ESQUEMA DE CERTIFICAÇÃO QNRCS

LISTA DE REFERÊNCIAS LEGAIS, NORMATIVAS E REGULAMENTARES

Legislação nacional	Enquadramento
Lei n.º 46/2018, de 13 de agosto	A Lei n.º 46/2018, de 13 de agosto, estabelece o Regime Jurídico da Segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União e estabelece assim o Regime Jurídico da Segurança do Ciberespaço. Este normativo define a orgânica do Conselho Superior de Segurança do Ciberespaço do Estado Português, assim como atribui competências e responsabilidades ao CNCS, na qualidade de Autoridade Nacional de Cibersegurança e ao CERT.PT, a Equipa de Resposta a Incidentes de Segurança Informática Nacional. Esta Lei determina ainda os requisitos de segurança e de notificação de incidentes, para operadores de serviços essenciais identificados, prestadores de serviços digitais, operadores de infraestruturas críticas, e Administração Pública. É ainda definido o quadro de fiscalização e sancionatório relativo ao Regime Jurídico da Segurança do Ciberespaço, cuja aplicação é da responsabilidade do CNCS.
Decreto-Lei n.º 65/2021, de 30 de julho	Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019. Este normativo define de forma transversal as obrigações relativas a requisitos de segurança e notificação de incidentes. Determina também as competências do CNCS como ANCC – Autoridade Nacional de Certificação em Cibersegurança e estabelece um regime sancionatório para a matéria da certificação.
Regulamento n.º 183/2021, de 21 de fevereiro	Regulamento que configura instrução técnica relativa à comunicação e informação para cumprimento das obrigações decorrentes do Regime Jurídico da Segurança do Ciberespaço referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes.

Legislação da União Europeia	Enquadramento
Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União	Esta Diretiva estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de melhorar o funcionamento do mercado interno.
Regulamento de Execução (UE) 2018/151, da Comissão, de 30 de janeiro de 2018	Estabelece normas de execução da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho no respeitante à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação, bem como à especificação pormenorizada dos parâmetros para determinar se o impacto de um incidente é substancial.
Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019	Este Regulamento é relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n. 526/2013 (Regulamento Cibersegurança). Estabelece o enquadramento europeu para a certificação da cibersegurança, os procedimentos para criação de esquemas europeus de certificação da cibersegurança e determina os elementos a constar em tais esquemas.

Normas Técnicas	Enquadramento
ISO/IEC 27001	A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados, de acordo com as necessidades e realidade da organização.
ISO/IEC 17065	A norma ISO/IEC 17065 especifica os requisitos que se destinam a assegurar que os organismos de certificação gerem os processos de certificação de forma competente, consistente e imparcial, facilitando o reconhecimento desses mesmos organismos. Esta norma pode ser utilizada como documento de critérios para acreditação, avaliação e indicação de organismos por autoridades governamentais, proprietários de esquemas e outros.
DNP TS 4577-1	O Documento Normativo Português – Especificação Técnica DNP TS 4577-1, Maturidade digital – Selo digital – Cibersegurança, especifica os requisitos técnicos a ser implementados em todos os locais e processos da organização onde há recurso a tecnologias de informação e comunicação com principal objetivo de mitigar muitos dos riscos físicos e digitais a que as organizações estão expostas, contribuindo para o aumento da segurança da informação e proteção das empresas. Contém o esquema de certificação correspondente.

Referenciais e ferramentas de suporte ou inspiração ao Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança	Enquadramento
Quadro Nacional de Referência para a Cibersegurança	Conjunto das melhores práticas para a Cibersegurança que permite às organizações reduzir o risco associado às ciberameaças, disponibilizando as bases para que qualquer entidade possa, de uma forma voluntária, cumprir os requisitos mínimos de segurança das redes e sistemas de informação. Designadamente, nas componentes de identificação, proteção, deteção, resposta e recuperação de ciberincidentes, incluindo a organização necessária para a sua gestão.
Quadro de Avaliação de Capacidades de Cibersegurança	Documento complementar ao Quadro Nacional de Referência para a Cibersegurança (QNRCS). Apresenta, para cada uma das medidas de cibersegurança do QNRCS, a definição de três níveis de capacidade, para que seja possível às organizações o autodiagnóstico da sua conformidade face aos requisitos do QNRCS e o cumprimento dos cinco objetivos do quadro, tendo em conta o seu contexto e dimensão.
Roteiro para as Capacidades Mínimas de Cibersegurança	Modelo de capacitação em cibersegurança, visando a melhoria de processos, pessoas e tecnologias nas organizações nacionais, com enfoque especial em PME (Pequenas e Médias Empresas), apoiando-a na vertente da cibersegurança nos seus processos de transição digital. O Roteiro para as Capacidades Mínimas em Cibersegurança, apresenta um conjunto de ações que se dividem em cinco fases, sendo que estas foram pensadas para uma adaptação gradual, a implementar em cada organização, quer seja por meios próprios internos, ou mesmo recorrendo a subcontratação ou externalização de soluções.
Guia para a Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança	Metodologia de gestão dos riscos que pretende servir de base orientadora para o cumprimento do artigo 10.º do Decreto-Lei n.º 65/2021, de 30 de julho e que tem como objetivo definir uma abordagem de referência sistematizada e coerente ao processo de análise, avaliação e tratamento periódico dos riscos e de aferição da forma como estes se relacionam no âmbito da prestação de um bem ou serviço.

Referenciais de suporte ao Quadro Nacional de Referência para a Cibersegurança	Enquadramento
NIST SP-800-53 Rev4	Publicado pela NIST9, é um catálogo de controlos de segurança e de privacidade para redes e sistemas de informação de organismos do governo. Disponibiliza, também, um processo de seleção de controlos para proteção da operação e dos ativos das organizações, de incidentes, desastres naturais, falhas estruturais ou erro humano.
COBIT 5	Da responsabilidade do ISACA, o COBIT é um referencial de boas práticas para a governação das TIC. Ajuda as organizações a criar valor a partir das TIC e contribui para o equilíbrio entre os benefícios, a otimização dos níveis do risco e a utilização dos recursos disponíveis pelas organizações.
CIS CSC 7.0	O Catálogo de controlos críticos de cibersegurança (CSC) é publicado pelo *Center for Internet* Security (CIS). Este catálogo disponibiliza uma lista de ações, priorizada, que é regularmente revista pela comunidade académica, de forma a ser utilizável pelas organizações.

Esquemas Europeus de Certificação da Cibersegurança	
EUCC - Common Criteria Scheme	Esquema de certificação de cibersegurança de produtos de TIC, com base nos *Common Criteria,* na *Common Methodology for Information Technology Security Evaluation* e nos padrões correspondentes, ISO/IEC 15408 e ISO/ IEC 18045, respetivamente.
EUCS – Cloud Services Scheme	Esquema candidato de certificação da cibersegurança de serviços de computação na nuvem. Suportado por três níveis de segurança, "básico", "substancial" e "elevado". Os requisitos de segurança aumentam de nível nas diversas dimensões: âmbito, rigor e profundidade.