1. Objetivo

O presente documento tem como objetivo definir o serviço de acreditação para a certificação de cibersegurança, no contexto da iniciativa dos Selos de Maturidade Digital, conforme definido na DNP TS 4577-1.

2. Entidade competente

O Centro Nacional de Cibersegurança (CNCS - https://www.cncs.gov.pt) é a autoridade competente na matéria de cibersegurança. A Imprensa Nacional – Casa da Moeda, S. A. (INCM - https://www.incm.pt) é a entidade detentora da marca de certificação 'Selos de Maturidade Digital'.

3. Norma de Acreditação

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

4. Documentos Aplicáveis

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

- DNP TS 4577-1, publicado pelo Instituto Português da Qualidade, I.P.;
- Regulamento de utilização da Marca Nacional 'Selos de Maturidade Digital', emitido pela INCM.

5. 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 qualificado para cada nível de certificação.

6. 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*		
C35.08 - Certificação de cibersegurança em conformidade com Selo de Maturidade Digital nacional		
Selo de Maturidade Digital em cibersegurança, níveis "Bronze", "Prata" e "Ouro"	DNP TS 4577-1:2021	DNP TS 4577-1:2021 *Procedimento(s) de certificação do OC, se aplicável*

Nota: O âmbito de acreditação constante do Anexo Técnico de Acreditação deverá fazer referência à versão de cada norma em vigor, exceto nos casos em que o organismo de certificação dispõe de uma descrição flexível do âmbito de acreditação.

7. 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 nas instalações do 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 "Ouro", não serão necessário testemunhos adicionais para certificar nos outros níveis; porém, se o primeiro testemunho for no nível "Prata", será necessário um testemunho adicional para certificar no nível "Ouro", mas não no nível "Bronze"; se o primeiro testemunho for no nível "Bronze", será necessário testemunho adicional para qualquer dos níveis "Prata" e "Ouro", aplicando-se depois a regra de testemunho desse nível.

Para a manutenção da acreditação, será realizado pelo menos 1 testemunho de auditoria em cada um dos níveis em que o OC certifique, em cada ciclo de acreditação. Estes testemunhos serão complementados pela(s) correspondente(s) avaliação(es) nas instalações do OC. Nas situações em que o IPAC considere existir um baixo risco de incumprimento dos requisitos de acreditação, nomeadamente quando exista pouca atividade de certificação, poderá ser dispensada a realização de testemunho no ciclo ou nível para se evitar repetir a avaliação no mesmo cliente do OC.

8. Requisitos para o processo de certificação

O processo de certificação deve seguir o exposto na DNP TS 4577-1, bem como as disposições abaixo.

8.1 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 no Anexo 1.

8.2 Requisitos de competência

O pessoal do OC com influência no procedimento 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 A da DNP TS 4577-1 para o nível correspondente de certificação.

Considera-se que esse conhecimento pode ser obtido através de uma das fontes abaixo:

- habilitação escolar ou universitária cobrindo as medidas citadas e experiência profissional mínima:
  - 12.º ano do ensino secundário ou curso profissional ou curso técnico-profissional, na área das Tecnologias de Informação e Comunicação, Ciências Informáticas ou equivalentes + 2 anos de experiência relevante no setor das tecnologias de informação e comunicação, preferencialmente na área da segurança de redes e sistemas de informação; OU
  - licenciatura em Engenharia Informática ou equivalente + 1 ano de experiência relevante no setor das tecnologias de informação e comunicação, preferencialmente na área da segurança de redes e sistemas de informação;

- formação profissional específica nas medidas citadas:
  - competência técnica de acordo com a norma NP ISO/IEC 27001 ou equivalente; OU
  - formação profissional específica credenciada por entidades competentes;

- experiência profissional significativa na implementação ou uso das medidas citadas:
  - 5 anos de experiência relevante na área da segurança de redes e sistemas de informação;

Para o nível "Ouro" será necessário acrescentar requisitos ao nível da gestão de risco - assim, as equipas auditoras para certificar entidades no nível "Ouro" devem ter, pelo menos, um auditor com competência técnica de acordo com a norma ISO/IEC 27005.

Anexo 1 - Duração das auditorias de certificação de cibersegurança

A duração mínima das auditorias de certificação deste esquema está indicada na tabela abaixo, 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 a fatores de risco relevantes (por exemplo, histórico de incidentes de cibersegurança). A duração das auditorias pode ser diminuída para a indicada na coluna "c/SGSI", se a empresa tiver certificação acreditada em SGSI (ISO 27001) 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*	Nível Bronze				Nível Prata				Nível Ouro			
	Concessão		Acompanham/		Concessão		Acompanham/		Concessão		Acompanham/	
	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI	mínimo	c/SGSI
5	1,5	1	1	0,5	2	1,5	1,5	1	2,5	1,5	1,5	1
15	2	1,5	1	1	2,5	2	1,5	1,5	3	2,5	1,5	1,5
25	2,5	2	1	1	3	2,5	1,5	1,5	4	3	1,5	1,5
45	2,5	2	1,5	1	3	2,5	2	1,5	4	3	2,5	1,5
65	3	2	1,5	1	3,5	2,5	2	1,5	4,5	3	2,5	1,5
85	3,5	2,5	1,5	1	4,5	3	2	1,5	5,5	4	2,5	1,5
125	3,5	2,5	2	1,5	4,5	3	2,5	2	5,5	4	3	2,5
175	4	3	2	1,5	5	3,5	2,5	2	6	4,5	3	2,5
225	4,5	3	2	1,5	5,5	3,5	2,5	2	7	4,5	3	2,5
275	4,5	3	2,5	2	5,5	3,5	3	2,5	7	4,5	4	3
350	5	3,5	2,5	2	6	4,5	3	2,5	7,5	5,5	4	3
425	5,5	4	2,5	2	6,5	5	3	2,5	8,5	6	4	3
525	5,5	4	3	2	6,5	5	3,5	2,5	8,5	6	4,5	3
625	6	4	3	2	7	5	3,5	2,5	9	6	4,5	3
750	6,5	4,5	3	2	7,5	5,5	3,5	2,5	10	7	4,5	3
875	6,5	4,5	3,5	2,5	7,5	5,5	4,5	3	10	7	5,5	4
1025	7	5	3,5	2,5	8,5	6	4,5	3	10,5	7,5	5,5	4
1175	7,5	5,5	3,5	2,5	9	6,5	4,5	3	11,5	8,5	5,5	4
1363	7,5	5,5	4	3	9	6,5	5	3,5	11,5	8,5	6	4,5
2025	8	5,5	4	3	9,5	6,5	5	3,5	12	8,5	6	4,5
2350	8,5	6	4	3	10	7	5	3,5	13	9	6	4,5
2675	8,5	6	4,5	3	10	7	5,5	3,5	13	9	7	4,5
3063	9	6,5	4,5	3	10,5	7,5	5,5	3,5	13,5	10	7	4,5
3450	9,5	6,5	4,5	3	11	7,5	5,5	3,5	14,5	10	7	4,5
3900	9,5	6,5	5	3,5	11	7,5	6	4,5	14,5	10	7,5	5,5
4350	10	7	5	3,5	11,5	8,5	6	4,5	15	10,5	7,5	5,5
4900	10,5	7,5	5	3,5	12,5	9	6	4,5	16	11,5	7,5	5,5
5450	10,5	7,5	5,5	4	12,5	9	6,5	5	16	11,5	8,5	6
6125	11	7,5	5,5	4	13	9	6,5	5	16,5	11,5	8,5	6
6800	11,5	8	5,5	4	13,5	9,5	6,5	5	17,5	12	8,5	6
7225	11,5	8	6	4	13,5	9,5	7	5	17,5	12	9	6
7650	12	8,5	6	4	14	10	7	5	18	13	9	6
8075	12,5	9	6	4	14,5	10,5	7	5	19	13,5	9	6
8500	12,5	9	6,5	4,5	14,5	10,5	7,5	5,5	19	13,5	10	7
9600	13	9	6,5	4,5	15	10,5	7,5	5,5	19,5	13,5	10	7
10700	13,5	9,5	6,5	4,5	16	11	7,5	5,5	20,5	14,5	10	7

*FTE = *Full Time Equivalent*