EN ISO/IEC 17065.

4 Documentos aplicáveis

Considera-se como documentos normativos aplicáveis (de cumprimento obrigatório) os seguintes:

- Esquema de certificação QNRCS
- Anexo 1 – Lista de critérios de auditoria
- Anexo 2 – Lista de referências legais, normativas e regulamentares
- Anexo 3 – Formulário de candidatura à certificação (*para clientes dos organismos de certificação*)
- Anexo 4 – Modelo e marcas dos certificados QNRCS
- Anexo 5 – Política de divulgação dos certificados QNRCS

Pode ainda ser oportuno aplicar o Guia de Gestão de Riscos do CNCS.

5 Marca de certificação

O Gabinete Nacional de Segurança / Centro Nacional de Cibersegurança é a entidade detentora da marca de certificação 'QNRCS', devendo o OC evidenciar estar autorizado a atribuir o uso desta marca aos clientes que certifica.

Pode ser consultada em https://www.cncs.gov.pt/pt/certificacao-nacional/ a informação relevante sobre esta iniciativa, incluindo a listagem dos organismos de certificação autorizados a licenciar a marca de certificação, bem como as empresas certificadas.

6 Condições de acesso

Para que possa ser aceite a candidatura de um organismo de certificação (OC), e posteriormente manter a respetiva acreditação, deve o mesmo:

- Não estar em estado de insolvência, liquidação ou de cessação de atividade, ou ter pendentes processos correspondentes;
- Não ter sido condenado, por sentença transitada em julgado, por qualquer delito que afete a honorabilidade profissional, nomeadamente fraude, ou ter sofrido punição disciplinar por falta grave em matéria profissional, se, entretanto, não tiver ocorrido a reabilitação;
- Não enviar, de forma consciente ou intencional, informação falsa, incompleta ou omissa com indução de dolo ao IPAC;
- Dispor de pelo menos um auditor com certificado de formação com aproveitamento, emitido pelo CNCS, nos termos definidos no número 9.2, para cada nível de certificação em que opere.

7 Descrição do âmbito de acreditação

A descrição dos âmbitos de acreditação é feita conforme tabela abaixo, sem discriminação de sector de atividade ou nível de certificação, o que implica que o OC deve poder demonstrar ser competente para qualquer um.

Produto/ Processo/ Serviço *Product/ Process/ Service*	Especificação de Certificação *Certification criteria*	Procedimento de Certificação *Certification procedure*
C35 - SERVIÇOS INFORMÁTICOS E CONEXOS *INFORMATION TECHNOLOGY SERVICE*		
C35.09 – Esquema de certificação QNRCS		
Certificação em cibersegurança, níveis "Básico", "Substancial" e "Elevado"	EC QNRCS – Anexo 1	EC QNRCS

8 Procedimento de acreditação

O procedimento de acreditação aplicável encontra-se descrito no DRC001 - Regulamento Geral de Acreditação e no DRC006 - Procedimento para Acreditação de Organismos de Certificação, os quais são complementados pelo conteúdo do presente documento.

Para a concessão ou extensão da acreditação será necessária a realização de uma avaliação de escritório ao OC, complementada pela realização de pelo menos 1 testemunho de uma auditoria no nível mais complexo que o OC certifique - assim, se for realizado um primeiro testemunho no nível "Elevado", não serão necessários testemunhos adicionais para certificar nos outros níveis; porém, se o primeiro testemunho for no nível "Substancial", será necessário um testemunho adicional para certificar no nível "Elevado", mas não no nível "Básico"; se o primeiro testemunho for no nível "Básico", será necessário testemunho adicional para qualquer dos níveis "Substancial" e "Elevado", aplicando-se depois a regra de testemunho desse nível.

Para a manutenção da acreditação, será realizado normalmente 1 testemunho de uma auditoria no nível mais complexo que o OC certifique, por ano, salvo se as considerações de risco implicarem uma abordagem distinta. Estes testemunhos serão complementados pela(s) correspondente(s) avaliação(ões) de escritório no OC.

9 Requisitos para o processo de certificação

O processo de certificação deve seguir o exposto no EC QNRCS, bem como as disposições abaixo.

9.1 Duração das auditorias

A duração das auditorias a cada empresa candidata ou certificada é estabelecida tendo em conta o nível de complexidade da certificação, a dimensão da empresa e a existência de certificações acreditadas complementares, conforme disposto na Tabela 10.1 abaixo.

Tabela 10.1 - Duração das auditorias de certificação de cibersegurança

A duração mínima das auditorias de certificação deste esquema está indicada na tabela a seguir, repartida pelos níveis de certificação e tipos de auditoria, devendo a duração mínima ser aumentada face a necessidades de amostragem de postos de trabalho ou equipamentos (face à sua potencial criticidade ou vulnerabilidade) ou a fatores de risco relevantes (por exemplo, um histórico de incidentes de cibersegurança que pela sua gravidade e/ou frequência impliquem um risco acrescido).

A duração das auditorias pode ser diminuída para a indicada na coluna "c/SGSI", se a empresa tiver certificação acreditada em SGSI (ISO 27001) pelo IPAC ou por qualquer signatário do respetivo acordo multilateral da EA ou IAF, à data da realização de cada auditoria. A duração mínima da auditoria de renovação é dada pela coluna "c/SGSI" da correspondente auditoria de concessão, independentemente de ter ou não essa certificação acreditada.

Até *n* FTE (*Full Time Equivalent*)	Nível Básico				Nível Substancial				Nível Elevado			
	Concessão		Acompanham/		Concessão		Acompanham/		Concessão		Acompanham/	
	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI
1	5	3,5	2,5	2	6	4	3	2	7,5	5,5	4	3
11	6	4	3	2	7	5	3,5	2,5	8,5	6	4,5	3
16	7	5	3,5	2,5	8	5,5	4	3	9,5	6,5	5	3,5
26	8,5	6	4,5	3	9,5	6,5	5	3,5	11	7,5	5,5	4
46	10	7	5	3,5	11	7,5	5,5	4	12,5	9	6,5	4,5
66	11	7,5	5,5	4	12	8,5	6	4	13,5	9,5	7	5
86	12	8,5	6	4	13	9	6,5	4,5	14,5	10	7,5	5,5
126	13	9	6,5	4,5	14	10	7	5	15,5	11	8	5,5
176	14	10	7	5	15	10,5	7,5	5,5	16,5	11,5	8,5	6
276	15	10,5	7,5	5,5	16	11	8	5,5	17,5	12,5	9	6,5
426	16,5	11,5	8,5	6	17,5	12,5	9	6,5	19	13,5	9,5	6,5
626	17,5	12,5	9	6,5	18,5	13	9,5	6,5	20	14	10	7
876	18,5	13	9,5	6,5	19,5	13,5	10	7	21	14,5	10,5	7,5
1176	19,5	13,5	10	7	20,5	14,5	10,5	7,5	22	15,5	11	7,5
1551	21	14,5	10,5	7,5	22	15,5	11	7,5	23,5	16,5	12	8,5
2026	22	15,5	11	7,5	23	16	11,5	8	24,5	17	12,5	9
2676	23	16	11,5	8	24	17	12	8,5	25,5	18	13	9
3451	24	17	12	8,5	25	17,5	12,5	9	26,5	18,5	13,5	9,5
4351	25	17,5	12,5	9	26	18	13	9	27,5	19,5	14	10
5451	26	18	13	9	27	19	13,5	9,5	28,5	20	14,5	10
6801	27	19	13,5	9,5	28	19,5	14	10	29,5	20,5	15	10,5
8501	28	19,5	14	10	29	20,5	14,5	10	30,5	21,5	15,5	11
Mais	Seguir progressão				Contatar IPAC				Contatar IPAC			

9.2 Amostragem de locais

Considera-se uma organização plurilocal ('*multisite*') aquela que possui vários locais no âmbito de certificação.

Pode ser efetuada uma amostragem de locais que apenas executem processos e atividades similares, desde que nenhum desses locais disponha de ativos críticos para o âmbito da certificação. É condição necessária que a empresa candidata ou certificada disponha de uma função central que é responsável pela definição, planeamento e controle desses processos e atividades similares, incluindo a sua monitorização e medição contínuos. É ainda requerido que esta função central tenha autoridade para assegurar que os locais implementem correções e/ou ações corretivas quando necessário.

A duração da auditoria deve ser calculada para o número total de trabalhadores (FTE) e depois distribuída com base no risco pelos locais elegidos segundo a amostragem efetuada. Devem ser guardados registos que justifiquem a amostragem considerada, bem como a duração da auditoria em cada local.

Estabelecem-se os seguintes critérios de amostragem para um número x de locais com processos e atividades similares e sujeitos a uma função central ($\surd$ = raiz quadrada):
- na auditoria de concessão devem ser auditados $\surd x$ (arredondado para cima);
- na auditoria de acompanhamento devem ser auditados 0,6 $\surd x$ (arredondado para cima);
- na auditoria de renovação devem ser auditados 0,8 $\surd x$ (arredondado para cima);
- em cada auditoria, a função central é sempre auditada e 25% da amostra deve ser selecionada aleatoriamente, podendo haver ajustes ao planeamento de locais selecionados após a auditoria à função central. A restante amostra deve ser escolhida com base no risco e na representatividade.

Para os locais em que não seja possível estabelecer uma amostragem conforme definido acima, o OC deve:
- na auditoria de concessão, auditar todos os locais;
- em cada auditoria de acompanhamento, auditar cerca de 1/3 dos locais e completar a amostragem de todos os locais na auditoria de renovação, de modo a que, em cada ciclo de certificação, sejam auditados todos os locais.

Sempre que seja solicitada a inclusão de um novo local no âmbito de certificação, deve seguir-se a abordagem estabelecida para as auditorias de concessão: se for possível a amostragem, auditam-se $\surd x$ (arredondado para cima), senão auditam-se todos os novos locais a incluir.

9.3 Requisitos de competência

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 no Anexo 1 do EC QNRCS para 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

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.

9.4 Registos de auditoria

Os relatórios de auditoria, em conjunto com as correspondentes listas de comprovação, devem poder evidenciar a verificação da conformidade com cada um dos critérios aplicáveis do Anexo 1 - Lista de critérios de Auditoria, ao EC QNRCS.