EUROPEAN UNION AGENCY
FOR CYBERSECURITY

QUADRO DE AVALIAÇÃO DAS CAPACIDADES NACIONAIS

DEZEMBRO DE 2020

ACERCA DA ENISA

A Agência da União Europeia para a Cibersegurança, ENISA, é a agência da União dedicada à obtenção de um elevado nível comum de cibersegurança na Europa. Estabelecida em 2004 e reforçada pelo Regulamento Cibersegurança da UE, a Agência da União Europeia para a Cibersegurança contribui para a ciberpolítica da UE, reforça a fiabilidade dos produtos, serviços e processos de TIC com sistemas de certificação da cibersegurança, coopera com os Estados-Membros e os organismos da UE e ajuda a Europa a preparar-se para os desafios cibernéticos do futuro. Através da partilha de conhecimentos, do reforço das capacidades e da sensibilização, a Agência trabalha em colaboração com as suas principais partes interessadas para reforçar a confiança na economia conectada, aumentar a resiliência das infraestruturas da União e, em última análise, manter a segurança digital da sociedade e dos cidadãos europeus. Para mais informações, consultar www.enisa.europa.eu.

CONTACTO

Para contactar os autores utilize team@enisa.europa.eu.
Para perguntas dos meios de comunicação social sobre o presente documento, utilize press@enisa.europa.eu.

AUTORES

Anna Sarri, Pinelopi Kyranoudi – Agência da União Europeia para a Cibersegurança (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

AGRADECIMENTOS

A ENISA gostaria de apresentar o seu reconhecimento e agradecer a todos os peritos que participaram e deram um contributo valioso para o presente relatório e, em especial, os seguintes, por ordem alfabética (em inglês):

Gabinete Central do Estado para o Desenvolvimento da Sociedade Digital (Croácia), Marin Ante Pivcevic

Centro de Cibersegurança (Bélgica)

CFCS – Center for Cybersikkerhed (Dinamarca), Thomas Wulff

Centro Europeu de Cibercriminalidade – EC3, Alzofra Martinez Alvaro

Centro Europeu da Cibercriminalidade – EC3, Adrian-Ionut Bobeica

Ministério Federal do Interior (Alemanha), Sascha-Alexander Lettgen

Administração da Segurança da Informação (República da Eslovénia), Marjan Kavčič

Governo italiano (Itália)

Agência das Tecnologias da Informação de Malta (Malta), Katia Bonello e Martin Camilleri

Ministério da Justiça e da Segurança Pública (Noruega), Robin Bakke

Ministério da Política Digital (Grécia), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali e Sotiris Vasilos

Ministério dos Assuntos Económicos e das Comunicações (Estónia), Anna-Liisa Pärnalaas

Agência Nacional de Cibersegurança e Segurança da Informação (República Checa), Veronika Netolická

Autoridade Nacional de Segurança (Eslováquia)

Departamento de Segurança Nacional (Espanha), Maria Mar Lopez Gil

NCTV, Ministério da Justiça e da Segurança (Países Baixos)

Centro Nacional de Cibersegurança (Portugal), Alexandre Leite e Pedro Matos

Unidade de Política de Cibersegurança, Departamento do Ambiente, Clima e Comunicações (Irlanda), James Caffrey

Universidade de Oxford – Global Cyber Security Capacity Centre, Carolin Weisser Harris

A ENISA gostaria igualmente de agradecer a valiosa contribuição para este estudo dos peritos que preferem manter o anonimato.

ADVERTÊNCIA JURÍDICA

Deve ter-se em conta que esta publicação representa as opiniões e as interpretações da ENISA, salvo indicação em contrário. A presente publicação não deve ser interpretada como uma ação judicial da ENISA ou dos organismos da ENISA, salvo se adotada nos termos do Regulamento (UE) n.º 2019/881.
A presente publicação não representa necessariamente o estado da técnica, podendo ser atualizada ocasionalmente pela ENISA.

As fontes da parte de terceiros são citadas consoante apropriado. A ENISA não é responsável pelo conteúdo de fontes externas, incluindo sítios Web externos referenciados na presente publicação.

A presente publicação tem fins exclusivamente informativos e deve estar acessível gratuitamente. Nem a ENISA, nem qualquer pessoa atuando em seu nome é responsável pela utilização que possa ser dada à informação constante da presente publicação.

DECLARAÇÃO DE DIREITOS DE AUTOR

ISBN: 978-92-9204-493-0

DOI: 10.2824/88591

CATÁLOGO: TP-02-21-253-PT-N

1. ÍNDICE

GLOSSÁRIO DE TERMOS

ACRÓNIMO	DEFINIÇÃO
ALN	Agentes de ligação nacionais
ARCC	Acordo de Reconhecimento dos Critérios Comuns
C2M2	Modelo de Maturidade da Capacitação de Cibersegurança
CCSMM	Modelo Comunitário de Maturidade em matéria de Cibersegurança
CMM	Modelo de Maturidade da Capacitação de Cibersegurança para as Nações
CMMC	Certificação do Modelo de Maturidade da Cibersegurança
CPI	Índice de Ciberpotência
CSIRT	Equipas de resposta a incidentes de segurança informática
DCV	Divulgação coordenada de vulnerabilidades
DPA	Lei da proteção de dados
ECSO	Organização Europeia para Cibersegurança
EFTA	Associação Europeia de Comércio Livre
EM	Estado-Membro
ENC	Estratégias nacionais de cibersegurança
GDS	Serviço Digital Governamental
GECC	Grupo europeu para a certificação da cibersegurança
I&D	Investigação e Desenvolvimento
IA	Inteligência Artificial
IA-CM	Modelo de Capacidade de Auditoria Interna para o Setor Público
ICI	Infraestruturas Críticas da Informação
IGC	Índice Global de Cibersegurança
ISMM	Modelo de maturidade da segurança da informação para o Quadro de cibersegurança do Instituto Nacional de Normas e Tecnologia (NIST)
MEC	Mês Europeu da Cibersegurança
MUD	Mercado Único Digital
NIS	Segurança das redes e da informação
NIST	Instituto Nacional de Normas e Tecnologia
OSE	Operadores de serviços essenciais

PET	Tecnologias de reforço da proteção da privacidade
PIMS	Sistema de gestão da informação em matéria de privacidade
PME	Pequenas e médias empresas
PPP	Parcerias público-privadas
Q-C2M2	Modelo de Maturidade da Capacitação de Cibersegurança Qatar
QEQ	Quadro Europeu de Qualificações
RGPD	Regulamento Geral sobre a Proteção de Dados
SAL	Serviço responsável pela aplicação da lei
SOG-IS MRA	Grupo de Altos Funcionários para a segurança dos sistemas informáticos, Acordo de Reconhecimento Mútuo
TIC	Tecnologias da Informação e da Comunicação
TO	Tecnologia operacional
UE	União Europeia
UIT	União Internacional das Telecomunicações

RESUMO

À medida que o atual cenário de ciberameaças continua a expandir-se e que os ciberataques continuam a aumentar em termos de intensidade e de número, os Estados-Membros da UE têm de dar uma resposta eficaz, continuando a desenvolver e a adaptar as suas estratégias nacionais de cibersegurança (ENC). Desde a publicação dos primeiros estudos relativos às ENC pela ENISA, em 2012, os Estados-Membros da UE e os países da EFTA realizaram grandes progressos no desenvolvimento e na implementação das suas estratégias.

O presente relatório apresenta o trabalho realizado pela ENISA para criar um quadro de avaliação das capacidades nacionais (QACN).

O quadro visa proporcionar aos Estados-Membros uma autoavaliação do seu nível de maturidade através da avaliação dos objetivos da sua ENC, que os ajudará a reforçar e a desenvolver capacidades em matéria de cibersegurança, tanto a nível estratégico como operacional.

Apresenta uma visão simples representativa do nível de maturidade do Estado-Membro em matéria de cibersegurança. O QACN é um instrumento que ajuda os Estados-Membros a:

- Prestar informações úteis para desenvolver uma estratégia de longo prazo (por exemplo, boas práticas, orientações);
- Ajudar a identificar elementos em falta na ENC;
- Ajudar a continuar a criar capacidades de cibersegurança;
- Apoiar a responsabilidade das ações políticas;
- Conferir credibilidade perante o público em geral e os parceiros internacionais;
- Apoiar a divulgação e melhorar a imagem pública enquanto organização transparente;
- Ajudar a antecipar as questões que se perfilam no horizonte;
- Ajudar a identificar ensinamentos retirados e boas práticas;
- Fornecer uma base de referência sobre a capacidade de cibersegurança em toda a UE para facilitar os debates; e
- Ajudar a avaliar as capacidades nacionais no tocante à cibersegurança.

O presente quadro foi criado com o apoio de peritos na matéria da ENISA e representantes de 19 Estados-Membros e de países da EFTA[1]. O público-alvo do presente relatório são decisores políticos, peritos e funcionários do governo que sejam responsáveis ou estejam envolvidos na

[1] Foram entrevistados representantes dos seguintes Estados-Membros e países da EFTA: Alemanha, Bélgica, Chéquia, Croácia, Dinamarca, Eslováquia, Eslovénia, Espanha, Estónia, Grécia, Hungria, Irlanda, Itália, Listenstaine, Malta, Noruega, Países Baixos, Portugal, Suécia.

conceção, aplicação e avaliação de uma ENC e, a um nível mais alargado, de capacidades em matéria de cibersegurança.

O Quadro de Avaliação das Capacidades Nacionais abrange 17 objetivos estratégicos e está estruturado em torno de quatro grupos principais:

- Grupo #1: Governação e normas de cibersegurança
  1. Desenvolver um plano de contingência cibernética nacional
  2. Estabelecer medidas de segurança de base
  3. Proteger a identidade digital e criar confiança nos serviços públicos digitais

- Grupo #2: Criação de capacidades e sensibilização
  4. Organizar exercícios de cibersegurança
  5. Estabelecer uma capacidade de resposta a incidentes
  6. Aumentar a sensibilização dos utilizadores
  7. Reforçar os programas de formação e educativos
  8. Promover a I&D
  9. Proporcionar incentivos para o setor privado investir em medidas de segurança
  10. Melhorar a cibersegurança da cadeia de abastecimento

- Grupo #3: Aspetos jurídicos e regulamentares
  11. Proteger infraestruturas críticas da informação, OSE e prestadores de serviços digitais (PSD)
  12. Combater a cibercriminalidade
  13. Criar mecanismos de comunicação de incidentes
  14. Reforçar a privacidade e a proteção de dados

- Grupo #4: Cooperação
  15. Estabelecer uma parceria público-privada
  16. Institucionalizar cooperação entre agências públicas
  17. Colaborar na cooperação internacional

1. INTRODUÇÃO

A Diretiva relativa à Segurança das Redes e da Informação (SRI), publicada em julho de 2016, obriga os Estados-Membros a adotarem uma estratégia nacional em matéria de segurança das redes e dos sistemas de informação, também referida como uma ENC (estratégia nacional de cibersegurança), conforme estabelecido nos artigos 1.º e 7.º. Neste contexto, uma ENC é definida como um quadro que estabelece princípios estratégicos, orientações, objetivos estratégicos, prioridades, políticas e medidas regulamentares adequadas. O objetivo previsto de uma ENC é alcançar e manter um elevado nível de segurança da rede e dos sistemas, permitindo, assim, aos Estados-Membros mitigarem potenciais ameaças. Além disso, as ENC podem também ser um catalisador para o desenvolvimento industrial e o progresso económico e social.

O Regulamento Cibersegurança da UE indica que a ENISA deverá promover a divulgação de boas práticas na definição e aplicação de uma ENC apoiando os Estados-Membros na adoção da Diretiva SRI e recolhendo reações valiosas sobre as suas experiências. Para o efeito, a ENISA desenvolveu vários instrumentos para prestar assistência aos Estados-Membros no desenvolvimento, na aplicação e na avaliação das suas estratégias nacionais de cibersegurança (ENC).

Enquanto parte do seu mandato, a ENISA pretende desenvolver um quadro de autoavaliação das capacidades nacionais a fim de aferir o nível de maturidade das diferentes ENC. O objetivo do presente relatório é apresentar o estudo realizado na definição do quadro de autoavaliação.

1.1 ÂMBITO DE APLICAÇÃO E OBJETIVOS DO ESTUDO

O objetivo principal do presente estudo é criar um quadro de autoavaliação das capacidades nacionais, adiante designado QACN, a fim de aferir o nível de maturidade das capacidades em matéria de cibersegurança dos Estados-Membros. Mais concretamente, o quadro deverá cometer poderes aos Estados-Membros em matéria de:

- Realização da avaliação das suas capacidades nacionais em matéria de cibersegurança;
- Reforço do conhecimento do nível de maturidade do país;
- Identificação de áreas para melhoria; e
- Criação de capacidades em matéria de cibersegurança.

O presente quadro deverá ajudar os Estados-Membros, e em especial os decisores políticos nacionais, a realizarem um exercício de autoavaliação com vista a melhorar as capacidades nacionais em matéria de cibersegurança.

1.2 ABORDAGEM METODOLÓGICA

A abordagem metodológica usada para desenvolver o quadro de autoavaliação das capacidades nacionais assenta em quatro etapas principais:

1. **Investigação documental**: A primeira etapa envolveu a realização de uma análise extensiva da literatura para recolher boas práticas no que diz respeito ao desenvolvimento de um quadro de avaliação da maturidade para as estratégias nacionais de cibersegurança. A investigação documental incidiu sobre uma análise sistemática de documentos pertinentes sobre criação de capacidades e definição de estratégias em matéria de cibersegurança, as ENC dos Estados-Membros e uma

comparação dos modelos de maturidade existentes em matéria de cibersegurança. Realizou-se um exercício comparativo sobre os modelos de maturidade existentes através da adoção de um quadro de análise desenvolvido para efeitos do presente estudo. O quadro de análise tem por base a metodologia de Becker[2] para a elaboração de modelos de maturidade que define um modelo de processo genérico e consolidado para a conceção de modelos de maturidade e prevê requisitos claros para a elaboração de modelos de maturidade. O quadro de análise foi posteriormente adaptado para satisfazer as necessidades do presente estudo.

2. **Recolha de pontos de vista de peritos e partes interessadas**: Com base nos dados recolhidos através da investigação documental e nas conclusões preliminares conexas da análise, esta etapa envolveu identificar e convidar peritos identificados com experiência no desenvolvimento e na aplicação de uma ENC ou de modelos de maturidade para entrevistar. A ENISA contactou o seu Grupo de Peritos sobre Estratégias Nacionais em matéria de Cibersegurança e Agentes de Ligação Nacionais (ALN) para encontrar os peritos relevantes em cada Estado-Membro. Ademais, foram entrevistados alguns peritos envolvidos na elaboração de modelos de maturidade. Globalmente, foram realizadas 22 entrevistas, 19 das quais realizadas com representantes de agências de cibersegurança nos diferentes Estados-Membros (e países EFTA).
3. **Análise dos contributos do inventário:** Os dados recolhidos através da investigação documental e das entrevistas foram subsequentemente analisados para identificar boas práticas na conceção de um quadro de autoavaliação para aferir a maturidade das ENC, para compreender as necessidades dos Estados-Membros e para determinar que dados podem de modo viável ser recolhidos nos diferentes países europeus[3]. A análise permitiu aperfeiçoar o modelo preliminar elaborado nas etapas anteriores e refinar o conjunto de indicadores incluídos no modelo, os níveis de maturidade e as suas dimensões.
4. **Conclusão do modelo:** Subsequentemente, peritos na matéria da ENISA reviram uma versão atualizada do quadro de autoavaliação das capacidades nacionais, a qual foi depois validada por peritos através de um seminário realizado em outubro de 2020 antes da publicação.

1.3 PÚBLICO-ALVO

O público-alvo do presente relatório são decisores políticos, peritos e funcionários do governo que sejam responsáveis ou estejam envolvidos na conceção, aplicação e avaliação da ENC e, a um nível mais alargado, de capacidades em matéria de cibersegurança. Adicionalmente, as conclusões formalizadas no presente documento podem ser úteis para peritos e investigadores em política de cibersegurança a nível nacional ou europeu.

[2] J. Becker, R. Knackstedt eJ. Pöppelbuß, «Developing Maturity Models for IT Management: A Procedure Model and its Application,» Business & Information Systems Engineering, vol. 1, n.º 3, p. 213–222, junho de 2009.
[3] Para efeitos desta investigação, os «países europeus» referidos no presente relatório incluem os 27 Estados-Membros da UE.

2. CONTEXTO

2.1 TRABALHO ANTERIOR SOBRE O CICLO DE VIDA DAS ENC

Conforme referido no Regulamento Cibersegurança da UE, um dos principais objetivos da ENISA é apoiar os Estados-Membros na elaboração de estratégias nacionais de segurança das redes e dos sistemas de informação, promover a divulgação dessas estratégias e acompanhar a sua aplicação. Enquanto parte deste mandato, a ENISA elaborou diversos documentos sobre esta matéria com o intuito de promover a partilha de boas práticas e apoiar a aplicação das ENC em toda a UE:

- O «Practical guide on the development and execution phase of NCSS» (Guia Prático sobre a elaboração e a fase de execução da ENC)[4] publicado em 2012.
- O «Setting the course for national efforts to strengthen security in cyberspace» (Traçar o rumo para reforçar a segurança no ciberespaço)[5] publicado em 2012.
- O primeiro quadro da ENISA para avaliar a ENC de um Estado-Membro, publicado[6] em 2014.
- O «Online NCSS Interactive Map» (Mapa Interativo de ENC em Linha)[7] publicado em 2014.
- O «NCSS Good Practice Guide» (Guia de Boas Práticas em matéria de ENC)[8] publicado em 2016.
- A «National Cybersecurity Strategies Evaluation Tool» (Ferramenta de Avaliação das Estratégias Nacionais de Cibersegurança)[9] publicada em 2018.
- O «Good practices in innovation on Cybersecurity under the NCSS» (Boas práticas em inovação em matéria de cibersegurança no âmbito da ENC»[10] publicado em 2019.

O ANEXO A proporciona um resumo sucinto das principais publicações da ENISA sobre este tópico.

Os guias e documentos supracitados foram objeto de estudo enquanto parte da investigação documental. Em especial o «National Cybersecurity Strategies Evaluation Tool»[11] constitui um

[4] «NCSS: Practical Guide on Development and Execution» (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] «NCSS: Setting the course for national efforts to strengthen security in cyberspace» (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] «An evaluation framework for NCSS» (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] «National Cybersecurity Strategies - Interactive Map» (ENISA, 2014, atualizado em 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Este documento atualiza o guia de 2012: «NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies» (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] «National Cybersecurity Strategies Evaluation Tool» (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] «National Cybersecurity Strategies Evaluation Tool» (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

elemento fundamental do QACN. O QACN baseia-se nos objetivos abrangidos pela ferramenta de avaliação em linha da ENC.

2.2 OBJETIVOS COMUNS IDENTIFICADOS NAS ENC EUROPEIAS

A disparidade entre os diferentes Estados-Membros torna difícil identificar atividades ou planos de ação comuns entre os diferentes contextos, quadros jurídicos e agendas políticas nacionais. Contudo, as ENC dos Estados-Membros têm amiúde objetivos estratégicos articulados em torno dos mesmos tópicos. Por conseguinte, com base no trabalho anterior da ENISA e na análise das ENC dos Estados-Membros, foram identificados 22 objetivos estratégicos. No trabalho anterior da ENISA tinham já sido identificados 15 desses objetivos estratégicos, dois foram recentemente acrescentados ao presente estudo e cinco objetivos foram identificados para futuras considerações.

2.2.1 Objetivos estratégicos comuns abrangidos pelos Estados-Membros

Com base no trabalho anterior da ENISA, nomeadamente o «National Cybersecurity Strategies Evaluation Tool»[12], o quadro que se segue mostra o conjunto supracitado de 15 objetivos estratégicos que são comummente abrangidos pelas ENC dos Estados-Membros. Os objetivos traçam o núcleo da «filosofia nacional» geral sobre o tópico. Para informações adicionais sobre os objetivos descritos a seguir, consulte o relatório «NCSS Good Practice Guide» da ENISA[13].

Quadro 1: Objetivos estratégicos comuns abrangidos pelos Estados-Membros nas respetivas ENC

ID	Objetivos estratégicos da ENC	Objetivos
1	**Desenvolver planos nacionais de contingência cibernética**	▶ Apresentar e explicar os critérios que deverão ser usados para definir uma situação como crise; ▶ Definir os principais processos e ações para gerir a crise; ▶ Definir claramente as funções e responsabilidades de diferentes partes interessadas durante uma cibercrise; ▶ Apresentar e explicar os critérios para uma crise terminar e/ou quem tem autoridade para o declarar.
2	**Estabelecer medidas de segurança de base**	▶ Harmonizar as diferentes práticas seguidas pelas organizações no setor público e privado; ▶ Criar uma linguagem comum entre as autoridades públicas competentes e as organizações e abrir canais de comunicação seguros; ▶ Permitir que diferentes partes interessadas verifiquem e afiram as suas capacidades em matéria de cibersegurança; ▶ Partilhar informações sobre boas práticas em matéria de cibersegurança em cada setor da indústria; e ▶ Ajudar as partes interessadas a darem prioridade aos seus investimentos na segurança.
3	**Organizar exercícios de cibersegurança**	▶ Identificar aquilo que é necessário testar (planos e processos, pessoas, infraestruturas, capacidades de resposta, capacidades de cooperação, comunicação, etc.); ▶ Criar uma equipa nacional de planeamento de exercícios de cibersegurança, munida de um mandato claro; e

[12] «National Cybersecurity Strategies Evaluation Tool» (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Este documento atualiza o guia de 2012: «NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies» (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Objetivos estratégicos da ENC	Objetivos
		▶ Integrar exercícios de cibersegurança no ciclo de vida da estratégia nacional de cibersegurança ou no plano nacional de contingência cibernética.
4	Estabelecer uma capacidade de resposta a incidentes	▶ Por mandato, entende-se os poderes e as responsabilidades que são necessários atribuir a uma equipa pelo respetivo governo; ▶ Por carteira de serviços, entende-se os serviços que uma equipa presta à sua circunscrição ou que está a usar para o seu próprio funcionamento interno; ▶ Por capacidades operacionais, entende-se os requisitos técnicos e operacionais que uma equipa deve observar; e ▶ Por capacidades de cooperação, entende-se os requisitos relativos à partilha de informações com outras equipas não abrangidos pelas três categorias anteriores, por exemplo, decisores políticos, exército, reguladores, operadores (infraestruturas críticas da informação), autoridades de aplicação da lei.
5	Aumentar a sensibilização dos utilizadores	▶ Identificar lacunas no conhecimento relativo a aspetos de cibersegurança ou de segurança da informação; e ▶ Colmatar as lacunas mediante a sensibilização ou o desenvolvimento/reforço das bases de conhecimento.
6	Reforçar os programas de formação e educativos	▶ Melhorar as capacidades operacionais da mão-de-obra de segurança da informação existente; ▶ Incentivar os estudantes a aderir e depois prepará-los para entrarem no domínio da cibersegurança; ▶ Promover e encorajar as relações entre ambientes académicos de segurança da informação e a indústria da segurança da informação; e ▶ Alinhar a formação em cibersegurança com as necessidades das empresas.
7	Promover a I&D	▶ Identificar as verdadeiras causas das vulnerabilidades em vez de reparar o seu impacto; ▶ Juntar cientistas de diferentes disciplinas com vista a prestar soluções para os problemas multidimensionais e complexos como as ciberameaças físicas; ▶ Reunir as necessidades da indústria e as conclusões da investigação, facilitando, assim, a transição da teoria para a prática; e ▶ Encontrar formas não apenas de manter, mas também de aumentar, o nível de cibersegurança dos produtos e serviços que apoiam as ciberinfraestruturas existentes.
8	Proporcionar incentivos para o setor privado investir em medidas de segurança	▶ Identificar possíveis incentivos para as empresas privadas investirem em medidas de segurança; e ▶ Proporcionar incentivos às empresas para encorajar investimentos em segurança.
9	Proteger infraestruturas críticas da informação, OSE e PSD (ICI)	▶ Identificar infraestruturas crítica da informação; e ▶ Identificar e mitigar riscos relevantes para as ICI.
10	Combater a cibercriminalidade	▶ Criar leis no domínio da cibercriminalidade; e ▶ Aumentar a eficácia das agências de aplicação da lei.
11	Criar mecanismos de comunicação de incidentes	▶ Obter conhecimento sobre o ambiente global de ameaças; ▶ Avaliar o impacto de incidentes (por exemplo, violações da segurança, falhas da rede, interrupções de serviço); ▶ Obter conhecimento sobre vulnerabilidades e tipos de ataques novos e existentes; ▶ Atualizar medidas de segurança em conformidade; e ▶ Aplicar as disposições da Diretiva SRI em matéria de comunicação de incidentes.
12	Reforçar a privacidade e a proteção de dados	▶ Contribuir para o reforço dos direitos fundamentais em matéria de privacidade e proteção de dados.
13	Estabelecer uma parceria público-privada (PPP)	▶ Dissuasão (para dissuadir os atacantes); ▶ Proteger (recurso à investigação sobre novas ameaças à segurança);

ID	Objetivos estratégicos da ENC	Objetivos
		▶ Detetar (recurso à partilha de informações para combater novas ameaças); ▶ Responder (proporcionar as capacidades para fazer face ao impacto inicial de um incidente); e ▶ Recuperar (proporcionar as capacidades para reparar o impacto inicial de um incidente).
14	**Institucionalizar cooperação entre agências públicas**	▶ Aumentar a cooperação entre as agências públicas com responsabilidades e competências relacionadas com a cibersegurança; ▶ Evitar uma sobreposição de competências e de recursos entre agências públicas; e ▶ Melhorar e institucionalizar a cooperação entre agências públicas em diferentes domínios da cibersegurança.
15	**Colaborar na cooperação internacional (não apenas com EM da UE)**	▶ Beneficiar da criação de uma base de conhecimentos comum entre os Estados-Membros da UE; ▶ Criar efeitos de sinergia entre autoridades nacionais de cibersegurança; e ▶ Possibilitar e aumentar a luta contra a criminalidade transnacional.

2.2.2 Objetivos estratégicos adicionais

Com base na investigação documental levada a cabo e nas entrevistas realizadas pela ENISA, foram identificados objetivos estratégicos adicionais. Os Estados-Membros estão cada vez mais a abordar estes tópicos nas respetivas ENC ou a definir planos de ação sobre a mesma temática. São também facultados exemplos de atividades desenvolvidas pelos Estados-Membros. Caso um exemplo seja proveniente de uma fonte disponível publicamente, é fornecida uma referência. Nos casos em que os exemplos tenham por base entrevistas confidenciais com funcionários dos Estados-Membros da UE, não são fornecidas referências.

Foram identificados os seguintes objetivos estratégicos adicionais:

- Melhorar a cibersegurança da cadeia de abastecimento; e
- Proteger a identidade digital e criar confiança nos serviços públicos digitais.

Melhorar a cibersegurança da cadeia de abastecimento

As pequenas e médias empresas (PME) são a espinha dorsal da economia da Europa. Representam 99 % do total de empresas na UE[14] e, em 2015, estimava-se que as PME tinham criado cerca de 85 % de novos postos de trabalho e asseguravam dois terços do emprego total do setor privado na UE. Além disso, dado que as PME prestam serviços a grandes empresas e trabalham cada vez mais com as administrações públicas[15], cumpre salientar que no atual contexto interligado, as PME são o elo mais fraco para os ciberataques. Com efeito, as PME são as mais expostas a ciberataques, no entanto, frequentemente não dispõem de meios para investir adequadamente em cibersegurança[16]. A melhoria da cibersegurança da cadeia de abastecimento deverá, portanto, ser realizada com uma tónica nas PME.

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Além desta abordagem sistémica, os Estados-Membros podem também salientar esforços em matéria da cibersegurança de serviços e produtos TIC específicos considerados essenciais: As tecnologias TIC utilizadas em infraestruturas críticas da informação, mecanismos de segurança obrigatórios no setor das telecomunicações [controlos a nível dos fornecedores de serviços Internet (FSI)...], serviços de confiança conforme definidos no Regulamento eIDAS e prestadores de serviços de computação em nuvem. Por exemplo, na sua estratégia nacional para a cibersegurança 2019-2024[17], a Polónia comprometeu-se a desenvolver um sistema nacional de avaliação e certificação da cibersegurança enquanto um mecanismo para garantia de qualidade na cadeia de abastecimento. Este sistema de certificação será alinhado com o enquadramento europeu para a certificação para produtos, serviços e processos digitais criado pelo Regulamento Cibersegurança da UE (2019/881).

Por conseguinte, a melhoraria da cibersegurança da cadeia de abastecimento reveste-se da maior importância. Tal pode ser conseguido estabelecendo políticas sólidas para promover as PME, emitindo orientações relativas a requisitos de cibersegurança em processos de adjudicação de contratos da administração pública, promovendo a cooperação no setor privado, criando PPP, promovendo mecanismos de divulgação coordenada das vulnerabilidades (DCV)[18], criando um sistema de certificação de produtos, incluindo componentes de cibersegurança em iniciativas digitais para as PME e financiando o desenvolvimento de competências, entre outros.

Proteger a identidade digital e criar confiança nos serviços públicos digitais

Em fevereiro de 2020, a Comissão definiu a sua visão para a transformação digital da UE na comunicação intitulada «Construir o futuro digital da Europa»[19], com o objetivo de apresentar tecnologias inclusivas que funcionem para as pessoas e respeitem os valores fundamentais da UE. Em especial, a comunicação indica que é essencial promover a transformação digital das administrações públicas em toda a Europa. Nesse sentido, criar confiança no governo em relação à identidade digital e confiança nos serviços públicos reveste-se da maior importância. Tal é ainda mais crucial se se considerar o facto de que as transações e os intercâmbios de dados do setor público são amiúde de caráter sensível.

Muitos países manifestaram a sua intenção de abordar este tópico nas respetivas ENC, tais como: Dinamarca, Espanha, Estónia, França, Luxemburgo, Malta, Países Baixos e Reino Unido. Entre esses países, alguns manifestaram igualmente que este objetivo estratégico poderá ser abordado enquanto parte de um plano mais geral:

- A Estónia liga o seu plano de ação sobre «A segurança da identidade eletrónica e capacidade de autenticação eletrónica» à Agenda Digital 2020 mais geral para a Estónia.
- A ENC francesa indica que o secretário de Estado responsável pela Tecnologia Digital supervisiona a criação de um roteiro «para proteger as vidas digitais, a privacidade e os dados pessoais dos cidadãos franceses».
- A ENC dos Países Baixos indica que a cibersegurança nas administrações públicas, bem como os serviços públicos prestados aos cidadãos e às empresas são analisados mais detalhadamente na Agenda Alargada para a Administração Pública Digital.
- À medida que continua a transferir mais dos seus serviços em linha, o Governo do Reino Unido nomeou o Serviço Digital Governamental (SDG) para assegurar que todos os novos serviços digitais integrados ou obtidos pela administração pública são

[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Construir o futuro digital da Europa, COM(2020) 67 final:
https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

também «seguros por defeito», com o apoio do Centro Nacional de Cibersegurança Britânico (CNCS).

2.2.3 Outros objetivos estratégicos considerados

Durante a etapa de investigação documental e enquanto parte das entrevistas realizadas pela ENISA, foram estudados outros objetivos estratégicos. Contudo, foi decidido que esses objetivos não fariam parte do quadro de autoavaliação. ANEXO C – Outros objetivos estudados

fornece definições para cada um desses objetivos que podem ser usados para promover as discussões sobre eventuais melhorias da ENC.

Os objetivos estratégicos que se seguem foram estudados enquanto considerações futuras:

- Desenvolver estratégias de cibersegurança setoriais;
- Combater as campanhas de desinformação.
- Proteger tecnologias de ponta (5G, IA, computação quântica, etc.);
- Assegurar a soberania em matéria de dados; e
- Proporcionar incentivos para o desenvolvimento da indústria dos ciberseguros.

2.3 PRINCIPAIS CONCLUSÕES DO EXERCÍCIO COMPARATIVO

A investigação documental sobre os modelos de maturidade existentes relacionados com a cibersegurança foi levada a cabo com o intuito de recolher informações e elementos para apoiar a conceção do quadro de autoavaliação das capacidades nacionais no domínio da ENC. Neste contexto, procedeu-se a uma análise extensiva da literatura de modelos existentes para complementar as conclusões da investigação inicial de delimitação do âmbito sobre modelos de maturidade de cibersegurança e ENC existentes, desenvolvidas nas secções 2.1 e 2.2. Esta análise sistemática apoia a seleção e justificação dos níveis de maturidade do quadro de avaliação e a definição das diferentes dimensões e indicadores.

No âmbito da análise sistemática de modelos de maturidade, foram considerados e analisados dez modelos com base nas respetivas características principais. A panorâmica global das principais características para cada modelo analisado no âmbito deste estudo encontra-se disponível no Quadro 2: Panorâmica dos modelos de **maturidade** analisados e pode ser encontrada uma análise mais pormenorizada no ANEXO A.

Quadro 2: Panorâmica dos modelos de maturidade analisados

Designação do modelo	# de Níveis de maturidade	# de Atributos	Método de avaliação	Representação dos resultados
Modelo de Maturidade da Capacitação de Cibersegurança para as Nações (CMM)	5	5 dimensões principais	Colaboração com uma organização local para aperfeiçoar o modelo antes de o aplicar ao contexto nacional	Radar de 5 secções
Modelo de Maturidade da Capacitação de Cibersegurança (C2M2)	4	10 domínios principais	Metodologia de autoavaliação e conjunto de ferramentas	Tabela de resultados com gráficos circulares
Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas	n/a (4 Patamares)	5 funções principais	Autoavaliação	n/a

Designação do modelo	# de Níveis de maturidade	# de Atributos	Método de avaliação	Representação dos resultados
Modelo de Maturidade da Capacitação de Cibersegurança Catar (Q-C2M2)	5	5 domínios principais	n/a	n/a
Certificação do Modelo de Maturidade da Cibersegurança (CMMC)	5	17 domínios principais	Avaliação por auditores externos	n/a
O Modelo Comunitário de Maturidade em matéria de Cibersegurança (CCSMM)	5	6 dimensões principais	Avaliação dentro das comunidades com contributos de agências de aplicação da lei do Estado e federais	n/a
Modelo de maturidade da segurança da informação para o Quadro de cibersegurança do Instituto Nacional de Normas e Tecnologia (NIST) (ISMM)	5	23 domínios avaliados	n/a	n/a
Modelo de Capacidade de Auditoria Interna (IA-CM) para o Setor Público	5	6 elementos	Autoavaliação	n/a
O Índice Global de Cibersegurança (IGC)	N/A	5 pilares	Autoavaliação	Tabela de classificação
O Índice de Ciberpotência (CPI)	N/A	4 categorias	Avaliação comparativa pela *Economist Intelligence Unit*	Tabela de classificação

A análise sistemática possibilitou extrair conclusões sobre boas práticas adotadas nos modelos existentes, a fim de apoiar a elaboração do modelo conceptual para o modelo de maturidade atual. Em especial, o exercício comparativo apoiou a definição dos níveis de maturidade, a criação de grupos de dimensão e a seleção de indicadores, bem como uma metodologia de visualização apropriada para os resultados do modelo. As conclusões mais relevantes para cada um desses elementos encontram-se pormenorizadas no Quadro 3.

Quadro 3: Principais conclusões do exercício comparativo

Característica	Principal conclusão
Níveis de maturidade	▶ Uma escala de maturidade de cinco níveis para quadros de avaliação sobre as capacidades em matéria de cibersegurança é comummente aceite e está disponível para prestar resultados de avaliação granulares (ver Quadro 6 Comparação de Níveis de Maturidade para uma visão exaustiva da definição dos níveis de maturidade para cada modelo); ▶ Todos os modelos apresentam uma definição de alto nível de cada nível de maturidade que é depois adaptada às diferentes dimensões ou grupos de dimensões; ▶ Normalmente, são avaliados dois aspetos principais na aferição da maturidade das capacidades em matéria de cibersegurança: a maturidade das estratégias e a maturidade dos processos criados para implementar estratégias.
Atributos	▶ A análise comparativa dos atributos dos modelos de maturidade existentes revelam resultados heterogéneos com um número médio de atributos por modelo entre quatro e cinco; ▶ Um modelo assente em cerca de quatro ou cinco atributos proporciona aos países o nível certo de granularidade dos dados agrupando as dimensões relevantes e assegurando a legibilidade dos resultados (ver Quadro 7: Comparação de Atributos/Dimensões para uma descrição dos atributos para cada modelo); ▶ O princípio fundamental adotado por todos os modelos na definição dos grupos é baseado na consistência do elemento agrupado em cada grupo.
Método de avaliação	▶ Os métodos de avaliação usados nos diferentes modelos analisados variam entre si; ▶ O método de avaliação mais comum baseia-se na autoavaliação.
Representação dos resultados	▶ É importante apresentar os resultados com um nível diferente de granularidade; ▶ A metodologia de visualização deverá ser explícita e fácil de ler.

O modelo conceptual foi criado com base no exercício comparativo dos diferentes modelos de maturidade, bem como no trabalho anterior da ENISA. Ademais, decidiu-se ter por base a *ferramenta interativa em linha da ENISA* para desenvolver indicadores de maturidade usados para cada atributo.

2.4 DESAFIOS DA AVALIAÇÃO DA ENC

Os Estados-Membros são confrontados com diversos desafios na criação de capacidades em matéria de cibersegurança e, mais concretamente, quando se trata de assegurar que as suas capacidades estão atualizadas relativamente às evoluções mais recentes. Segue-se uma síntese dos desafios identificados pelos Estados-Membros e com eles debatidos enquanto parte deste estudo:

- **Dificuldades na coordenação e cooperação:** A coordenação dos esforços em matéria de cibersegurança a nível nacional com vista a dispor de uma resposta eficiente a problemas de cibersegurança é suscetível de constituir um desafio devido a um elevado número de partes interessadas envolvidas.
- **Insuficiência de recursos para realizar a avaliação:** Dependendo do contexto local e da estrutura nacional de governação da cibersegurança, a avaliação da ENC e dos respetivos objetivos pode demorar mais de 15 pessoas-dia.
- **Insuficiência de apoio para desenvolver capacidades em matéria de cibersegurança:** Alguns Estados-Membros afiançaram que para defender um orçamento e obter apoio para desenvolver capacidades em matéria de cibersegurança, primeiro tinham de realizar uma fase de avaliação para identificar lacunas e limitações.

- **Dificuldades na atribuição de sucessos ou mudanças à estratégia:** Dado que as ameaças evoluem todos os dias e a tecnologia melhora, os planos de ação necessitam de ser constantemente adaptados em resposta. Contudo, avaliar uma ENC e atribuir mudanças à estratégia continua a ser por si só uma tarefa laboriosa. Por sua vez, tal torna difícil a identificação de limitações e insuficiências da ENC.
- **Dificuldades para medir a eficácia da ENC:** Podem ser recolhidas métricas para medir diferentes domínios, tais como progresso, implementação, maturidade e eficácia. Embora medir o progresso e a implementação seja relativamente fácil em comparação com a medição da eficácia, esta última continua a ser mais significativa para avaliar os resultados e impactos de uma ENC. Com base nas entrevistas realizadas pela ENISA, um grande número de Estados-Membros afirmou que medir quantitativamente a eficácia de uma ENC é importante, mas também representa uma tarefa muito exigente que nalguns casos é praticamente impossível.
- **Dificuldade para adotar um quadro comum:** Os Estados-Membros da UE operam em diferentes contextos em termos de políticas, organizações, cultura, estrutura da sociedade e maturidade da ENC. Alguns Estados-Membros entrevistados no âmbito do presente estudo manifestaram que poderá revelar-se difícil defender e usar um quadro de autoavaliação de «modelo único».

2.5 BENEFÍCIOS DE UMA AVALIAÇÃO DAS CAPACIDADES NACIONAIS

Desde 2007, todos os Estados-Membros da UE dispõem de uma ENC[20]. Embora se trate de uma evolução positiva, é também importante que os Estados-Membros sejam capazes de avaliar adequadamente essas ENC, conferindo, desta forma, valor acrescentado ao seu planeamento estratégico e implementação.

Um dos objetivos do quadro de avaliação das capacidades nacionais é avaliar as capacidades em matéria de cibersegurança com base nas prioridades estabelecidas nas várias ENC. Fundamentalmente, o quadro avalia o nível de maturidade das capacidades em matéria de cibersegurança dos Estados-Membros nos domínios definidos pelos objetivos da ENC. Por conseguinte, os resultados do quadro apoiam os decisores políticos dos Estados-Membros na definição da estratégia nacional em matéria de cibersegurança fornecendo-lhes informações relativas ao país sobre o ponto da situação[21]. O QACN destina-se, em última instância, a ajudar os Estados-Membros a identificarem áreas para melhoria e criarem capacidades.

O quadro visa proporcionar aos Estados-Membros uma autoavaliação do seu nível de maturidade através da avaliação dos objetivos da respetiva ENC, que os ajudará a reforçar e a desenvolver capacidades em matéria de cibersegurança, tanto a nível estratégico como operacional.

Numa abordagem mais prática, com base nas entrevistas realizadas pela ENISA com várias agências responsáveis pelo domínio da cibersegurança em diferentes Estados-Membros, foram identificados e sublinhados os seguintes benefícios do quadro de avaliação das capacidades nacionais:

- Prestar informações úteis para desenvolver uma estratégia de longo prazo (por exemplo, boas práticas, orientações);
- Ajudar a identificar elementos em falta na ENC;
- Ajudar a continuar a criar capacidades de cibersegurança;

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). «The interface between evaluation and public policy. Evaluation, 5(4), 468-486.»

- Apoiar a responsabilidade das ações políticas;
- Conferir credibilidade perante o público em geral e os parceiros internacionais;
- Apoiar a divulgação e melhorar a imagem pública enquanto organização transparente;
- Ajudar a antecipar as questões que se perfilam no horizonte;
- Ajudar a identificar ensinamentos retirados e boas práticas;
- Fornecer uma base de referência sobre a capacidade de cibersegurança em toda a UE para facilitar os debates; e
- Ajudar a avaliar as capacidades nacionais no tocante à cibersegurança.

3. METODOLOGIA DO QUADRO DE AVALIAÇÃO DAS CAPACIDADES NACIONAIS

3.1 OBJETIVO GERAL

O **objetivo principal** do QACN é medir o nível de maturidade das capacidades em matéria de cibersegurança dos **Estados-Membros** para os apoiar na realização de uma avaliação da sua capacidade nacional em matéria de cibersegurança, reforçar a sensibilização para o nível de maturidade do país, identificar áreas para melhoria e criar capacidades em matéria de cibersegurança.

3.2 NÍVEIS DE MATURIDADE

O quadro baseia-se em **cinco níveis de maturidade** que definem as etapas pelas quais os Estados-Membros passam quando criam capacidades em matéria de cibersegurança no domínio abrangido por cada objetivo da ENC. Os níveis representam níveis crescentes de maturidade, começando no **Nível 1** inicial, no qual os Estados-Membros não têm uma abordagem claramente definida para a criação de capacidades em matéria de cibersegurança nos domínios abrangidos pelos objetivos da ENC e terminando no **Nível 5**, no qual a estratégia de criação de capacidades em matéria de cibersegurança é dinâmica e adaptativa às evoluções do ambiente. O Quadro 4 mostra a escala do nível de maturidade com uma descrição de cada nível de maturidade.

Quadro 4: A escala de maturidade de cinco níveis do Quadro de Avaliação das Capacidades Nacionais da ENISA

NÍVEL 1 - INICIAL/*AD HOC*	NÍVEL 2 - DEFINIÇÃO ANTECIPADA	NÍVEL 3 - ESTABELECIMENTO	NÍVEL 4- OTIMIZAÇÃO	NÍVEL 5 - ADAPTABILIDADE
O Estado-Membro não tem uma abordagem claramente definida para a criação de capacidades em matéria de cibersegurança nos domínios abrangidos pelos objetivos da ENC. Contudo, o país poderá ter alguns objetivos genéricos preparados e ter realizado alguns estudos (técnicos, políticos, linha de conduta) para melhorar as capacidades nacionais.	A abordagem nacional para a criação de capacidades no domínio abrangido pelos objetivos da ENC foi definida. Os planos de ação ou atividades para alcançar os resultados estão criados, mas numa fase incipiente. Além disso, poderão ter sido identificadas e/ou envolvidas partes interessadas ativas.	O plano de ação para a criação de capacidades no domínio abrangidos pelos objetivos da ENC está claramente definido e apoiado pelas partes interessadas relacionadas. As práticas e atividades são executadas e implementadas uniformemente a nível nacional. As atividades estão definidas e documentadas com uma clara afetação de recursos e governação e um conjunto de prazos.	O plano de ação é avaliado regularmente: é priorizado, otimizado e sustentável. O desempenho das atividades de criação de capacidades em matéria de cibersegurança é regularmente medido. Os fatores de sucesso, os desafios e as lacunas na implementação das atividades estão identificados.	A estratégia de criação de capacidades em matéria de cibersegurança é dinâmica e adaptativa. A atenção constante às evoluções do ambiente (avanços tecnológicos, conflito global, novas ameaças, etc.) promove uma capacidade de decisão rápida e uma aptidão para atuar rapidamente com vista à melhoria.

3.3 GRUPOS E ESTRUTURA ABRANGENTE DO QUADRO DE AUTOAVALIAÇÃO

O quadro de autoavaliação caracteriza-se por **quatro grupos**: (I) Governação e normas de cibersegurança, (II) Criação de capacidades e sensibilização, (III) Aspetos jurídicos e regulamentares e (IV) Cooperação. Cada um desses grupos abrange uma área temática principal para criar capacidades em matéria de cibersegurança num país e contém um conjunto de diferentes objetivos que os Estados-Membros podem incluir na sua ENC. Em especial:

- **(I) Governação e normas de cibersegurança**: este grupo mede a capacidade dos Estados-Membros de estabelecerem governação, normas e boas práticas adequadas no domínio da cibersegurança. Esta dimensão considera diferentes aspetos da ciberdefesa e resiliência ao mesmo tempo que apoia o desenvolvimento da indústria nacional de cibersegurança e cria confiança nas administrações públicas;
- **(II) Criação de capacidades e sensibilização**: este grupo avalia a capacidade dos Estados-Membros de melhorar a sensibilização para os riscos e as ameaças de cibersegurança e como resolvê-los. Além disso, esta dimensão avalia a capacidade do país de criar continuamente capacidades em matéria de cibersegurança e aumentar o nível global de conhecimento e competências neste domínio. Aborda o desenvolvimento do mercado da cibersegurança e os avanços na I&D em matéria de cibersegurança**.** Este grupo congrega todos os objetivos lançando as bases para promover a criação de capacidades;
- **(III) Aspetos jurídicos e regulamentares**: este grupo mede a capacidade dos Estados-Membros de criar os instrumentos jurídicos e regulamentares necessários para dar resposta e combater o aumento da cibercriminalidade e ciberincidentes conexos, bem como proteger infraestruturas críticas da informação. Ademais, esta dimensão avalia igualmente a capacidade dos Estados-Membros de criar um quadro jurídico para proteger os cidadãos e as empresas como, por exemplo, no caso do estabelecimento do equilíbrio entre a segurança e a privacidade; e
- **(IV) Cooperação:** este grupo avalia a cooperação e a partilha de informações entre diferentes grupos de partes interessadas a nível nacional e internacional enquanto um instrumento importante para compreender e responder melhor a um ambiente de ameaças em constante evolução.

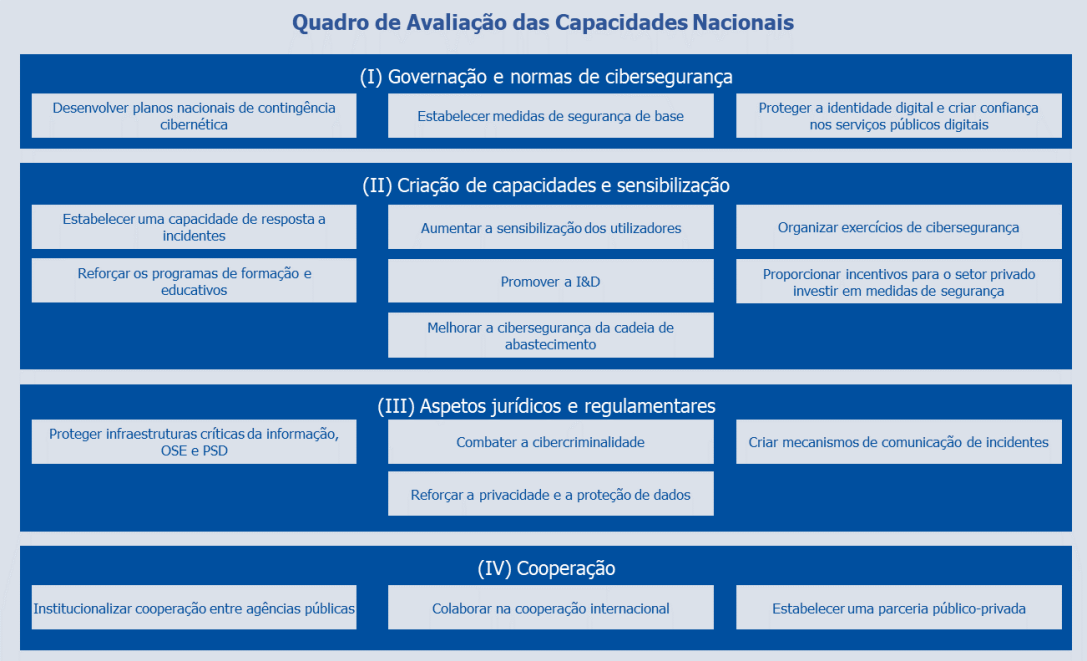
Os objetivos que foram incluídos no modelo são os comummente adotados pelos Estados-Membros e foram selecionados entre os objetivos elencados na secção 2.2. Em especial, o modelo avalia os seguintes objetivos:

- 1. Desenvolver planos nacionais de contingência cibernética (I)
- 2. Estabelecer medidas de segurança de base (I)
- 3. Proteger a identidade digital e criar confiança nos serviços públicos digitais (I)
- 4. Estabelecer uma capacidade de resposta a incidentes (II)
- 5. Aumentar a sensibilização dos utilizadores (II)
- 6. Organizar exercícios de cibersegurança (II)
- 7. Reforçar os programas de formação e educativos (II)
- 8. Promover a I&D (II)
- 9. Proporcionar incentivos para o setor privado investir em medidas de segurança (II)
- 10. Melhorar a cibersegurança da cadeia de abastecimento (II)
- 11. Proteger infraestruturas críticas da informação, OSE e PSD (III)
- 12. Combater a cibercriminalidade (III)
- 13. Criar mecanismos de comunicação de incidentes (III)
- 14. Reforçar a privacidade e a proteção de dados (III)
- 15. Institucionalizar cooperação entre agências públicas (IV)
- 16. Colaborar na cooperação internacional (IV)
- 17. Estabelecer uma parceria público-privada (IV)

Os quatro grupos e objetivos subjacentes são combinados no modelo para se ter uma perspetiva holística da maturidade das capacidades em matéria de cibersegurança dos

Estados-Membros. A Figura 1 apresenta a estrutura abrangente do quadro de autoavaliação e mostra de que modo esses elementos, nomeadamente objetivos, grupos e quadro de autoavaliação, estão ligados à avaliação do desempenho de um país.

Figura 1: Estrutura do quadro de autoavaliação



Para cada objetivo incluído no quadro de autoavaliação, há uma série de indicadores distribuídos pelos cinco níveis de maturidade. Cada indicador baseia-se numa pergunta dicotómica (sim/não). O indicador pode ser um requisito ou um não requisito.

3.4 MECANISMO DE PONTUAÇÃO

O **mecanismo de pontuação** do quadro de autoavaliação tem em conta os elementos supracitados e os princípios elencados na secção 3.5. Com efeito, o modelo fornece uma pontuação com base no valor de dois parâmetros, o **nível de maturidade** e o **rácio de cobertura**. Cada um desses parâmetros pode ser calculado em diferentes níveis: (i) por objetivo, (ii) por grupo de objetivos ou (iii) globalmente.

Pontuações ao nível do objetivo

A **pontuação do nível de maturidade** proporciona uma panorâmica do nível de maturidade mostrando que capacidades e práticas foram criadas. A pontuação do nível de maturidade é calculada como o nível mais elevado relativamente ao qual o inquirido satisfez todos os requisitos (ou seja, uma resposta SIM a todas as perguntas sobre requisitos), além de ter satisfeito todos os requisitos dos níveis precedentes de maturidade.

O **rácio de cobertura** mostra o grau de cobertura de todos os indicadores relativamente aos quais a resposta é positiva, independentemente do seu nível. Trata-se de um valor complementar que tem em conta todos os indicadores que medem um objetivo. O rácio de cobertura é calculado como a proporção entre o número total de perguntas no objetivo e o número de perguntas para as quais a resposta é positiva.

É importante esclarecer que no resto do documento o termo ***pontuação*** é usado para se referir aos valores do nível de maturidade e ao rácio de cobertura.

Figura 2 - O mecanismo de pontuação por objetivo proporciona uma visualização do mecanismo descrito na secção 3.1 que será desenvolvido mais aprofundadamente adiante.

Figura 2: Mecanismo de pontuação por objetivo

A Figura 2 mostra um exemplo de que como o nível de maturidade é calculado por objetivo. Cumpre salientar que o inquirido satisfez todos os requisitos dos primeiros três níveis de maturidade e satisfez apenas parcialmente os do Nível 4. Por conseguinte, a pontuação indica que o ***nível de maturidade do inquirido corresponde ao Nível 3*** *para o objetivo «****Organizar exercício de cibersegurança****».*

Contudo, no exemplo apresentado na Figura 2, o nível de maturidade do objetivo não consegue captar a informação fornecida pelos indicadores que têm uma pontuação positiva e que estão acima do Nível 3 de maturidade. Nesse caso, o rácio de cobertura pode fornecer uma panorâmica de todos os elementos que o inquirido implementou para alcançar esse objetivo, apesar do seu nível real de maturidade. Neste caso, a proporção entre o número total de perguntas no objetivo e o número de perguntas para as quais a resposta é positiva é igual a 19/27, ou seja, ***o valor do rácio de cobertura é 70 %****.*

Adicionalmente, para se adaptar às especificidades dos Estados-Membros permitindo, simultaneamente, uma panorâmica consistente, a pontuação é calculada a partir de duas amostras diferentes a nível do grupo e a nível global:

- **Pontuações gerais:** uma amostra completa que cobre todos os objetivos incluídos no grupo ou no quadro geral (de um a 17);
- **Pontuações específicas:** uma amostra específica que cobre apenas os objetivos selecionados pelo Estado-Membro (normalmente, correspondendo aos objetivos presentes na ENC do país específico) no grupo ou no quadro geral.

Pontuações ao nível do grupo

O **nível geral de maturidade de cada grupo** é calculado como a média aritmética do nível de maturidade de todos os objetivos nesse grupo.

O **nível específico de maturidade de cada grupo** é calculado como a média aritmética do nível de maturidade dos objetivos nesse grupo que o Estado-Membro escolheu avaliar (normalmente, correspondendo aos objetivos presentes na ENC do país específico).

Por exemplo, a Figura 1 mostra que o grupo (I) Governação e normas de cibersegurança é composto por três objetivos. Assumindo que o inquirido escolhe avaliar apenas os primeiros dois objetivos, mas não o terceiro, e assumindo que os primeiros dois objetivos apresentam, respetivamente, um nível de maturidade de 2 e 4, então o nível de maturidade do grupo considerando todos os objetivos corresponde ao Nível 2 [Grupo (I) nível de maturidade genérico = (2+4)/3], ao passo que o nível de maturidade do grupo considerando apenas os objetivos específicos selecionados pelo avaliador corresponde ao Nível 3 [Grupo (I) nível de maturidade genérico = (2+4)/2].

O **rácio de cobertura geral de cada grupo** é calculado como a proporção entre o número total de perguntas no grupo e o número de perguntas para as quais a resposta é positiva.

O **rácio de cobertura específico de cada grupo** é calculado como a proporção entre o número total de perguntas no grupo pertencentes aos objetivos que o Estado-Membro escolhe avaliar (normalmente, correspondendo aos objetivos presentes na ENC do país específico) e o número de perguntas para as quais a resposta é positiva.

Pontuações a nível global

O **nível global de maturidade de um país** é calculado como a média aritmética do nível de maturidade de todos os objetivos nesse quadro, de um a 17.

O **nível específico de maturidade de um país** é calculado como a média aritmética do nível de maturidade dos objetivos no quadro que o Estado-Membro escolheu avaliar (normalmente, correspondendo aos objetivos presentes na ENC do país específico).

O **rácio de cobertura geral de um país** é calculado como a proporção entre o número total de perguntas em todos os objetivos incluídos no quadro (de um a 17) e o número de perguntas para as quais a resposta é positiva.

O **rácio de cobertura geral de um país** é calculado como a proporção entre o número total de perguntas dos objetivos do quadro que o Estado-Membro escolhe avaliar (normalmente, correspondendo aos objetivos presentes na ENC do país específico) e o número de perguntas para as quais a resposta é positiva.

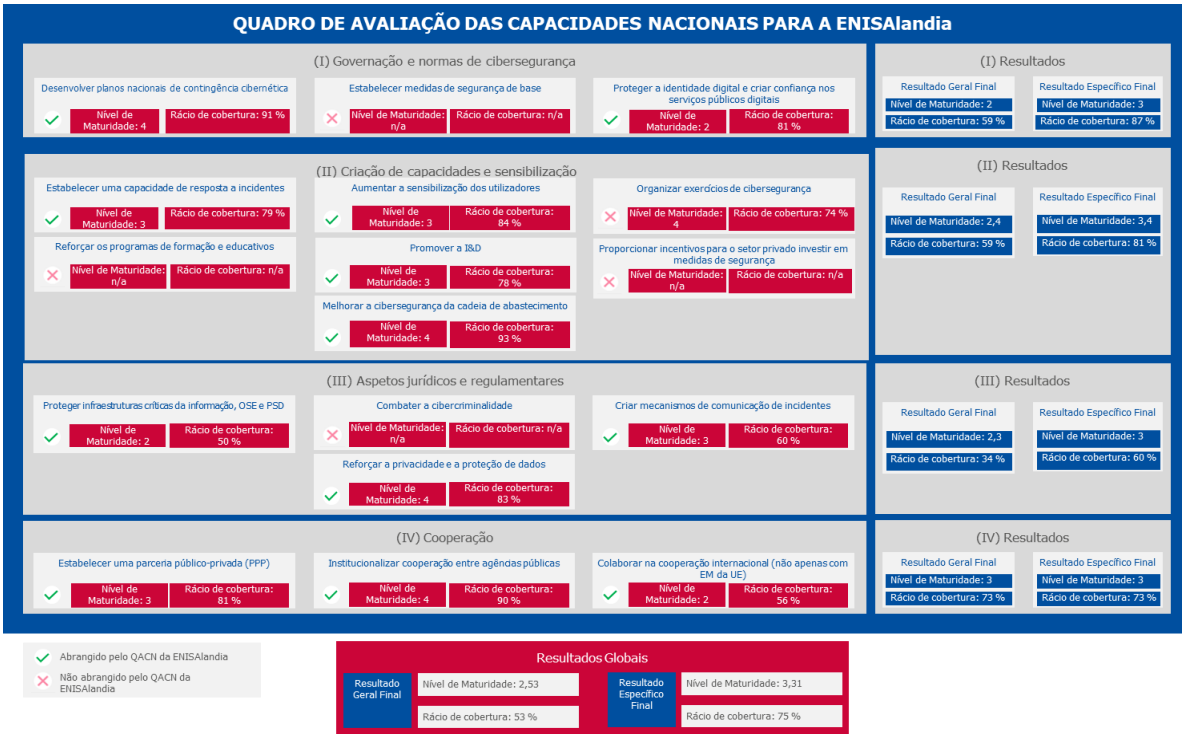
Para cada indicador, os inquiridos podem selecionar uma terceira opção «não sabe/não aplicável» para a sua resposta. Neste caso, o indicador é excluído do cálculo total dos resultados.

Os níveis de maturidade a nível do grupo e a nível geral são calculados com uma média aritmética para mostrar os progressos entre duas avaliações. Com efeito, a alternativa que consiste em calcular os níveis de maturidade do grupo e gerais como o nível de maturidade do objetivo menos maduro - embora relevante de uma perspetiva de maturidade - não pode contabilizar os progressos registados em domínios abrangidos por outros objetivos.

Dado que o nível de grupo e o nível geral são consolidados para efeitos de apresentação de relatórios, optou-se por usar a média aritmética. Para mais exatidão, utilizar as pontuações a nível dos objetivos para efeitos de apresentação de relatórios.

A figura 3 a seguir sintetiza os mecanismos de pontuação nos diferentes níveis do modelo (objetivo, grupo, geral).

Figura 3: Mecanismo de pontuação geral



3.5 REQUISITOS PARA O QUADRO DE AUTOAVALIAÇÃO

O quadro de avaliação das capacidades nacionais apresentado nesta secção baseia-se nas necessidades salientadas pelos Estados-Membros e está estruturado em torno de um conjunto de requisitos listados a seguir:

- O QACN é implementado voluntariamente pelo Estado-Membro enquanto um quadro de autoavaliação;
- O QACN visa medir as capacidades em matéria de cibersegurança dos Estados-Membros no atinente aos 17 objetivos. Contudo, o Estado-Membro pode escolher os objetivos relativamente aos quais pretende fazer a avaliação e apenas avaliar um subconjunto dos 17 objetivos;
- O quadro de autoavaliação visa medir o nível de maturidade das capacidades em matéria de cibersegurança do Estado-Membro;
- Os resultados da avaliação não são publicados, salvo se o Estado-Membro decidir fazê-lo por iniciativa própria;
- O Estado-Membro pode expor os resultados da avaliação apresentando o nível de maturidade das capacidades em matéria de cibersegurança do país, de um grupo ou até mesmo de um único objetivo;
- Todos os objetivos avaliados apresentam a mesma relevância no quadro de avaliação, pelo que têm a mesma importância. O mesmo se aplica aos indicadores nele utilizados; e
- O Estado-Membro pode acompanhar o seu progresso ao longo do tempo.

O quadro de autoavaliação visa apoiar os Estados-Membros a criarem capacidades em matéria de cibersegurança. Por conseguinte, também inclui um conjunto de recomendações ou orientações para guiar os países europeus na melhoria do respetivo nível de maturidade.

Nota: essas recomendações ou orientações são de caráter genérico e baseadas nas publicações da ENISA e nos ensinamentos extraídos de outros países e dependerão do resultado da autoavaliação.

4. INDICADORES DO QACN

4.1 INDICADORES DO QUADRO

Esta secção apresenta os indicadores do Quadro de Avaliação das Capacidades Nacionais da ENISA. As secções que se seguem estão organizadas por grupo.

Para cada grupo, um quadro apresenta um conjunto abrangente de indicadores na forma de perguntas representativas de um determinado nível de maturidade. O questionário é o principal instrumento para a autoavaliação. Para cada objetivo, há dois conjuntos de indicadores a salientar:

- Um conjunto de perguntas genéricas relativas à maturidade da estratégia (9 perguntas genéricas), assinaladas de «a» a «c» para cada nível de maturidade, repetidas para cada objetivo; e
- Um conjunto de perguntas sobre capacidade em matéria de cibersegurança (319 perguntas sobre capacidades em matéria de cibersegurança), numeradas de «1» a «10» para cada nível de maturidade, específicas do domínio abrangido pelo objetivo.

Cada pergunta é apresentada com uma etiqueta (0-1) indicando se a pergunta é um indicador exigido (1) ou um indicador não exigido (0) para o nível de maturidade.

Cada pergunta pode ser identificada por um número de identificação composto por:

- O número do objetivo;
- O nível de maturidade; e
- O número da pergunta.

Por exemplo, a pergunta ID 1.2.4 é a quarta pergunta no nível 2 de maturidade do objetivo estratégico (I) «Desenvolver planos nacionais de contingência cibernética».

Cumpre salientar que ao longo do questionário, o âmbito das perguntas é ao nível nacional, salvo indicação em contrário. Em todas as perguntas, a utilização da terceira pessoa do singular refere-se ao Estado-Membro de um modo genérico e não se refere à pessoa ou organismo governamental que realiza a avaliação.

A definição de cada objetivo pode ser consultada no capítulo 2.2 - Objetivos comuns identificados nas ENC europeias.

4.1.1 Grupo #1: Governação e normas de cibersegurança

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
1 – Desenvolver planos nacionais de contingência cibernética	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Começou a trabalhar na criação de planos nacionais de contingência cibernética? Ou seja, estabelecendo os objetivos gerais, o âmbito e/ou os princípios dos planos de contingência...	1	Dispõe de uma doutrina/estratégia nacional que inclua a cibersegurança como um fator de crise (isto é, uma matriz, uma política, etc.)?	1	Dispõe um plano de gestão de crise cibernética de nível nacional?	1	Está satisfeito com o número ou a percentagem de setores críticos incluídos no plano nacional de contingência cibernética?	1	Dispõe de um processo de recolha de experiências na sequência de exercícios no domínio da cibersegurança ou de crises reais a nível nacional?	1
	2	É geralmente aceite que os ciberincidentes constituem um fator de crise que poderá ameaçar a segurança nacional?	0	Dispõe de um centro para obter informações e informar os decisores? Ou seja, métodos, plataformas ou locais para assegurar que todos os intervenientes de resposta a crises podem aceder às mesmas informações em tempo real sobre a cibercrise?	1	Dispõe de procedimentos específicos de cibercrise de nível nacional?	1	Organiza atividades (ou seja, exercícios) relacionados com planeamento nacional de contingência cibernética com uma frequência suficiente?	1	Dispõe de um processo para testar regularmente o plano nacional?	1
	3	Foram realizados estudos (técnicos, operacionais, políticos) no domínio do planeamento de contingência cibernética?	0	Estão envolvidos os recursos relevantes para supervisionar o desenvolvimento e a execução de planos nacionais de contingência cibernética?	1	Tem um equipa de comunicação com formação específica para responder a cibercrises e informar o público?	1	Dispõe de pessoas suficientes dedicadas a planos de crise, à análise dos ensinamentos extraídos e à implementação da mudança?	1	Dispõe de ferramentas e plataformas adequadas para criar um conhecimento da situação?	1
	4	-		Dispõe de uma metodologia de avaliação das ciberameaças a nível nacional que inclua procedimentos para avaliação de impacto?	0	Envolve todas as partes interessadas nacionais relevantes (segurança nacional, defesa, proteção civil, aplicação da lei, ministérios, autoridades, etc.?)	1	Dispõe de pessoas suficientes com formação para responder a cibercrises a nível nacional?	1	Segue um modelo de maturidade específico para acompanhar e melhorar o plano de contingência cibernética?	0
	5	-		-		Dispõe de instalações adequadas de gestão de crises e de salas de situação?	1	-		Dispõe de recursos especializados na antecipação de ameaças ou que trabalhem em cibersegurança prospetiva para resolver futuras crises ou desafios de amanhã?	0
	6	-		-		Colabora com partes interessadas nacionais na UE, se necessário?	0	-		-	
	7	-		-		Colabora com partes interessadas internacionais em países terceiros, se necessário?	0	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
2 – Estabelecer medidas de segurança de base	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Realizou um estudo para identificar requisitos e lacunas para organizações **públicas** com base em normas reconhecidas internacionalmente? Por exemplo, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	As medidas de segurança são elaboradas em conformidade com normas internacionais/nacionais?	1	As medidas de segurança de base são obrigatórias?	1	Existe um processo para atualizar frequentemente medidas de segurança de base?	1	Dispõe de um processo para reforçar as TIC quando as medidas não conseguem resolver incidentes?	1
	2	Realizou um estudo para identificar requisitos e lacunas para organizações **privadas** com base em normas reconhecidas internacionalmente? Por exemplo, SO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	O setor privado e outras partes interessadas são consultados aquando da definição de medidas de segurança de base?	1	Implementa medidas de segurança horizontais em setores críticos?	1	Existe um mecanismo de monitorização para examinar a adoção de medidas de segurança de base?	1	Avalia a relevância de novas normas que são desenvolvidas em resposta à evolução mais recente no cenário de ameaças?	1
	3	-		-		Implementa medidas de segurança setoriais específicas em setores críticos?	1	Existe uma autoridade nacional para verificar se as medidas de segurança de base são ou não aplicadas?	1	Dispõe de ou promove um processo nacional de divulgação coordenada das vulnerabilidades (DCV)?	1
	4	-				As medidas de segurança de base são consentâneas com os sistemas de certificação relevantes?	1	Dispõe de um processo para identificar organizações não conformes num prazo específico?	1	-	
	5	-		-		Existe um processo de autoavaliação de riscos para medidas de segurança de base?	1	Existe um processo de auditoria para garantir que as medidas de segurança são corretamente aplicadas?	1	-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
2 – Estabelecer medidas de segurança de base	6	-		-		Examina medidas de segurança de base obrigatórias no processo de contratação de organismos governamentais?	0	Define ou encoraja ativamente a adoção de normas seguras para o desenvolvimento de produtos de TI/TO (equipamento médico, veículos conectados e autónomos, rádio profissional, equipamento para a indústria pesada...)?	0	-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
3 – Proteger a identidade digital e criar confiança nos serviços públicos digitais	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Realizou estudos ou análises de lacunas para identificar as necessidades de proteger serviços públicos digitais prestados aos cidadãos e às empresas?	1	Realiza análises de risco para determinar o perfil de risco dos ativos ou serviços antes de os transferir para a nuvem ou envolver-se em projetos de transformação digital?	1	Promove metodologias de privacidade desde a conceção em todos os projetos de administração pública em linha (eGoverno)?	1	Recolhe indicadores sobre incidentes de cibersegurança que envolvam a violação de serviços públicos digitais?	1	Participa em grupos de trabalho europeus para manter normas e/ou conceber novos requisitos para serviços de confiança eletrónicos (assinaturas eletrónicas, selos eletrónicos, serviços de envio registado eletrónico, marca temporal, autenticação de sítios Web)? Por exemplo, ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU...	1
	2	-		Tem uma estratégia para criar ou promover sistemas nacionais de identificação eletrónica seguros (eIDs) para cidadãos e empresas?	1	Inclui partes interessadas privadas na conceção e prestação de serviços públicos digitais seguros?	1	Implementou o reconhecimento mútuo de meios de identificação eletrónica com outros Estados-Membros?	1	Participa ativamente em análises pelos pares enquanto parte da notificação de sistemas de identificação eletrónica à Comissão Europeia?	1

	3	-		Dispõe de uma estratégia para criar ou promover serviços nacionais de confiança eletrónicos (assinaturas eletrónicas, selos eletrónicos, serviços de envio registado eletrónico, marca temporal, autenticação de sítios Web) para cidadãos e empresas?	1	Implementa uma linha de base de segurança mínima para todos os serviços públicos digitais?	1	-		-	
Objetivo da ENC	**#**	**Nível 1**	**R**	**Nível 2**	**R**	**Nível 3**	**R**	**Nível 4**	**R**	**Nível 5**	**R**
3 – Proteger a identidade digital e criar confiança nos serviços públicos digitais	4	-		Dispõe de uma estratégia sobre informática governamental em nuvem («Governmental Cloud») (uma estratégia de computação em nuvem orientada para organismos do Estado ou públicos, tais como ministérios, agências governamentais e administrações públicas...) que tenha em conta as implicações para a segurança?	0	Estão disponíveis sistemas de identificação eletrónica para cidadãos e empresas com um nível de garantia substancial ou elevado conforme definido no anexo do Regulamento eIDAS (UE) n.º 910/2014?	1	-		-	
	5	-		-		Tem serviços públicos digitais que requeiram sistemas de identificação eletrónica com um nível de garantia substancial ou elevado conforme definido no anexo do Regulamento eIDAS (UE) n.º 910/2014?	1	-		-	
	6	-		-		Dispõe de prestadores de serviços de confiança para os cidadãos e as empresas (assinaturas eletrónicas, selos eletrónicos, serviços de envio registado eletrónico, marca temporal, autenticação de sítios Web)?	1	-		-	
	7	-		-		Promove a adoção de medidas de segurança de base para todos os modelos de implantação de computação em nuvem (por exemplo, privado, público, híbrido, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Grupo #2: Criação de capacidades e sensibilização

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
4 – Estabelecer uma capacidade de resposta a incidentes	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Dispõe de capacidades informais de resposta a incidentes geridas nos ou entre os setores público e privado?	1	Dispõe de, pelo menos, uma equipa de resposta a incidentes de segurança informática (CSIRT) nacional oficial?	1	Dispõe de capacidades de resposta a incidentes para os setores mencionados no anexo II da Diretiva SRI?	1	Definiu e promoveu práticas normalizadas para procedimentos de resposta a incidentes e sistemas de classificação de incidentes?	1	Dispõe de mecanismos para deteção antecipada, identificação, prevenção, resposta e mitigação de vulnerabilidades previamente desconhecidas (de dia zero)?	1
	2	-		A(s) sua(s) CSIRT têm um âmbito de intervenção claramente definido? Por exemplo, dependendo do setor visado, dos tipos de incidente, dos impactos	1	Existe um mecanismo de cooperação das CSIRT no seu país para responder a incidentes?	1	Avalia a sua capacidade de resposta a incidentes para garantir que dispõe dos recursos e competências adequados para realizar as tarefas estabelecidas no ponto (2) do anexo I da Diretiva SRI?	1	-	
	3	-		A(s) sua(s) CSIRT tem(êm) relações claramente definidas com outras partes interessadas nacionais no que diz respeito ao cenário nacional de cibersegurança e à prática de resposta a incidentes (por exemplo, SAL, exército, FSI, CNCS)?	0	A(s) sua(s) CSIRT dispõe(m) de uma capacidade de resposta a incidentes em conformidade com o anexo I da Diretiva SIR? Ou seja, disponibilidade, segurança física, continuidade das atividades, cooperação internacional, monitorização de incidentes, capacidade de avisos e alertas precoces, resposta a incidentes, análise de riscos e conhecimento da situação, cooperação com o setor privado, práticas normalizadas...	1	-		-	
	4	-				Existe um mecanismo de cooperação com outros países vizinhos no tocante a incidentes?	1	-		-	
	5	-		-		Definiu formalmente políticas e procedimentos claros de tratamento de incidentes?	1	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
4 – Estabelecer uma capacidade de resposta a incidentes	6	-		-		A(s) sua(s) CSIRT nacional(ais) participa(m) em exercícios de cibersegurança a nível nacional e internacional?	1	-		-	
	7	-		-		A(s) sua(s) CSIRT nacional(ais) está(ão) associada(s) ao FIRST (Fórum das equipas de segurança e de resposta a incidentes)?	0	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
5 – Aumentar a sensibilização dos utilizadores	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Existe um reconhecimento mínimo por parte da administração pública, do setor privado ou dos utilizadores em geral de que é preciso sensibilizar para as questões da cibersegurança e da privacidade?	1	Identificou um público-alvo específico para sensibilização dos utilizadores? Por exemplo, utilizadores em geral, jovens, utilizadores de empresas (que podem ser subdivididos em: PME, OSE, PSD, etc.)	1	Elaborou planos/estratégia de comunicação para as campanhas?	1	Elaborou métricas para avaliar a sua campanha durante a fase de planeamento?	1	Dispõe de mecanismos para garantir que as campanha de sensibilização são constantemente pertinentes no tocante ao avanço tecnológico, às alterações ao cenário de ameaças, às normas jurídicas e às diretivas de segurança nacionais?	1
	2	As agências públicas realizam campanhas de sensibilização para a cibersegurança dentro da sua organização e numa base *ad hoc*? Por exemplo, na sequência de um incidente de cibersegurança.	0	Elabora um plano de projeto para sensibilizar para a segurança da informação e as questões da privacidade?	1	Dispõe de um processo para criar conteúdo a nível governamental?	1	Avalia as suas campanhas após a execução?	1	Realiza uma avaliação ou estudo periódico para medir a mudança de atitude ou mudanças de comportamento no tocante a matérias de cibersegurança e privacidade nos setores privados e públicos?	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
5 – Aumentar a sensibilização dos utilizadores	3	As agências públicas realizam campanhas de sensibilização para a cibersegurança destinadas ao público em geral e numa base *ad hoc*? Por exemplo, na sequência de um acidente de cibersegurança.	0	Dispõe de recursos disponíveis e facilmente identificáveis (por exemplo, um portal em linha único, conjuntos de sensibilização) para todos os utilizadores que procurem instruir-se em matéria de informações sobre cibersegurança e questões de privacidade?	1	Dispõe de mecanismos para identificar áreas-alvo para sensibilização (ou seja, cenário de ameaças da ENISA, cenários nacionais, cenários internacionais, retorno de informação de centros de cibercriminalidade, etc.)?	1	Dispõe de mecanismos para identificar o meio de comunicação social ou canal de comunicação mais relevante, em função do público-alvo para maximizar o alcance e envolvimento? Por exemplo, diferentes tipos de meios digitais, brochuras, correios eletrónicos, material educativo, cartazes em zonas movimentadas, televisão, rádio...	1	Consulta especialistas comportamentais para adaptar as suas campanhas ao público-alvo?	1
	4	-		-		Reúne partes interessadas com peritos e equipas de comunicação para criarem conteúdos?	1			-	
	5	-		-		Associa e vincula o setor privado nos seus esforços de sensibilização para promover e disseminar as mensagens a um público mais vasto?	1	-		-	
	6	-		-		Prepara iniciativas de sensibilização específicas para executivos nos setores público, privado, académico ou da sociedade civil?	1	-		-	
	7	-		-		Participa nas campanhas do «Mês europeu da cibersegurança» (MEC) da ENISA?	0	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5
6 – Organizar exercícios de cibersegurança	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
6 – Organizar exercícios de cibersegurança	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Realiza exercícios de crise noutros setores (que não cibersegurança) a nível nacional ou pan-europeu?	1	Dispõe de um programa de exercício de cibersegurança a nível nacional?	1	Envolve todas as autoridades relacionadas da administração pública? (mesmo que o cenário seja específico de um setor)	1	Redige relatórios após as ações/relatórios de avaliação?	1	Dispõe de uma capacidade de análise de ensinamentos extraídos em matéria de cibernética (processos de comunicação, análise, mitigação)?	1
	2	Dispõe de recursos afetados a conceção e planeamento de exercício de gestão de crises?	1	Realiza ou dá prioridade a exercícios de gestão de cibercrises em funções societais vitais e infraestruturas críticas?	1	Envolve o setor privado no planeamento e na execução dos exercícios?	1	Testa planos e procedimentos a nível nacional?	1	Dispõe de um processo estabelecido de ensinamentos extraídos?	1
	3	-		Identificou um organismo de coordenação para supervisionar a conceção e o planeamento de exercícios de cibersegurança (agência pública, gabinete de consultoria...)?	0	Organiza exercícios setoriais a nível nacional e/ou internacional?	1	Participa em exercícios de cibersegurança a nível pan-europeu?	1	Adapta os cenários de exercício em função das evoluções mais recentes (avanços tecnológicos, conflitos mundiais, cenário de ameaças...)?	1
	4	-		-		Organiza exercícios em todos os setores críticos referidos no anexo II da Diretiva SRI?	1	-		Alinha os seus procedimentos de gestão de crises com outros Estados-Membros para assegurar uma gestão de crises pan-europeia eficaz?	1
	5	-		-		Organiza exercícios de cibersegurança intersectoriais e/ou transectoriais?	1	-		Dispõe de um mecanismo para adaptar rapidamente a estratégia, os planos e os procedimentos a partir dos ensinamentos extraídos durante os exercícios?	0
	6	-		-		Organiza exercícios de cibersegurança específicos para vários níveis? (nível técnico e operacional, nível de procedimentos, nível de tomada de decisão, nível político...)	0	-		-	

Objetivo da ENC	#	Level 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
7 – Reforçar os programas de formação e educativos	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Pondera desenvolver formação e programas educativos em matéria de cibersegurança?	1	Cria cursos dedicados à cibersegurança?	1	O seu país engloba a cultura da cibersegurança na fase inicial do percurso escolar dos alunos? Por exemplo, favorece a cibersegurança no 2.º e 3.º ciclos do ensino básico e no ensino secundário?	1	Incita o pessoal no setor privado e público a ser acreditado ou certificado?	1	Dispõe de mecanismos para garantir que as formações e os programas educativos são constantemente pertinentes no tocante às evoluções tecnológicas atuais e emergentes, às alterações ao cenário de ameaças, às normas jurídicas e às diretivas de segurança nacionais?	1
	2	-		As universidades do seu país oferecem doutoramentos em cibersegurança enquanto uma cadeira autónoma e não como uma disciplina das ciências da computação?	1	Dispõe de laboratórios de investigação nacionais e instituições de ensino especializados em cibersegurança?	1	O seu país desenvolveu formação ou programas de mentoria em cibersegurança para apoiar as empresas em fase de arranque e PME nacionais?	1	Cria centros académicos de excelência em matéria de cibersegurança para atuarem como plataformas de investigação e educação?	1
	3	-		Planeia formar educadores, independentemente do respetivo domínio, em segurança da informação e questões de privacidade? Por exemplo, segurança em linha, proteção de dados pessoais, ciberassédio.	1	Encoraja/financia cursos e planos de formação dedicados a cibersegurança destinados a funcionários de agência de emprego do Estado-Membro?	1	Promove ativamente a inclusão de cursos de segurança da informação no ensino superior não apenas para estudantes de ciências da computação, mas também para qualquer outra especialidade profissional? Por exemplo, cursos adaptados às necessidades dessa profissão.	1	As instituições académicas estão a participar em debates proeminentes no domínio da educação e investigação em cibersegurança a nível internacional?	0
	4	-		-		Dispõe de cursos e/ou programa curricular especializado em cibersegurança para o nível 5 a 8 do QEQ (Quadro Europeu de Qualificações)?	1	Avalia regularmente o défice de competências (escassez de trabalhadores em cibersegurança) no domínio da segurança da informação?	1	-	
	5	-		-		Incentiva e/ou apoia iniciativas para incluir cursos de segurança da Internet no nível primário e secundário do ensino?	1	Promove a criação de redes e a partilha de informações entre instituições académicas, a nível nacional e internacional?	1		

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
7 - Reforçar os programas de formação e educativos	6	-		-		Financia ou oferece formações básicas em cibersegurança aos cidadãos?	0	Envolve de alguma forma o setor privado nas iniciativas de educação em matéria de cibersegurança? Por exemplo, conceção e ministração dos cursos, estágios e programas de aprendizagem...	1	-	
	7	-		-		Organiza eventos anuais de segurança da informação [por exemplo, concursos relacionados com pirataria informática ou *hackathons* (maratonas tecnológicas)]?	0	Implementa mecanismos de financiamento para encorajar a adesão a diplomas de cibersegurança? Por exemplo, bolsas de estudo, aprendizagem/estágio garantido, emprego garantido em indústria específica ou funções no setor público	0	-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
8 – Promover a I&D	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Realizou estudos ou análises para identificar prioridades de I&D em cibersegurança?	1	Dispõe de um processo para definir prioridades de I&D (por exemplo, tópicos emergentes para impedir, proteger, detetar e adaptar a novos tipos de ciberataques)?	1	Existe um plano para ligar iniciativas de I&D à economia real?	1	As iniciativas de I&D em cibersegurança são consentâneas com os objetivos estratégicos relevantes, por exemplo, MUD, H2020, Europa Digital, Estratégia da UE para a Cibersegurança?	1	Procura cooperar a nível nacional com quaisquer iniciativas de I&D relacionadas com cibersegurança?	1
	2	-		O setor privado é envolvido na definição de prioridades de I&D?	1	Existem projetos nacionais implantados relacionados com cibersegurança?	1	Existe um sistema de avaliação para iniciativas de I&D?	1	As prioridades de I&D estão alinhadas com a regulamentação em vigor e futura (a nível nacional)?	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
8 – Promover a I&D	3	-		O meio académico é envolvido na definição de prioridades de I&D?	1	Dispõe de ecossistemas de empresas em fase de arranque locais/regionais e outros canais de criação de redes (por exemplo, parques tecnológicos, polos de inovação, eventos/plataformas de criação de redes) para promover a inovação (incluindo para empresas em fase de arranque no domínio da cibersegurança)?	1	Existem acordos de cooperação com universidades e outras instalações de investigação?	1	Participa em debates proeminentes num ou vários tópicos de I&D de ponta a nível internacional?	0
	4	-		Existem iniciativas nacionais de I&D relacionadas com a cibersegurança?	0	Existe investimento em programas de I&D no meio académico e no setor privado?	1	Existe um organismo institucional reconhecido que supervisione atividades de I&D no domínio da cibersegurança?	0	-	
	5	-		-		Dispõe de cátedras de investigação industrial nas universidades para fazer a ponte entre áreas temáticas de investigação e as necessidades do mercado?	1	-		-	
	6	-		-		Dispõe de programas de financiamento de I&D específicos para cibersegurança?	0	-		-	

Objetivo da ENC	#	Level 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
9 – Proporcionar incentivos para o setor privado investir em medidas de segurança	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Existe uma política industrial ou vontade política para encorajar o desenvolvimento da indústria da cibersegurança?	1	O setor privado é envolvido na conceção de incentivos?	1	Existem incentivos económicos/regulamentares ou de outro tipo para promover investimentos em cibersegurança?	1	Existem intervenientes privados que reagem a incentivos investindo em medidas de segurança? Por exemplo, investidores especializados em cibersegurança e investidores não especializados.	1	Concentra incentivos em tópicos de cibersegurança dependendo das mais recentes evoluções de ameaças?	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
9 – Proporcionar incentivos para o setor privado investir em medidas de segurança	2	-		Identificou tópicos de cibersegurança a serem desenvolvidos? Por exemplo, criptografia, privacidade, nova forma de autenticação, IA para cibersegurança...	0	Presta apoio (por exemplo, incentivos fiscais) a empresas em fase de arranque e PME de cibersegurança?	1	Proporciona incentivos ao setor privado para se concentrar em tecnologias de ponta de segurança? Por exemplo, 5G, inteligência artificial, IdC, computação quântica...	1	-	
	3	-		-		Proporciona incentivos ou outra motivação financeira para investidores do setor privado em empresas em fase de arranque de cibersegurança?	1	-		-	
	4	-		-		Facilita o acesso a empresas em fase de arranque e PME de cibersegurança ao processo de contratos públicos?	0	-		-	
	5	-		-		Existe orçamento disponível para proporcionar incentivos ao setor privado?	0	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
10 – Melhorar a cibersegurança da cadeia de abastecimento	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Realizou um estudo sobre boas práticas de segurança para a gestão da cadeia de abastecimento usada pela contratação em vários segmentos da indústria e/ou no setor público?	1	Realiza avaliações de cibersegurança em toda a cadeia de abastecimento de serviços e produtos TIC em setores críticos (conforme identificados no anexo II da Diretiva SRI (2016/1148)?	1	Utiliza um sistema de certificação da segurança para produtos e serviços baseados nas TIC? Por exemplo, SOG-IS MRA na Europa (Grupo de Altos Funcionários para a segurança dos sistemas informáticos, Acordo de Reconhecimento Mútuo), Acordo de Reconhecimento dos Critérios Comuns (ARCC), iniciativas nacionais, iniciativas setoriais...	1	Dispõe de um processo para atualizar as avaliações de cibersegurança da cadeia de abastecimento de serviços e produtos TIC em setores críticos (conforme identificados no anexo II da Diretiva SRI (2016/1148)?	1	Dispõe de sondas de deteção em elementos-chave na cadeia de abastecimento para detetar sinais precoces de comprometimento? Por exemplo, controlos de segurança a nível dos FSI, inquéritos de segurança em grandes componentes de infraestruturas...	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
10 – Melhorar a cibersegurança da cadeia de abastecimento	2	-		Aplica normas às políticas de contratação das administrações públicas para garantir que os fornecedores de produtos ou serviços TIC satisfazem os requisitos base de segurança da informação? Por exemplo, ISO/IEC 27001 e 27002, ISO/IEC 27036...	1	Promove ativamente boas práticas de segurança e proteção desde a conceção no desenvolvimento de produtos e serviços TIC? Por exemplo, ciclo de vida do desenvolvimento de *software* seguro, ciclo de vida da IdC	1	Dispõe de um processo para identificar ligações fracas de cibersegurança na cadeia de abastecimento de setores críticos (conforme identificados no anexo II da Diretiva SRI (2016/1148)?	1	-	
	3	-		-		Elabora e fornece catálogos centralizados com informações aprofundadas sobre normas existentes de segurança da informação e privacidade que sejam escalonáveis para e aplicáveis pelas PME?	1	Dispõe de mecanismos para garantir que os produtos e serviços TIC que são críticos para OSE são ciberresilientes (ou seja, a capacidade de manter a disponibilidade e segurança contra um ciberincidente)? Por exemplo, através de testes, avaliações regulares, deteção de elementos comprometidos...	1	-	
	4	-				Participa ativamente na conceção de um enquadramento europeu para a certificação destinado a produtos, serviços e processos digitais de TIC conforme estabelecido no Regulamento Cibersegurança da UE [Regulamento (UE) 2019/881)? Por exemplo, participação no Grupo Europeu para a Certificação da Cibersegurança (GECC), promoção de normas técnicas e procedimentos para segurança de produtos/serviços TIC	0	Promove o desenvolvimento de sistemas de certificação direcionados para as PME a fim de aumentar a segurança da informação e a adoção de um padrão de privacidade?	0	-	
	5	-		-		Proporciona quaisquer tipos de incentivos às PME para adotarem normas de segurança e privacidade?	0	Tem disposições para encorajar as grandes empresas a aumentarem a cibersegurança das pequenas empresas nas respetivas cadeias de abastecimento? Por exemplo, polo de cibersegurança, formação e campanhas de sensibilização...	0	-	
	6	-		-		Encoraja os distribuidores de *software* a apoiarem as PME garantindo configurações por defeito seguras em produtos que visam pequenas organizações?	0	-		-	

4.1.3 Grupo #3: Aspetos jurídicos e regulamentares

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
11 – Proteger infraestruturas críticas da informação, OSE e PSD	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Existe um entendimento geral de que os operadores de ICI contribuem para a segurança nacional?	1	Dispõe de uma metodologia para identificar serviços essenciais?	1	Implementou a Diretiva SRI (2016/1148)?	1	Dispõe de um procedimento para atualizar o registo de riscos?	1	Elabora e atualiza relatórios sobre o cenário de ameaças?	1
	2	-		Dispõe de uma metodologia para a identificação de ICI?	1	Implementou a Diretiva ICE (2008/114) relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção?	1	Dispõe de outros mecanismos para medir se as medidas técnicas e organizacionais implementadas pelos OSE são apropriadas para gerir os riscos colocados à segurança das redes e da informação? Por exemplo, auditorias de cibersegurança regulares, quadro nacional para a implementação de medidas-tipo, ferramentas técnicas fornecidas pelo governo tais como sondas de deteção ou revisão da configuração específica do sistema.	1	Dependendo das evoluções mais recentes no cenário de ameaças, consegue integrar um novo setor no seu plano de ação PICI?	1
	3	-		Dispõe de uma metodologia para identificar OSE?	1	Dispõe de um registo nacional para OSE identificados por setor crítico?	1	Revê e, consequentemente, atualiza a lista de OSE identificados no mínimo de dois em dois anos?	1	Dependendo das evoluções mais recentes no cenário de ameaças, consegue adaptar novos requisitos no seu plano de ação PICI?	1

Objetivo da ENC	#										
11 – Proteger infraestruturas críticas da informação, OSE e PSD	4	-		Dispõe de uma metodologia para identificar prestadores de serviços digitais?	1	Dispõe de um registo nacional para prestadores de serviços digitais identificados?	1	Dispõe de outros mecanismos para medir se as medidas técnicas e organizacionais implementadas pelos prestadores de serviços digitais são apropriadas para gerir os riscos colocados à segurança da rede e dos sistemas de informação? Por exemplo, auditorias de cibersegurança regulares, quadro nacional para a implementação de medidas-tipo, ferramentas técnicas fornecidas pelo governo tais como sondas de deteção ou revisão da configuração específica do sistema...	1	-	
	5	-		Tem uma autoridade nacional ou mais que supervisione a proteção das infraestruturas críticas da informação e a segurança das redes e da informação? Por exemplo, conforme exigido pela Diretiva SRI (2016/1148)	1	Dispõe de um registo nacional para riscos identificados ou conhecidos?	1	Revê e, consequentemente, atualiza a lista de prestadores de serviços digitais identificados no mínimo de dois em dois anos?	1	-	
	6	-		Elabora planos de proteção específicos de setor? Por exemplo, que incluam medidas de cibersegurança de base (obrigatórias ou orientações)	0	Dispõe de uma metodologia para cartografar dependências de ICI?	1	Utiliza um sistema de certificação da segurança (nacional ou internacional) para ajudar os OSE e os prestadores de serviços digitais a identificarem produtos TIC seguros? Por exemplo, SOG-IS MRA na Europa, iniciativas nacionais...	1	-	
	7	-		-		Implementa práticas de gestão de riscos para identificar, quantificar e gerir riscos relacionadas com as ICI a nível nacional?	1	Utiliza um sistema de certificação da segurança ou procedimento de qualificação para avaliar os prestadores de serviços que trabalham com OSE? Por exemplo, prestadores de serviços no domínio da deteção de incidentes, resposta a incidentes, auditoria de cibersegurança, serviços em nuvem, cartões inteligentes...	1	-	
	8	-		-		Inicia um processo de consulta para identificar dependências transfronteiriças?	1	Dispõe de mecanismos para medir o nível de conformidade dos OSE e dos prestadores de serviços digitais no tocante a medidas de cibersegurança de base?	0	-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
11 – Proteger infraestruturas críticas da informação, OSE e PSD	9					Tem um ponto único de contacto responsável pela coordenação de questões relacionadas com a segurança das redes e da informação a nível nacional e a cooperação transfronteiriça a nível da União?	1	Tem disposições em vigor para garantir a continuidade dos serviços prestados por infraestruturas críticas da informação? Por exemplo, antecipação de crises, procedimentos para reconstruir sistemas de informação críticos, continuidade das atividades sem TI, procedimentos de salvaguarda «air gap»...	0		
	10					Define medidas de cibersegurança de base (obrigatórias ou orientações) para prestadores de serviços digitais e todos os setores identificados no anexo II da Diretiva SRI (2016/1148)?	1				
	11	-		-		Fornece ferramentas ou metodologias para detetar ciberincidentes?	1	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
12 – Combater a cibercriminalidade	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Realizou um estudo para identificar requisitos de aplicação da lei (base jurídica, recursos, competências...) para combater eficazmente a cibercriminalidade?	1	O seu quadro jurídico nacional cumpre cabalmente o quadro jurídico da UE relevante, nomeadamente a Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação? Por exemplo, acesso ilegal a sistemas de informação, interferência ilegal em sistemas, interferência ilegal nos dados, interceção ilegal, instrumentos utilizados para cometer infrações...	1	Tem unidades dedicadas ao tratamento da cibercriminalidade nos gabinetes dos procuradores?	1	Recolhe estatísticas seguindo o disposto no artigo 14.º, n.º 1, da Diretiva 2013/40/UE (Diretiva relativa a ataques contra os sistemas de informação)?	1	Dispõe de formação interinstitucional ou seminários de formação para SAL, juízes, procuradores e CSIRT nacionais/governamentais a nível nacional e/ou a nível multilateral?	1
	2	Realizou um estudo para identificar os requisitos dos procuradores e juízes (base jurídica, recursos, competências...) para combater eficazmente a cibercriminalidade?	1	Tem uma disposição legal que aborde a usurpação de identidade em linha e o roubo de dados pessoais?	1	Dispõe de um orçamento específico atribuído às unidades que combatem a cibercriminalidade?	1	Recolhe estatísticas discriminadas sobre cibercriminalidade? Por exemplo, estatísticas operacionais, estatísticas sobre tendências de cibercriminalidade, estatísticas sobre o produto e os danos causados pela cibercriminalidade...	1	Participa em ações coordenadas a nível internacional para interromper as atividades criminosas? Por exemplo, infiltração em fóruns de intrusões informáticas criminosas, grupos de cibercriminalidade organizada, mercados da Web obscura e eliminação de redes de computadores infetados (*botnets*)...	1
	3	O seu país assinou a Convenção de Budapeste sobre o Cibercrime do Conselho da Europa?	1	Tem disposições legais que abordem as infrações à propriedade intelectual e aos direitos de autor em linha?	1	Criou um organismo/entidade central para coordenar as atividades no domínio do combate à cibercriminalidade?	1	Avalia a adequação da formação prestada aos SAL, ao pessoal do poder judicial e da(s) CSIRT nacional(ais) para combater a cibercriminalidade?	1	Existe uma separação nítida de funções nas CSIRT, nos SAL e no poder judicial (procuradores e juízes) quando cooperam para combater cibercrimes?	1
	4			Tem disposições legais que abordem o assédio em linha ou o ciberassédio?	1	Criou mecanismos de cooperação entre as instituições nacionais relevantes envolvidas no combate à cibercriminalidade, nomeadamente CSIRT nacionais envolvidas na aplicação da lei?	1	Realiza avaliações regulares para garantir que dispõe de recursos suficientes (humanos, orçamentais e ferramentas) dedicados às unidades de combate à cibercriminalidade nos SAL?	1	O seu quadro regulamentar facilita a cooperação entre as CSIRT/SAL e o poder judicial (procuradores e juízes)?	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
12 - Combater a cibercriminalidade	5			Tem disposições legais que abordem a fraude informática? Por exemplo, conformidade com as disposições da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa	1	Coopera e partilha informações com outros Estados-Membros no domínio do combate à cibercriminalidade?	1	Realiza avaliações regulares para garantir que dispõe de recursos suficientes (humanos, orçamentais e ferramentas) dedicados às unidades de combate à cibercriminalidade no seio das autoridades judiciais?	1	Participa na criação e manutenção de instrumentos e metodologias, formulários e procedimentos normalizados a serem partilhados com as partes interessadas da UE (SAL, CSIRT, ENISA, EC3 da Europol...)?	1
	6	-		Tem disposições legais que abordem a proteção em linha das crianças? Por exemplo, conformidade com as disposições da Diretiva 2011/93/UE e a Convenção de Budapeste sobre o Cibercrime do Conselho da Europa...	1	Coopera e partilha informações com outras agências da UE (por exemplo, o EC3 da Europol, a Eurojust, a ENISA) no domínio do combate à cibercriminalidade?	1	Dispõe de unidades de tribunais específicos ou juízes especializados para tratar de processos de cibercriminalidade?	1	Dispõe de mecanismos avançados para impedir que as pessoas sejam atraídas ou envolvidas na cibercriminalidade?	0
	7	-		Identificou um ponto de contacto nacional operacional para trocar informações e responder a pedidos urgentes de informação de outros Estados-Membros relacionados com infrações estabelecidas na Diretiva 2013/40/UE (Diretiva relativa a ataques contra os sistemas de informação)?	1	Dispõe dos instrumentos adequados para combater a cibercriminalidade? Por exemplo, taxonomia e classificação da cibercriminalidade, instrumentos para recolher meios de prova eletrónicos, instrumentos de informática forense, plataformas de partilha de confiança...	1	Tem disposições dedicadas a prestar apoio e assistências às vítimas de cibercriminalidade (utilizadores em geral, PME, grandes empresas)?	1	O seu país utiliza a Matriz da UE e/ou o Protocolo relativo à resposta de emergência dos serviços repressivos (EU LE ERP) para responder eficazmente a ciberincidentes de grande escala?	0
	8			A sua agência de aplicação da lei inclui uma unidade específica de combate à cibercriminalidade?	1	Dispõe de procedimentos operacionais normalizados, para tratar meios de prova eletrónicos?	1	Criou um quadro interinstitucional e mecanismos de cooperação entre todas as partes interessadas relevantes (por exemplo, SAL, CSIRT nacional, comunidades do poder judicial), incluindo o setor privado (por exemplo, operadores de serviços essenciais, prestadores de serviços) quando apropriado, para responder a ciberataques?	1	-	
	9			Designou, em conformidade com o artigo 35.º da Convenção de Budapeste, um ponto de contacto 24/7?	1	O seu país participa em oportunidades de formação oferecidas e/ou apoiadas por agências da UE (por exemplo, Europol, Eurojust, OLAF, Cepol, ENISA)?	0	O seu quadro regulamentar facilita a cooperação entre as CSIRT e os SAL?	1	-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
12 – Combater a cibercriminalidade	10	-		Designou um ponto de contacto nacional 24/7 operacional para o Protocolo relativo à resposta de emergência dos serviços repressivos (EU LE ERP) para responder a ciberataques de grande dimensão?	1	O seu país está a ponderar adotar o segundo protocolo adicional da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa?	0	Dispõe de mecanismos (por exemplo, instrumentos, procedimentos) para facilitar o intercâmbio de informações e a cooperação entre CSIRT/SAL e eventualmente o poder judicial (procuradores e juízes) no domínio do combate à cibercriminalidade?	1	-	
	11			Presta regularmente formação especializada a partes interessadas envolvidas no combate à cibercriminalidade (SAL, poder judicial, CSIRT)? Por exemplo, sessões de formação sobre o registo/instauração ações penais por crimes possibilitados pelo ciberespaço, formações sobre a recolha de meios de prova eletrónicos e garantia da integridade ao longo da cadeia digital de custódia e informática forense, entre outros	1						
	12			O seu país ratificou/aderiu à Convenção de Budapeste sobre o Cibercrime do Conselho da Europa?	1			-	-	-	
	13	-		O seu país assinou e ratificou o protocolo adicional (incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos) da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa?	0	-	-	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
13 – Criar mecanismos de comunicação de incidentes	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Dispõe de mecanismos informais de partilha de informações sobre incidentes de cibersegurança, incidentes entre organizações privadas e autoridades nacionais?	1	Dispõe de um sistema de comunicação de incidentes para todos os setores mencionados no anexo II da Diretiva SRI?	1	Dispõe de um sistema obrigatório de comunicação de incidentes que esteja a funcionar na prática?	1	Dispõe de um procedimento harmonizado para sistemas de comunicação de incidentes setoriais?	1	Elabora um relatório anual de incidentes?	1
	2	-		Implementou os requisitos de notificação para os fornecedores de serviços de telecomunicação em conformidade com o artigo 40.º da Diretiva (UE 2018/1972)? A diretiva obriga a que os Estados-Membros assegurem que os fornecedores de redes públicas de comunicações eletrónicas ou de serviços de comunicações eletrónicas acessíveis ao público notifiquem sem demora injustificada a autoridade competente de qualquer incidente de segurança que tenha tido um impacto significativo no funcionamento das redes ou serviços.	1	Existe um mecanismo de coordenação/cooperação para obrigações de comunicação de incidentes relativamente ao RGPD, Diretiva SRI, artigo 40.º (ex-art 13.º-A) e eIDAS?	1	Dispõe de um sistema de comunicação de incidentes para setores que não os mencionados na Diretiva SRI?	1	Existem relatórios sobre o cenário de cibersegurança ou outros tipos de análise elaborados pela entidade que recebe os relatórios de incidentes?	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
13 – Criar mecanismos de comunicação de incidentes	3	-		Implementou os requisitos de notificação para os prestadores de serviços de confiança em conformidade com o artigo 19.º do Regulamento eIDAS [Regulamento (UE) n.º 910/2014]? O artigo 19.º exige, entre outros requisitos, que os prestadores de serviços de confiança notifiquem a entidade supervisora sobre incidentes/violações significativas.	1	Dispõe dos instrumentos adequados para garantir a confidencialidade e a integridade das informações partilhadas através dos vários canais de comunicação?	1	Mede a eficácia dos procedimentos de comunicação de incidentes? Por exemplo, indicadores sobre incidentes que foram comunicados através dos canais apropriados, momento da comunicação do incidente...	1	-	
	4	-		Implementou os requisitos de notificação para os prestadores de serviços digitais em conformidade com o artigo 16.º da Diretiva SRI? O artigo 16.º exige que os prestadores de serviços digitais notifiquem a autoridade competente ou a CSIRT nacional, sem demora injustificada, dos incidentes com impacto substancial na prestação dos serviços referidos no anexo III no anexo III por si oferecidos na União.	1	Dispõe de uma plataforma/instrumento para facilitar o processo de comunicação?	0	Tem uma taxonomia comum a nível nacional para a classificação de incidentes e categorias de causas profundas?	0	-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
14 – Reforçar a privacidade e a proteção de dados	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Realizou estudos ou análises para identificar áreas de melhoria a fim de melhor proteger aos direitos dos cidadãos em matéria de privacidade?	1	A autoridade nacional de proteção de dados é envolvida em domínios críticos de cibersegurança (por exemplo, redação de novas leis e regulamentos sobre cibersegurança, medidas mínimas de segurança definidas)?	1	Promove boas práticas sobre medidas de segurança e proteção de dados desde a conceção para o público e/ou o setor privado?	1	Realiza avaliações regulares para garantir que dispõe de recursos suficientes (humanos, orçamentais e ferramentas) dedicados à autoridade de proteção de dados?	1	Dispõe de mecanismos para acompanhar as evoluções tecnológicas mais recentes a fim de adaptar orientações e disposições/obrigações jurídicas relevantes?	1
	2	Desenvolveu uma base jurídica a nível nacional para aplicar o Regulamento Geral sobre a Proteção de Dados [Regulamento (UE) 2016/679]? Por exemplo, manter ou introduzir disposições ou limitações mais específicas às regras do regulamento	0	-		Lança programas de sensibilização e formação em torno deste tópico?	1	Encoraja as organizações e empresas a obterem certificação de acordo com a norma ISO/IEC 27701:2019 sobre Sistema de Gestão da Privacidade da Informação (SGPI)?	1	Participa/promove ativamente iniciativas de I&D no que diz respeito às tecnologias de reforço da privacidade (TRP)?	0
	3	-		-		Coordena procedimentos de comunicação de incidentes com a APD?	1	-		-	
	4	-		-		Promove e apoia o desenvolvimento de normas sobre segurança da informação e proteção da privacidade? São as mesmas especificamente adaptadas a pequenas e médias empresas (PME)?	0	-		-	
	5	-		-		Fornece orientações práticas e escalonáveis para apoiar diferentes tipos de responsáveis pelo tratamento no cumprimento dos requisitos e obrigações legais em matéria de proteção e privacidade dos dados?	0	-		-	

4.1.4 Grupo #4: Cooperação

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
15 – Estabelecer uma parceria público-privada (PPP)	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	É de uma forma geral entendido que as PPP contribuem para aumentar o nível de cibersegurança no país através de diferentes meios? Por exemplo, partilha de interesses no crescimento da indústria de cibersegurança, cooperação na criação de um quadro regulamentar de cibersegurança relevante, promoção da I&D...	1	Dispõe de um plano de ação nacional para criar PPP?	1	Criou parcerias público-privadas nacionais?	1	Criou PPP intersectoriais?	1	Dependendo das mais recentes evoluções tecnológicas e regulamentares, está em condições de adaptar ou criar PPP?	1
	2	-		Estabelece uma base jurídica ou contratual (leis específicas, acordos de confidencialidade, propriedade intelectual) para definir a esfera de ação das PPP?	1	Criou PPP específicas de setores?	1	Nas PPP criadas, também se concentra na cooperação público-público e privado-privado?	1		
	3	-		-		Concede financiamento para a criação de PPP?	1	Promove PPP entre as pequenas e médias empresas (PME)?	1	-	
	4	-		-		As instituições públicas assumem a liderança das PPP de um modo geral? Ou seja, um ponto de contacto único do setor público que governa e coordena a PPP, organismos públicos acordam previamente o que pretendem alcançar, orientações claras das administrações públicas sobre as suas necessidades e limitações para o setor privado...	1	Mede os resultados das PPP?	1	-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
15 – Estabelecer uma parceria público-privada (PPP)	5	-		-		É membro da parceria público-privada contratual da Organização Europeia de Cibersegurança (ECSO) (PPPc)?	0	-		-	
	6	-		-		Dispõe de uma ou várias PPP a trabalharem em atividades da CSIRT?	0	-		-	
	7					Dispõe de uma ou várias PPP a trabalharem em questões de proteção das infraestruturas críticas da informação?	0				
	8	-		-		Dispõe de uma ou várias PPP a trabalharem na sensibilização para a cibersegurança e o desenvolvimento de competências?	0	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
16 – Institucionalizar cooperação entre agências públicas	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Dispõe de canais de cooperação informais entre agências públicas?	1	Dispõe de um sistema de cooperação nacional que incida sobra a cibersegurança? Por exemplo, conselhos consultivos, grupos diretores, fóruns, conselhos, cibercentros ou grupos de reunião de peritos	1	As autoridades públicas participam no sistema de cooperação?	1	Assegura que existem, pelo menos, entre os seguintes organismos público canais de cooperação dedicados à cibersegurança: serviços de informações, autoridades nacionais de aplicação da lei, autoridades judiciais, intervenientes governamentais, CSIRT e o exército?	1	São prestadas às agências públicas informações mínimas uniformizadas sobre as evoluções mais recentes do cenário de ameaças e o conhecimento da situação em matéria de cibersegurança?	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
16 – Institucionalizar cooperação entre agências públicas	2	-		-		Criou plataformas de cooperação para o intercâmbio de informações?	1	Mede os sucessos e limites dos diferentes sistemas de cooperação na promoção de uma cooperação eficaz?	1	-	
	3	-		-		Definiu o âmbito de plataformas de cooperação (por exemplo, funções e responsabilidades, número de domínios problemáticos)?	1	-		-	
	4	-		-		Realiza reuniões anuais?	1	-		-	
	5	-		-		Dispõe de mecanismos de cooperação entre autoridades competentes nas regiões geográficas? Por exemplo, rede de correspondentes de segurança por região, responsável pela cibersegurança nas câmaras económicas regionais...	1	-		-	

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
17 – Colaborar na cooperação internacional (não apenas com os EM da UE)	a	O objetivo encontra-se abrangido na sua ENC atual ou planeia abrangê-lo na próxima edição?	1	Existem práticas ou atividades informais que contribuem para alcançar o objetivo de uma forma não coordenada?	1	Tem um plano de ação que esteja formalmente definido e documentado?	1	Revê o seu plano de ação relativamente ao objetivo para testar o seu desempenho?	1	Dispõe de mecanismos para assegurar que o plano de ação é dinamicamente adaptado às evoluções do ambiente?	1
	b			Definiu resultados pretendidos, princípios orientadores ou principais atividades do seu plano de ação?	1	Tem um plano de ação com uma afetação de recursos e governação claras?	1	Revê o seu plano de ação relativamente ao objetivo para garantir que é corretamente priorizado e otimizado?	1		
	c			Se pertinente, o seu plano de ação está implementado e já é eficaz num âmbito limitado?	0						
	1	Dispõe de uma estratégia de envolvimento internacional?	1	Dispõe de acordos de cooperação com outros países (bilaterais, multilaterais) ou parceiros noutros países? Por exemplo, partilha de informações, criação de capacidades, assistência...	1	Procede ao intercâmbio de informações a nível estratégico? Por exemplo, política de alto nível, perceção de riscos...	1	As agências públicas de cibersegurança nacionais no seu país estão envolvidas em sistemas de cooperação internacional?	1	Lidera discussões sobre um ou vários tópicos no âmbito de acordos multilaterais?	1

Objetivo da ENC	#	Nível 1	R	Nível 2	R	Nível 3	R	Nível 4	R	Nível 5	R
17 – Colaborar na cooperação internacional (não apenas com os EM da UE)	2	Dispõe de canais de cooperação informais com outros países?	1	Dispõe de um ponto de contacto único que possa exercer uma função de ligação para garantir a cooperação transfronteiriça com autoridades dos Estados-Membros (grupo de cooperação, rede de CSIRT...)?	1	Procede ao intercâmbio de informações a nível tático? Por exemplo, boletim de autores de ameaças, centros de partilha e análise de informações, terceiros de confiança...	1	Avalia, regularmente, os resultados das iniciativas de cooperação internacional?	1	Lidera discussões sobre um ou vários tópicos no âmbito de tratados ou convenções internacionais?	1
	3	A liderança pública manifestou intenção de colaborar na cooperação internacional no domínio da cibersegurança?	1	Tem pessoas dedicadas envolvidas na cooperação internacional?	1	Procede ao intercâmbio de informações a nível operacional? Por exemplo, informação de coordenação operacional, incidentes contínuos, OIC...	1	-		Lidera discussões ou negociações num ou vários tópicos em grupos de peritos internacionais? Por exemplo, Comissão Mundial sobre a Estabilidade do Ciberespaço (GCSC), Grupo de Cooperação SRI da ENISA, Grupo de Peritos Estatais da ONU sobre a Segurança da Informação (GGE)...	1
	4	-		-		Colabora em exercícios de cibersegurança internacionais?	1	-		-	
	5	-		-		Colabora em atividades de criação de capacidades internacionais? Por exemplo, formações, desenvolvimento de competências, elaboração de procedimentos normalizados...	0	-		-	
	6	-		-		Estabeleceu acordos de assistência mútua com outros países? Por exemplo, atividades dos SAL, processos judiciais, mutualização de capacidades de resposta a incidentes, partilha de ativos de cibersegurança...	0	-		-	
	7	-		-		Assinou ou ratificou tratados ou convenções internacionais no domínio da cibersegurança? Por exemplo, Código de Conduta Internacional para a Segurança da Informação, Convenção sobre o Cibercrime	0	-		-	

4.2 ORIENTAÇÕES PARA A UTILIZAÇÃO DO QUADRO

Esta secção visa prestar aos Estados-Membros algumas orientações e recomendações para implementar o quadro ou preencher o questionário. As recomendações enunciadas a seguir resultam essencialmente do retorno de informação recolhido a partir das entrevistas com os representantes dos Estados-Membros:

- **Antecipar atividades de coordenação para recolher dados e consolidar dados.** A maioria dos Estados-Membros reconhece que a realização de um tal exercício de autoavaliação deverá implicar cerca de 15 pessoas-dia. A fim de realizar a autoavaliação, será necessário solicitar um vasto conjunto de partes interessadas. Por conseguinte, recomenda-se destinar tempo à fase de preparação para identificar todas as partes interessadas nos organismos governamentais, nas agências públicas e no setor privado.
- **Identificar um organismo central responsável pela realização da autoavaliação a nível nacional.** Uma vez que a recolha de material para todos os indicadores do QACN poderá envolver muitas partes interessadas, recomenda-se ter um organismo ou agência central encarregado da realização da autoavaliação assegurando a ligação e a coordenação com todas as partes interessadas relevantes.
- **Utilizar o exercício de avaliação como forma para partilhar e comunicar sobre tópicos de cibersegurança.** Os ensinamentos extraídos partilhados pelos Estados-Membros revelaram que as discussões (na forma de entrevistas individuais ou seminários coletivos) constituem uma boa oportunidade para promover o diálogo em torno de tópicos de cibersegurança e partilhar visões e áreas comuns de melhoria. Além de elucidar sobre os principais avanços, a partilha de resultados pode também ajudar a promover tópicos de cibersegurança.
- **Utilizar a ENC como uma oportunidade para selecionar os objetivos sujeitos à avaliação.** Os 17 objetivos que compõem o QACN foram criados com base nos objetivos comummente abrangidos pelos Estados-Membros nas suas ENC. Os objetivos abrangidos como parte da ENC deverão ser usados como um meio para definir a esfera de ação da avaliação. Contudo, a ENC não deverá limitar a avaliação. Dado que o QACN incide naturalmente sobre prioridades, certos domínios são propositadamente omitidos do mesmo. No entanto, não implica que uma determinada capacidade não esteja presente. Por exemplo, no caso em que um objetivo específico é omitido do QACN, mas o país dispõe de capacidades em matéria de cibersegurança relacionadas com esse objetivo, a avaliação desse objetivo pode ser realizada.
- **Quando o âmbito da ENC evolui, garantir que a interpretação da pontuação continua a ser consistente com a evolução da ENC.** O ciclo de vida da ENC trata-se de um processo plurianual. As ENC de alguns Estados-Membros são normalmente executadas com um roteiro de 3 a 5 anos com alterações do âmbito entre duas edições sucessivas da ENC. Nessa perspetiva, há que ter especial cuidado ao apresentar os resultados da autoavaliação entre duas edições da ENC: as alterações ao âmbito poderão de facto afetar a pontuação da maturidade final. Recomenda-se comparar as pontuações relativas ao âmbito completo de objetivos estratégicos de um ano para outro (ou seja, pontuação total global).

Chamada de atenção sobre o mecanismo de pontuação - exemplo sobre o rácio de cobertura

O mecanismo de pontuação inclui dois níveis de pontuações:
(i) um **rácio de cobertura geral global** com base na lista completa de objetivos estratégicos presentes no quadro de autoavaliação; e
(ii) um **rácio de cobertura específico global** com base nos objetivos estratégicos selecionados pelo Estado-Membro (normalmente correspondendo aos objetivos presentes na ENC do país específico).

Por conceção (ver a secção 3.1 sobre o mecanismo de pontuação), o rácio de cobertura específico geral será igual ou superior ao rácio de cobertura geral global, dado que o último pode incluir objetivos que não são abrangidos pelo Estado-Membro, baixando, assim, o rácio de cobertura geral global. Quando um Estado-Membro adita um objetivo, o rácio de cobertura global aumentará (ou seja, mais indicadores de maturidade abrangidos), ao passo que a maturidade específica global pode diminuir (caso um objetivo recém-adicionado esteja numa fase incipiente e, portanto, tem um nível baixo de maturidade).

- **Ao preencher o questionário de autoavaliação, ter presente que o objetivo principal é apoiar os Estados-Membros na criação de capacidades em matéria de cibersegurança.** Por conseguinte, ao preencher a autoavaliação, apesar de em algumas situações poder ser difícil responder a uma pergunta de forma definitiva, recomenda-se escolher a resposta mais geralmente aceite. Se, por exemplo, a resposta a uma pergunta for SIM sobre um determinado âmbito mas for NÃO sobre outro âmbito, os Estados-Membros devem ter presente que uma resposta NÃO exige uma ação; um plano de reparação ou um plano para atuar sobre uma área de melhoria que deverá ser considerada em desenvolvimentos futuros.

5. PRÓXIMAS ETAPAS

5.1 MELHORIAS FUTURAS

Durante as entrevistas com representantes dos Estados-Membros e durante a fase de investigação documental, identificaram-se igualmente como evoluções futuras potenciais as seguintes recomendações para melhorar o atual Quadro de Avaliação das Capacidades Nacionais:

- **Desenvolver um sistema de pontuação que permita mais exatidão.** Por exemplo, poderia ser introduzida uma percentagem da cobertura em vez da resposta binária SIM/NÃO, a fim de ter devidamente em conta a complexidade de consolidar as capacidades a nível nacional. Como primeiro passo, optou-se por uma abordagem simples de respostas SIM/NÃO.
- **Introduzir métricas quantitativas para medir a eficácia da ENC dos Estados-Membros.** Com efeito, o Quadro de Avaliação das Capacidades Nacionais incide sobre a avaliação do nível de maturidade das capacidades em matéria de cibersegurança dos Estados-Membros. Tal poderá ser complementado com métricas para medir a eficácia das atividades e dos planos de ação implementados pelos Estados-Membros para criar essas capacidades. Não se afigurou realista criar essas métricas de eficácia na fase atual dado que há: pouco retorno de informação do terreno, dificuldade em encontrar indicadores significativos que liguem resultados à implementação da ENC e dificuldade em criar indicadores realistas que possam ser subsequentemente recolhidos. No entanto, continua a ser um tópico para trabalho futuro.
- **Transição de um exercício de autoavaliação para uma abordagem de avaliação.** Uma potencial evolução futura do quadro poderá passar pela transição para uma abordagem de avaliação, a fim de avaliar a maturidade das capacidades em matéria de cibersegurança dos Estados-Membros de um modo mais consistente. Ter um terceiro a realizar a avaliação poderá de facto permitir minimizar o potencial enviesamento.

ANEXO A – PANORÂMICA DOS RESULTADOS DA INVESTIGAÇÃO DOCUMENTAL

O anexo A apresenta uma síntese do trabalho anterior da ENISA sobre a ENC e uma análise dos modelos de maturidade publicamente disponíveis sobre capacidade em matéria de cibersegurança. Os pressupostos que se seguem são tidos em conta para a seleção e análise dos modelos:

- Nem todos os modelos são baseados numa metodologia de investigação rigorosa;
- A estrutura e os resultados dos modelos nem sempre são inteiramente explicados com ligações claras entre os diferentes elementos que caracterizam cada modelo;
- Alguns modelos não oferecem pormenores sobre o processo de desenvolvimento, a estrutura e a metodologia de avaliação;
- Outros modelos e instrumentos que encontrámos não oferecem quaisquer pormenores no tocante à estrutura e ao conteúdo, pelo que não são listados; e
- A seleção dos modelos para análise baseia-se na cobertura geográfica. O foco principal incidirá sobre modelos de maturidade sobre capacidade em matéria de cibersegurança criada para avaliar o desempenho dos países europeus. Todavia, é importante expandir a cobertura geográfica para analisar boas práticas na criação de modelos de maturidade em todo o mundo.

Esta análise sistemática de modelos de maturidade relevantes disponíveis publicamente sobre capacidade em matéria de cibersegurança foi realizada utilizando um quadro de análise adaptado com base na metodologia definida por Becker para a elaboração de modelos de maturidade[22]. Para cada modelo de maturidade existente foram analisados os seguintes elementos:

- **Nome do modelo de maturidade:** O nome do modelo de maturidade e as principais referências;
- **Instituição fonte:** A instituição, pública ou privada, responsável pela conceção do modelo;
- **Finalidade geral e alvo:** O âmbito global do modelo e o(s) alvo(s) visado(s);
- **Número e definição de níveis:** O número de níveis de maturidade do modelo e a respetiva descrição geral;
- **Número e nome dos atributos:** O número e nome de atributos utilizados pelo modelo de maturidade. A análise dos atributos tem um triplo objetivo:
  - Subdividir o modelo de maturidade em secções facilmente compreensíveis;
  - Agregar vários atributos em grupos de atributos que satisfaçam o mesmo objetivo; e
  - Proporcionar diferentes pontos de vista do tema do nível de maturidade.
- **Método de avaliação:** O método de avaliação do modelo de maturidade;

[22] J. Becker, R. Knackstedt eJ. Pöppelbuß, «Developing Maturity Models for IT Management: A Procedure Model and its Application,» Business & Information Systems Engineering, vol. 1, n.º 3, p. 213–222, junho de 2009.

- **Representação dos resultados**: Definir o método de visualização dos resultados do modelo de maturidade. A lógica subjacente a esta etapa é a de que os modelos de maturidade têm tendência a falhar se forem demasiado complexos e, portanto, o modo de representação deve satisfazer necessidades práticas.

Trabalho anterior sobre ENC

A ENISA publicou dois documentos sobre o tópico da ENC em 2012 enquanto parte dos seus esforços iniciais. Em primeiro lugar, o «Practical guide on the development and execution phase of NCSS»[23] propôs um conjunto de ações concretas para a implementação eficiente de uma ENC e apresenta o ciclo de vida de uma ENC em quatro etapas: desenvolvimento da estratégia, execução da estratégica, avaliação da estratégia e manutenção da estratégia. Em segundo lugar, um documento intitulado «Setting the course for national efforts to strengthen security in cyberspace»[24] descreveu o estudo das estratégias de cibersegurança dentro e fora da UE em 2012 e propôs que os Estados-Membros deveriam determinar temas comuns e diferenças entre as suas ENC.

Em 2014, foi publicado o primeiro quadro da ENISA para avaliar a ENC de um Estado-Membro[25]. Este quadro contém recomendações e boas práticas, bem como um conjunto de instrumentos de criação de capacidades para avaliar uma ENC (por exemplo, objetivos identificados, entradas, saídas, indicadores-chave de desempenho...). Esses instrumentos são adaptados às necessidades diversas dos países em diferentes níveis de maturidade no respetivo planeamento estratégico. No mesmo ano, a ENISA publicou o «Online NCSS Interactive Map»[26], que permite aos utilizadores consultarem rapidamente a ENC de todos os Estados-Membros e países da EFTA, incluindo os seus objetivos estratégicos e bons exemplos de implementação. Desenvolvido inicialmente como um repositório de ENC (2014), foi atualizado com exemplos de implementação em 2018 e, desde 2019, o mapa atua como um *polo de informação* para centralizar dados prestados pelos Estados-Membros sobre os seus esforços destinados ao reforço da cibersegurança nacional.

Publicado em 2016, o «NCSS Good Practice Guide»[27] identifica quinze objetivos estratégicos. Este guia analisa a o estado de implementação da ENC de cada Estado-Membro e identifica várias lacunas e desafios no atinente a esta implementação.

Em 2018, a ENISA publicou depois a «National Cybersecurity Strategies Evaluation Tool»[28]: uma ferramenta de autoavaliação interativa para ajudar os Estados-Membros a avaliarem as suas prioridades e objetivos estratégicos relacionados com a sua ENC. Através de um conjunto de perguntas simples, esta ferramenta proporciona aos Estados-Membros recomendações específicas para a implementação de cada objetivo. Por último, o «Good practices in innovation on Cybersecurity under the NCSS»[29] publicado em 2019 apresente o tema da inovação na cibersegurança no âmbito da ENC. O documento estabelece desafios e boas práticas nas

[23] «NCSS: Practical Guide on Development and Execution» (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] «NCSS: Setting the course for national efforts to strengthen security in cyberspace» (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] «An evaluation framework for NCSS» (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] «National Cybersecurity Strategies - Interactive Map» (ENISA, 2014, atualizado em 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Este documento atualiza o guia de 2012: «NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies» (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] «National Cybersecurity Strategies Evaluation Tool» (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

diferentes dimensões da inovação, conforme percecionados por peritos na matéria, a fim de ajudar a elaborar futuros objetivos estratégicos inovadores.

A.1 Modelo de Maturidade da Capacitação de Cibersegurança para as Nações (CMM)

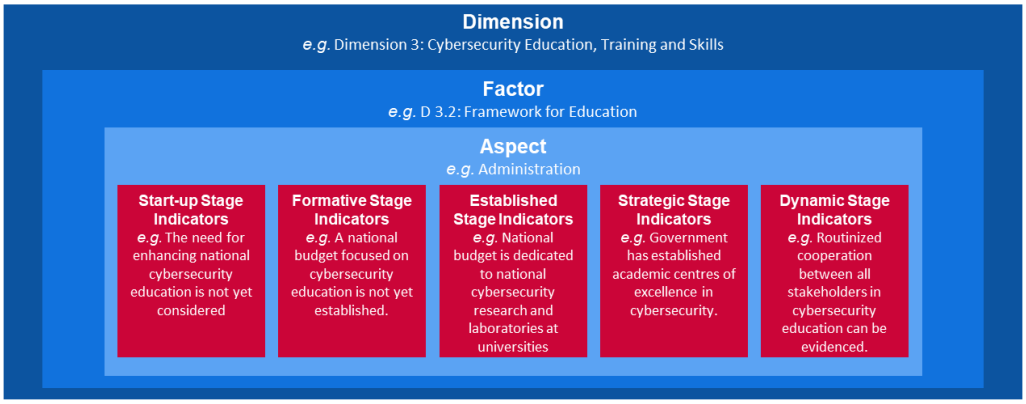
O Modelo de Maturidade da Capacitação de Cibersegurança para as Nações (CMM) foi desenvolvido pelo Global Cyber Security Capacity Centre (Centro de Capacidade), parte da Oxford Martin School na Universidade de Oxford. O objetivo do Centro de Capacidade é aumentar a escala e a eficácia da criação de capacidades de cibersegurança, no Reino Unido e internacionalmente, através da implementação de um Modelo de Maturidade da Capacitação de Cibersegurança (CMM). O CMM está diretamente direcionado para países que pretendam aumentar a sua capacidade nacional em matéria de cibersegurança. Implementado inicialmente em 2014, o CMM foi revisto em 2016 na sequência da sua utilização na análise de 11 capacidades em matéria de cibersegurança nacionais.

Atributos/Dimensões

O CMM considera que a capacidade em matéria de cibersegurança inclui **cinco dimensões** que representam os grupos de capacidade em matéria de cibersegurança. Cada grupo representa uma «objetiva» de investigação diferente através da qual a capacidade em matéria de cibersegurança pode ser estudada e compreendida. Nas cinco dimensões, **fatores** descrevem os pormenores de possuir capacidade em matéria de cibersegurança. Esses pormenores são elementos que contribuem para o reforço da maturidade da capacidade em matéria de cibersegurança em cada dimensão. Para cada fator, vários **aspetos** representam diferentes componentes do fator. Os aspetos representam um método organizacional para dividir indicadores em grupos mais pequenos que são mais fáceis de compreender. Cada aspeto é depois avaliado através de **indicadores** para descrever as etapas, ações, ou elementos constitutivos que são indicativos de um estádio específico de maturidade (definido na secção seguinte) com um aspeto, fator e dimensão distintos.

Os termos mencionados anteriormente podem ser estratificados como mostrado na figura a seguir.

Figura 4: Exemplo de indicadores do CMM



Dimension
e.g. Dimension 3: Cybersecurity Education, Training and Skills
Factor
e.g. D 3.2: Framework for Education
Aspect
e.g. Administration

Start-up Stage Indicators
e.g. The for enhancing national cybersecurity education is not yet considered

Formative Stage Indictors
e.g. A national budget focused on cybersecurity education is not yet established

Dimensão
p. ex. dimensão 3: Educação, Formação e Competências para a Cibersegurança
Fator
p. ex. D 3.2: Quadro para Educação
Aspeto
p. ex. administração
Indicadores de Fase de Arranque
p. ex. ainda não foi considerada a necessidade de melhorar a educação para a cibersegurança.
Indicadores de Fase Formativa
p. ex. ainda não está criado um orçamento nacional concentrado na educação para a cibersegurança.

Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced. Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indicadores de Fase Estabelecida p. ex. é dedicado orçamento, a nível nacional, a investigação no domínio da cibersegurança e laboratórios em universidades. Indicadores de Fase Estratégica p. ex. o governo criou centros académicos de excelência no domínio da cibersegurança. Indicadores de Fase Dinâmica p. ex. é possível demonstrar a cooperação rotineira entre todas as partes interessadas no domínio da educação para a cibersegurança.

As cinco dimensões são especificadas a seguir:

i Dividir a política e estratégia de cibersegurança (6 fatores);
ii Encorajar uma cultura de cibersegurança responsável na sociedade (5 fatores);
iii Desenvolver conhecimentos em matéria de cibersegurança (3 fatores);
iv Criar quadros jurídicos e regulamentares eficazes (3 fatores); e
v Controlar os riscos através de normas, organizações e tecnologias (7 fatores).

Níveis de maturidade

O CMM usa **5 níveis de maturidade** para determinar em que medida um país registou progressos em relação a um determinado fator/aspeto de capacidade em matéria de cibersegurança. Estes níveis servem de retrato da capacidade em matéria de cibersegurança existente:

- **Arranque**: Nesta fase, não existe maturidade em matéria de cibersegurança, ou tem um caráter muito embrionário. Poderão existir discussões iniciais sobre criação de capacidades em matéria de cibersegurança, mas não foram adotadas ações concretas. Há uma ausência de dados observáveis nesta fase;
- **Formativa**: Algumas características dos aspetos começaram a crescer e a serem formuladas, mas podem ser *ad hoc*, desorganizadas, definidas deficientemente ou simplesmente «novas». Contudo, os dados desta atividade podem ser claramente demonstrados;
- **Estabelecida**: Os elementos do aspeto estão criados e a funcionar. Não há, porém, uma consideração bem planeada da afetação relativa de recursos. Há pouca tomada de decisões de compromisso no que diz respeito ao investimento «relativo» nos vários elementos do aspeto. No entanto, o aspeto está funcional e definido;
- **Estratégica**: Foram feitas escolhas sobre que partes do aspeto são importantes e quais são menos importantes para a organização ou nação em causa. A fase estratégica reflete o facto de que estas escolhas foram feitas, subordinadas às circunstâncias específicas da nação ou organização; e
- **Dinâmica**: Nesta fase, existem mecanismos claros para alterar a estratégia dependendo das circunstâncias prevalecentes, tais como a tecnologia do ambiente de ameaças, conflito mundial ou uma mudança significativa num domínio de preocupação (por exemplo, cibercriminalidade ou privacidade). Organizações dinâmicas desenvolveram métodos para alterar estratégias a passos largos. Tomada de decisões célere, reafectação de recursos e atenção constante ao ambiente em mutação são características desta fase.

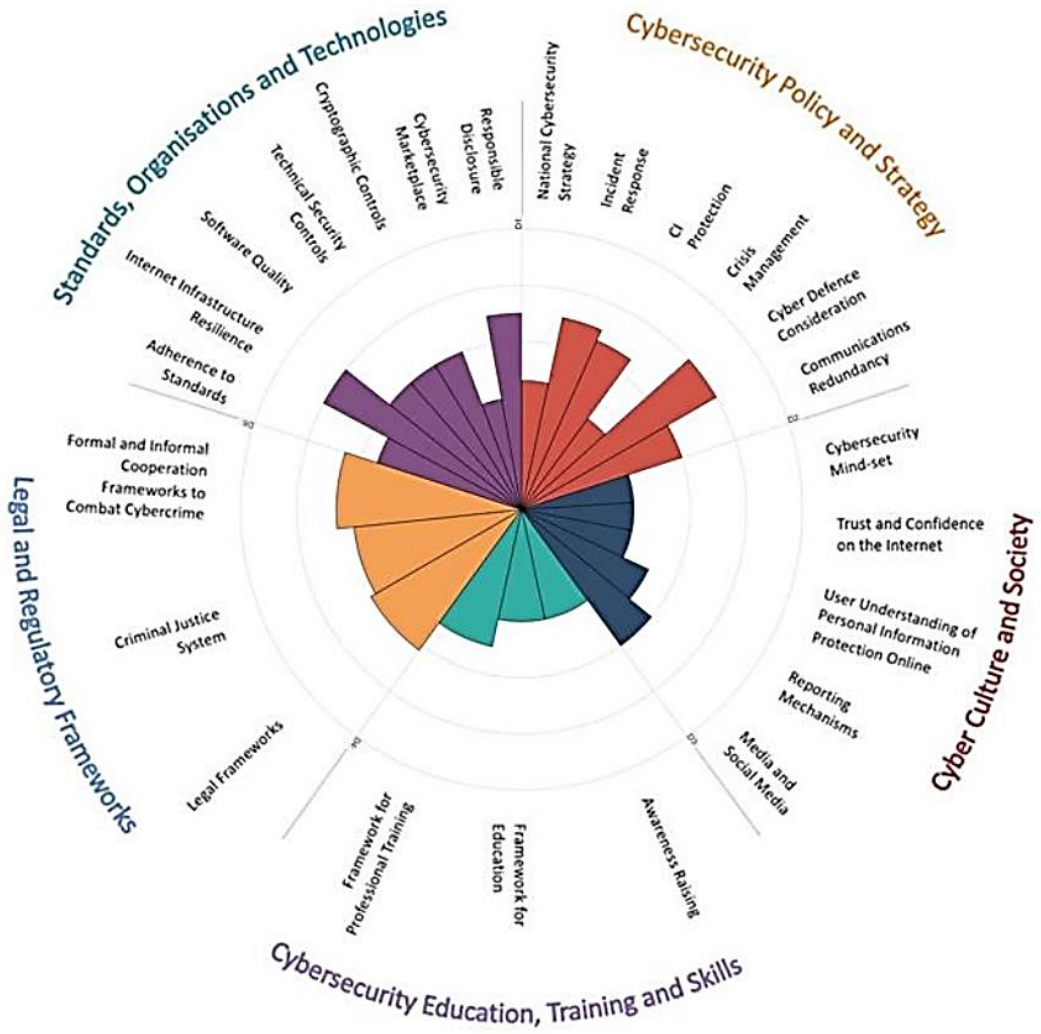
Método de avaliação

Uma vez que o Centro de Capacidade não possui uma compreensão sólida e aprofundada de cada contexto doméstico no qual o modelo é implementado, colabora com organizações internacionais, acolhe ministérios ou organizações no respetivo país para analisar a maturidade da capacidade em matéria de cibersegurança. A fim de avaliar o nível de maturidade das cinco dimensões incluídas no CMM, o Centro de Capacidade e a organização anfitriã reúnem-se com as partes interessadas nacionais dos setores público e privado ao longo de dois ou três dias para realizar grupos de reflexão sobre as dimensões do CMM. Cada dimensão é debatida, pelo menos, duas vezes por diferentes grupos de partes interessadas. Tal constitui o conjunto preliminar de dados para a avaliação subsequente.

Modo ou representação dos resultados

O CMM oferece uma panorâmica do nível de maturidade de cada país através de um radar composto por cinco secções, uma para cada dimensão. Cada dimensão representa um quinto do gráfico, com cinco fases de maturidade para cada fator que se estendem a partir do exterior do centro do gráfico; conforme mostrado abaixo, «arranque» está mais próximo do centro do gráfico e «dinâmica» está no perímetro.

Figura 5 CMM: Panorâmica de resultados



Standards, Organisations and Technologies	Normas, organizações e tecnologias
Legal Regulatory Frameworks	Quadros regulamentares e jurídicos
Cybersecurity Education, Training and Skills	Educação, Formação e Competências para a Cibersegurança
Cybersecurity Policy and Strategy	Política e estratégia de cibersegurança
Cyber Culture and Society	Cibercultura e sociedade
Responsible Disclosure	Divulgação responsável
Cybersecurity market place	Mercado de cibersegurança
Cryptographic Controls	Controlos criptográficos
Technical Security Controls	Controlos de segurança técnica
Software Quality	Qualidade do *software*
Internet Infrastructure Resilience	Resiliência das infraestruturas de Internet
Adherence to Standards	Adesão a normas

Formal and Informal Cooperation Frameworks to Combat Cybercrime	Quadros de cooperação formal e informal para combater a cibercriminalidade
Criminal Justice System	Sistema de justiça penal
Legal Frameworks	Quadros jurídicos
Framework for Professional Training	Quadro para formação profissional
Framework for Education	Quadro para educação
Awareness Raising	Sensibilização
Media and Social Medai	Meios de comunicação social e redes sociais
Reporting Mechanisms	Mecanismos de comunicação
User Understanding of Personal Information Protection Online	Compreensão do utilizador da proteção de informações pessoais em linha
Trust and Confidence on the Internet	Confiança na Internet
Cybersecurity Mind-set	Mentalidade orientada para a cibersegurança
Communications Redundancy	Redundância das comunicações
Cyber Defence Consideration	Consideração da ciberdefesa
Crisis Management	Gestão de crises
CI Protection	Proteção de IC
Incident Response	Resposta a incidentes
National Cybersecurity Strategy	Estratégia Nacional de Cibersegurança

Global Cyber Security Capacity Centre Oxford Martin School, Universidade de Oxford, 2017.

A.2 Modelo de Maturidade da Capacitação de Cibersegurança (C2M2)

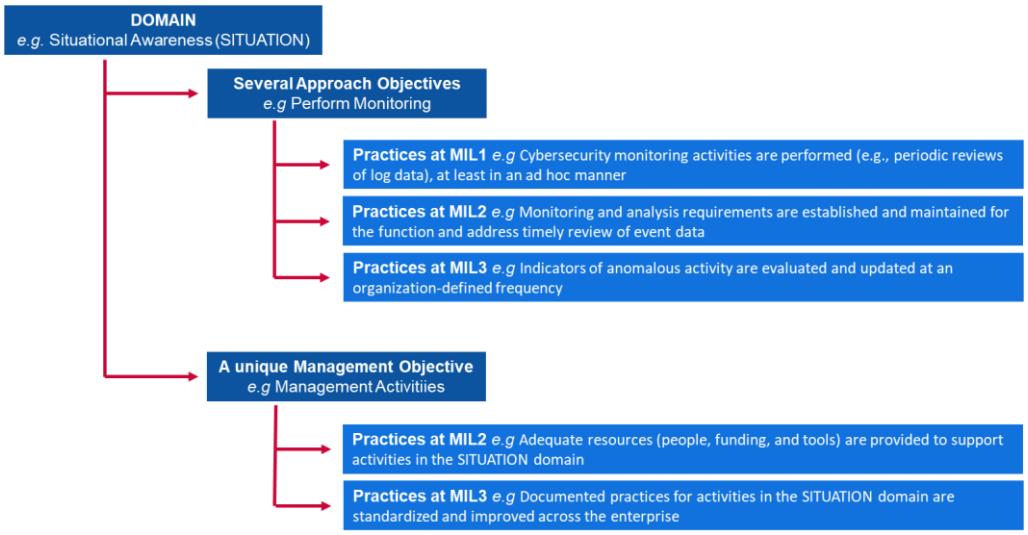
O Modelo de Maturidade da Capacitação de Cibersegurança (C2M2) foi desenvolvido pelo Departamento da Energia dos EUA em colaboração com peritos do setor privado e público. O objetivo do Centro de Capacidade é ajudar as organizações de todos os setores, tipos e dimensões a avaliarem e fazerem melhorias aos seus programas de cibersegurança e reforçar a sua resiliência operacional. O C2M2 concentra-se na implementação e gestão de práticas de cibersegurança associadas à informação, às tecnologias da informação (TI) e aos ativos da tecnologia das operações (TO) e aos ambientes nos quais opera. O C2M2 define modelos de maturidade como: «um conjunto de características, atributos, indicadores, ou padrões que representam capacidade e progressão numa disciplina específica». Inicialmente implementado em 2014, o C2M2 foi revisto em 2019.

Atributos/Dimensões

O C2M2 considera **dez domínios** que representam um agrupamento lógico de práticas em matéria de cibersegurança. Cada conjunto de práticas representa as atividades que uma organização pode realizar para criar e amadurecer capacidade no domínio. Cada domínio é depois associado a um **objetivo de gestão** único e a **vários objetivos de abordagem**. Nos objetivos de abordagem e de gestão, **várias práticas** são especificadas para descrever atividades institucionalizadas.

A relação entre estas noções é sintetizada a seguir:

Figura 6: Exemplo de indicador do C2M2



Domain eg Situational Awareness (SITUATION)	**Domínio** p. ex. Conhecimento da situação (SITUAÇÃO)
Several Approaches Objectives e.g. Perform Monitoring	**Vários Objetivos de Abordagens** p. ex. Realizar Monitorização
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Práticas em NIM1** por exemplo, são realizadas atividades de monitorização da cibersegurança (por exemplo, análises periódicas de dados de registo), pelo menos de um modo *ad hoc*
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Práticas em NIM2** por exemplo, são estabelecidos e mantidos requisitos de monitorização e análise para o funcionamento e abordar a revisão oportuna de dados de eventos
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Práticas em NIM3** por exemplo, são avaliados e atualizados indicadores de atividade anómala numa frequência definida pela organização
A unique Management Objectve e.g. Management Activities	Um Objetivo de Gestão único p. ex. Atividades de Gestão
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Práticas em NIM2** por exemplo, são prestados recursos adequados (pessoas, financiamento e instrumentos) para apoiar atividades no domínio SITUAÇÃO
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Práticas em NIM3** por exemplo, são normalizadas e melhoradas práticas documentadas no domínio SITUAÇÃO na empresa

Os dez domínios são especificados a seguir:

i Gestão de riscos (RISCO);
ii Gestão de ativos, mudança e configuração (ATIVOS);
iii Gestão de identidades e acessos (ACESSO);
iv Gestão de ameaças e vulnerabilidades (AMEAÇAS);
v Conhecimento da situação (SITUAÇÃO);
vi Resposta a eventos e incidentes (RESPOSTA);
vii Gestão da cadeia de abastecimento e das dependências externas (DEPENDÊNCIAS);
viii Gestão da mão-de-obra (MÃO-DE-OBRA);
ix Arquitetura de cibersegurança (ARQUITETURA); e
x Gestão de programa de cibersegurança (PROGRAMA).

Níveis de maturidade

O C2M2 usa **quatro níveis de maturidade** (designados Níveis de Indicador de Maturidade - NIM) para determinar uma progressão dupla de maturidade: uma progressão da abordagem e uma progressão da gestão. Os NIM variam de NIM0 a NIM3 e destinam-se a ser aplicados de forma independente a cada domínio.

- **NIM0**: Não são realizadas práticas.
- **NIM1**: São realizadas práticas iniciais, mas podem ser *ad hoc*.
- **NIM2**: Características de gestão:
  - As práticas estão documentadas;
  - São prestados recursos adequados para apoiar o processo;
  - O pessoal que realiza as práticas possui competências e conhecimento adequados; e

- São atribuídas responsabilidade e autoridade para a realização das práticas.

Característica de abordagem:

- As práticas são mais completas ou avançadas do que no NIM1.

- **NIM3**: Características de gestão:
  - As atividades são orientadas por políticas (ou outras diretivas organizacionais);
  - São estabelecidos e monitorizados objetivos de desempenho para atividades do domínio para acompanhar as realizações; e
  - São normalizadas e melhoradas práticas documentadas para atividades do domínio na empresa.

  Característica de abordagem:
  - As práticas são mais completas ou avançadas do que no NIM2.

Método de avaliação

O C2M2 está concebido para utilização com uma **metodologia de avaliação** e conjunto de instrumentos (disponível mediante pedido) para uma organização medir e melhorar o seu programa de cibersegurança. É possível realizar num dia uma autoavaliação utilizando o conjunto de instrumentos, mas o conjunto de instrumentos poderá ser adaptado para um esforço de avaliação mais rigoroso. Adicionalmente, o C2M2 pode ser usado para orientar a elaboração de um novo programa de cibersegurança.

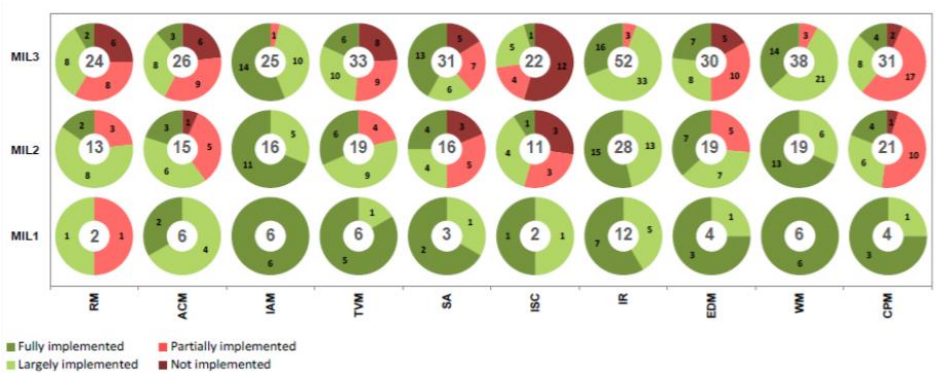
O conteúdo do modelo é apresentado com um elevado nível de abstração, para que possa ser interpretado pelas organizações de vários tipos, estruturas, dimensões e indústrias. A ampla utilização do modelo por um setor pode apoiar a avaliação comparativa das capacidades em matéria de cibersegurança do setor.

Modo ou representação dos resultados

O C2M2 oferece um Relatório de Pontuação da Avaliação gerado a partir dos resultados do inquérito. O relatório apresenta os resultados em duas visões: a visão do Objetivo, que mostra respostas a perguntas relacionadas com a prática por cada domínio e respetivos objetivos, e a visão do Domínio, que mostra respostas por todos os domínios e NIM. Ambas as visões são baseadas num sistema de representação caracterizado por gráficos circulares (ou «donuts»), um por resposta, e um mecanismo de pontuação por sistema de semáforo. Como mostrado na Figura 7, os setores a vermelho num gráfico circular mostram uma contagem do número de perguntas que receberam respostas ao inquérito de «Não implementado» (vermelho-escuro) ou «Parcialmente implementado» (vermelho-claro). Os setores a verde mostram o número de perguntas que receberam respostas de «Amplamente implementado» (verde-claro) ou «Totalmente implementado» (verde-escuro).

A Figura 7 abaixo é um exemplo de um cartão de pontuação no fim de uma avaliação da maturidade. No eixo X estão os dez domínios do C2M2 e no eixo Y os níveis de maturidade (NIM). Olhando para o gráfico e considerando o domínio de Gestão de riscos (GR), é possível notar três gráficos circulares, um correspondendo a cada nível de maturidade NIM1, NIM2 e NIM3. Em relação ao domínio GR, o gráfico salienta que existem dois itens a serem avaliados para alcançar o primeiro nível de maturidade, NIM1. Neste caso, uma pontuação «Amplamente implementado» e uma pontuação «Parcialmente implementado». Em relação ao segundo nível de maturidade, NIM2, o modelo prevê 13 itens para serem avaliados. Dois desses 13 itens pertencem ao primeiro nível, NIM1, e 11 ao segundo nível, NIM2. O mesmo se aplica em relação ao terceiro nível, NIM3.

Figura 7: C2M2 – Exemplo de visão de domínio



Fully implemented	Totalmente implementado
Largely implemented	Amplamente implementado
Partially implemented	Parcialmente implementado
Not implemented	Não implementado
MIL1	NIM1
MIL2	NIM2
MIL3	NIM3
RM	RM
ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Fonte: Departamento da Energia dos EUA, Gabinete do fornecimento de eletricidade e da fiabilidade da energia, 2015.

A.3 Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas

O Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas foi desenvolvido no Instituto Nacional de Normas e Tecnologia (NIST). Incide sobre orientar atividades de cibersegurança e gerir riscos no seio de uma organização. Destina-se a todos os tipos de organizações, independentemente da dimensão, grau de risco em matéria de cibersegurança, ou sofisticação de cibersegurança. Uma vez que se trata de um quadro e não de um modelo, é criado de forma distinta dos modelos analisados anteriormente.

O quadro consiste em três partes: o Núcleo do Quadro, os Patamares de Implementação e o os Perfis do Quadro:

- O **Núcleo do Quadro** é um conjunto de atividades em matéria de cibersegurança, resultados pretendidos e referências aplicáveis que são comuns nos setores de infraestruturas críticas. São similares aos atributos ou dimensões encontrados nos modelos de maturidade da capacidade.
- Os **Patamares de Implementação do Quadro** (Patamares) fornecem contexto sobre como uma organização visualiza o risco em matéria de cibersegurança e os processos criados para gerir esse risco. Variando de Parcial (Patamar 1) a Adaptativo (Patamar 4), os Patamares descrevem um grau crescente de rigor e sofisticação em práticas de gestão de riscos em matéria de cibersegurança. Os patamares não representam níveis de maturidade, ao invés, destinam-se a apoiar a tomada de decisões organizacionais sobre como gerir riscos em matéria de cibersegurança, bem como que dimensões da organização têm prioridade mais alta e poderão receber recursos adicionais.
- Um **Perfil do Quadro** («Perfil») representa os resultados com base em necessidades comerciais que uma organização selecionou das Categorias e Subcategorias do Quadro. O Perfil pode ser caracterizado no que diz respeito ao alinhamento de normas, orientações e práticas com o Núcleo do Quadro num cenário de implementação específico. Os perfis podem ser utilizados para identificar

oportunidades para melhorar a postura em matéria de cibersegurança comparando o perfil «Atual» (o estado «tal como está») com o perfil «Alvo» (o estado «a alcançar»).

Núcleo do Quadro

O Núcleo do Quadro consiste em cinco **Funções**. Quando consideradas em conjunto, as Funções fornecem uma visão estratégia de alto nível do ciclo de vida da gestão de uma organização dos riscos em matéria de cibersegurança. O Núcleo do Quadro identifica **Categorias** e **Subcategorias** principais subjacentes para cada Função e relaciona-as com exemplos de Referências Informativas, tais como normas, orientações e práticas existentes para cada Subcategoria.

As Funções e Categorias são especificadas a seguir:

i **Identificar**: Desenvolver uma compreensão organizacional sobre como gerir riscos de cibersegurança para sistemas, pessoas, ativos, dados e capacidades.
- Subcategorias: Gestão de Ativos; Ambiente Empresarial; Governação; Avaliação dos Riscos; e Estratégia de Gestão dos Riscos

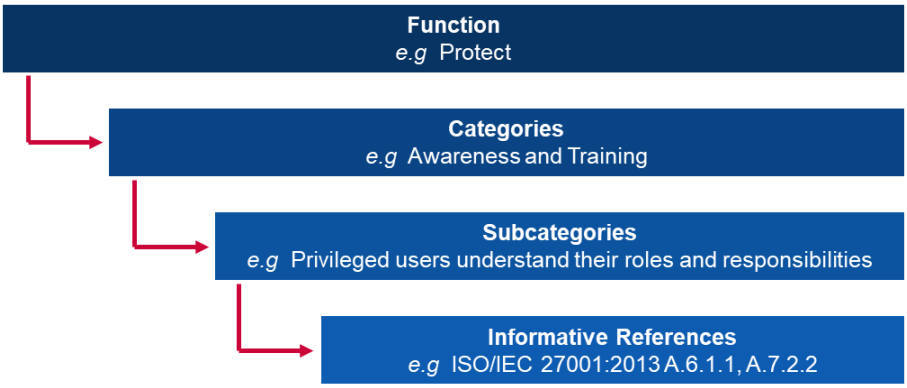
ii **Proteger**: Desenvolver e implementar salvaguardas apropriadas para garantir a prestação de serviços críticos.
- Subcategorias: Gestão de Identidade e Controlo do Acesso; Sensibilização e Formação; Segurança dos Dados; Processos e Procedimentos de Proteção da Informação; Manutenção; e Tecnologia de Proteção

iii **Detetar**: Desenvolver e implementar atividades apropriadas para identificar a ocorrência de um evento de cibersegurança.
- Subcategorias: Anomalias e Eventos; Monitorização Contínua da Segurança; e Processos de Deteção.

iv **Responder**: Desenvolver e implementar atividades apropriadas para adotar medidas relativamente a um incidente de cibersegurança detetado.
- Subcategorias: Planeamento da Resposta; Comunicações, Análises; Mitigação; e Melhorias.

v **Recuperar**: Desenvolver e implementar atividades apropriadas para manter planos para resiliência e para restaurar quaisquer capacidades ou serviços que foram afetados devido a um incidente de cibersegurança.
- Subcategorias: Planeamento da Recuperação; Melhorias; e Comunicações

Figura 8: Exemplo de Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas



Function e.g Project	**Função** p. ex. Projeto
Categories e.g Awarness and Training	**Categorias** p. ex. Sensibilização e Formação
Subcategories e.g Privileged useres understand their roles and responsibilities	**Subcategorias** p. ex. Utilizadores privilegiados compreendem as suas funções e responsabilidades
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Referências Informativas** p. ex. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Patamares

O Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas assenta em **4 Patamares**, cada um dos quais definidos em três eixos: Processo de Gestão de Riscos, Programa de Gestão de Riscos Integrado e Participação Externa. Os Patamares não devem ser considerados níveis de maturidade, mas um quadro para proporcionar às organizações uma contextualização das suas visões de risco de cibersegurança e os processos criados para gerir esse risco.

- **Patamar 1: Parcial**
  - **Processo de Gestão do Risco**: não estão formalizadas práticas organizacionais de gestão de riscos de cibersegurança e o risco é gerido de uma forma *ad hoc* e por vezes reativa;
  - **Programa de Gestão de Riscos Integrado**: existe pouca sensibilização para o risco de cibersegurança a nível organizacional. A organização implementa gestão de riscos de cibersegurança numa base irregular, caso a caso, e pode não ter processos que permitam partilhar informações de cibersegurança dentro da organização;
  - **Participação Externa**: a organização não compreende a sua função no ecossistema mais geral no que diz respeito às suas dependências ou dependentes. A organização não está de um modo geral ciente dos ciberriscos da cadeia de abastecimento dos produtos e serviços que presta e que utiliza;
- **Patamar 2: Informado sobre os riscos**
  - **Processo de Gestão de Riscos**: são aprovadas práticas de gestão de riscos pela direção, mas podem não estar estabelecidas como uma política à escala organizacional;
  - **Programa de Gestão de Riscos Integrado**: existe um conhecimento do risco de cibersegurança a nível organizacional, mas não foi estabelecidas uma abordagem à escala da organização para gerir o risco de cibersegurança. A avaliação do ciberrisco de ativos organizacionais e externos ocorre, mas não é normalmente repetível ou recorrente;
  - **Participação Externa**: de um modo geral, a organização compreende a sua função no ecossistema mais geral no que diz respeito às suas próprias dependências ou dependentes, mas não ambos. Além disso, a organização está ciente dos ciberriscos da cadeia de abastecimento associados aos produtos e serviços que presta, mas não atua de forma consistente ou formal sobre esses riscos;
- **Patamar 3: Repetível**
  - **Processo de Gestão de Riscos**: as práticas de gestão de riscos da organização estão formalmente aprovadas e expressas como política. As práticas de cibersegurança organizacionais são regularmente atualizadas com base na aplicação de processos de gestão de riscos a mudanças nos requisitos de atividade/missão e num cenário de tecnologia e ameaças em mutação;
  - **Programa de Gestão de Riscos Integrado**: existe uma abordagem à escala da organização para gerir o risco de cibersegurança. Políticas, processos e procedimentos baseados no conhecimento dos riscos são definidos, implementados como previsto e revistos. Os quadros superiores garantem a consideração da cibersegurança através de todas as linhas de operação na organização;
  - **Participação Externa**: a organização compreende a sua função, dependências e dependentes no ecossistema geral e pode contribuir para uma compreensão mais ampla dos riscos por parte da comunidade. A organização está ciente dos ciberriscos da cadeia de abastecimento dos produtos e serviços que presta e que utiliza;
- **Patamar 4: Adaptativo**
  - **Processo de Gestão de Riscos**: a organização adapta as suas práticas de cibersegurança com base em atividades de cibersegurança anteriores e atuais, incluindo ensinamentos extraídos e indicadores preditivos;
  - **Programa de Gestão de Riscos Integrado**: existe uma abordagem à escala da organização para gerir o risco de cibersegurança que utiliza políticas, processos e

procedimentos baseados no conhecimento dos riscos para resolver potenciais eventos de cibersegurança; e
- **Participação Externa**: a organização compreende a sua função, dependências e dependentes no ecossistema geral e contribui para uma compreensão mais ampla dos riscos por parte da comunidade.

Método de avaliação

O Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas destina-se a organizações para autoavaliarem o seu risco, a fim de tornar a sua abordagem e investimentos de cibersegurança mais racionais, eficazes e úteis. Para examinar a eficácia dos investimentos, uma organização deve, em primeiro lugar, ter uma compreensão clara dos seus objetivos organizacionais, a relação entre esses objetivos e resultados em matéria de cibersegurança favoráveis. Os resultados em matéria de cibersegurança do Núcleo do Quadro apoiam a autoavaliação da eficácia do investimento e das atividades em matéria de cibersegurança.

A.4 Modelo de Maturidade da Capacitação de Cibersegurança Catar (Q-C2M2)

O Modelo de Maturidade da Capacitação de Cibersegurança Catar (Q-C2M2) foi desenvolvido pela Faculdade de Direito da Universidade de Catar em 2018. O Q-C2M2 baseia-se em vários modelos existentes para criar uma metodologia de avaliação abrangente destinada a reforçar o quadro de cibersegurança do Catar.

Atributos/Dimensões

O Q-C2M2 adota as abordagem do Quadro do Instituto Nacional de Normas e Tecnologia (NIST) de usar cinco funções essenciais como os principais domínios do modelo. As cinco funções essenciais são aplicáveis ao contexto catariano por serem comuns em setores de infraestruturas críticas, um elemento importante no quadro de cibersegurança catariano. O Q-C2M2 baseia-se em **cinco domínios**, cada domínio é depois dividido em vários **subdomínios** para abranger o conjunto completo de maturidade de capacidade em matéria de cibersegurança.

Os cinco domínios são especificados a seguir:

i. O **domínio Compreender** inclui quatro subdomínios: Cibergovernação, Ativos, Riscos e Formação;
ii. Os subdomínios no **domínio Proteger** incluem Segurança dos Dados, Segurança da Tecnologia, Segurança do Controlo do Acesso, Segurança das Comunicações e Segurança do Pessoal;
iii. O **domínio Expor** inclui os subdomínios da Monitorização, Gestão de Incidentes, Deteção, Análise e Exposição;
iv. O **domínio Responder** inclui Planeamento da Resposta, Mitigação e Comunicação de Resposta; e
v. O **domínio Sustentar** inclui Planeamento da Recuperação, Gestão da Continuidade, Melhoria e Dependências Externas.

Níveis de maturidade

O Q-C2M2 usa **cinco níveis de maturidade** que medem a maturidade da capacidade de uma entidade pública ou uma organização não pública ao nível da função essencial. Esses níveis destinam-se a avaliar a maturidade nos cinco domínios especificados na secção anterior.

- **Inicial**: Emprega práticas e processos de cibersegurança *ad hoc* ao abrigo de alguns dos domínios;
- **Em implementação**: Políticas adotadas para implementar todas as atividades em matéria de cibersegurança ao abrigo dos domínios com o propósito de concluir a implementação num determinado período;

- **Em desenvolvimento**: Políticas e práticas implementadas para desenvolver e melhorar atividades em matéria de cibersegurança ao abrigo dos domínios com o objetivo de sugerir novas atividades a implementar;
- **Adaptativo**: Revisita e revê atividades em matéria de cibersegurança e adota práticas baseadas em indicadores preditivos resultantes de experiências e medições anteriores; e
- **Ágil**: Continua a exercer a fase adaptativa com uma ênfase adicional na agilidade e rapidez aquando da implementação de atividades nos domínios.

Método de avaliação

O Q-C2M2 encontra-se numa fase incipiente de investigação e ainda não está criado para implementação. Trata-se de um quadro que poderá ser usado para implementar um modelo de avaliação pormenorizado para organizações catarianas no futuro.

A.5 Certificação do Modelo de Maturidade da Cibersegurança (CMMC)

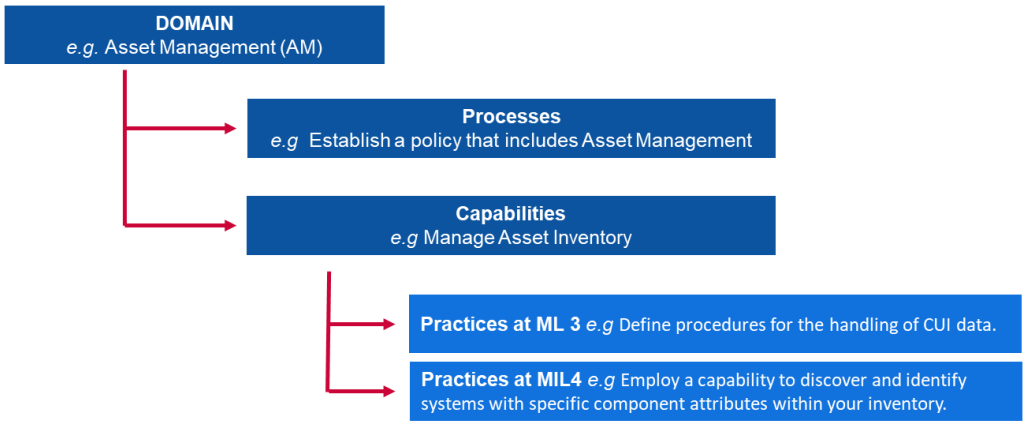
A Certificação do Modelo de Maturidade da Cibersegurança (CMMC) foi desenvolvida pelo Departamento da Defesa (DdD) dos EUA em colaboração com a Universidade Carnegie Mellon e o Laboratório de Física Aplicada da Universidade Johns Hopkins. O principal objetivo do DdD na conceção deste modelo é proteger as informações do setor da Base Industrial de Defesa (BID). As informações visadas pelo CMMC estão classificadas como «Informações Contratuais Federais», informações prestadas ou geradas pelo Governo ao abrigo de contratos não destinadas a divulgação pública, ou «Informações Não Classificadas Controladas», informações que requerem controlos de salvaguarda ou de divulgação nos termos da legislação, regulamentação e políticas a nível do governo e consistente com as mesmas. O CMMC mede a maturidade em matéria de cibersegurança e presta boas práticas juntamente com um elemento de certificação para garantir a implementação de práticas associadas a cada nível de maturidade. A versão mais recente do CMMC foi publicada em 2020.

Atributos/Dimensões

O CMMC considera **dezassete domínios** que representam grupos de processos e capacidades em matéria de cibersegurança. Cada domínio é depois decomposto em vários **processos** que são similares entre domínios; e uma a várias **capacidades** que abrangem cinco níveis de maturidade. As capacidades (ou capacidade) são depois detalhadas em **práticas** para cada nível de maturidade relevante.

A relação entre estas noções é a seguinte:

Figura 9: Exemplo de indicadores do CMMC



DOMAIN e.g. Asset Management (AM)	**DOMÍNIO** p. ex. Gestão de Ativos (GA)

Processes e.g Establish a policy that includes Asset Management	**Processos** p. ex. Estabelecer uma política que inclua a Gestão de Ativos
Capabilities e.g Manage Asset Inventory	**Capacidades** p. ex. Gerir o Inventário de Ativos
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Práticas no NIM 3** p. ex. Definir procedimentos para o tratamento de dados de informações não classificadas controladas (CUI)
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Práticas no NIM 4** p. ex. Utilizar uma capacidade para descobrir e identificar sistemas com atributos de componente específicos no inventário

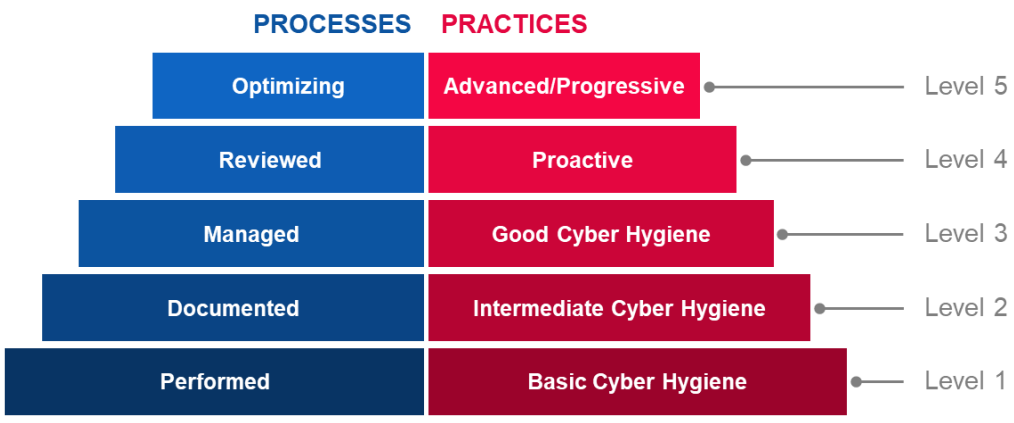
Os dezassete domínios são especificados a seguir:

i Controlo do acesso (CA);
ii Gestão de Ativos (GA);
iii Auditoria e Prestação de Contas (APC);
iv Sensibilização e Formação (SF);
v Gestão da Configuração (GC);
vi Identificação e Autenticação (IA);
vii Resposta a Incidentes (RI);
viii Manutenção (MA);
ix Proteção dos Meios (PM);
x Segurança do Pessoal (SP);
xi Proteção Física (PF);
xii Recuperação (RE);
xiii Gestão de Riscos (GR);
xiv Avaliação da Segurança (CA);
xv Conhecimento da Situação (CS);
xvi Proteção do Sistema e das Comunicações (SC); e
xvii Integridade do Sistema e da Informação (SI).

Níveis de maturidade

O CMMC utiliza **5 níveis de maturidade** definidos com base em processos e práticas. Para alcançar um determinado nível de maturidade no CMMC, uma organização tem de satisfazer os pré-requisitos para os processos e as práticas para esse nível. Tal implica igualmente satisfazer os pré-requisitos de todos os níveis abaixo desse.

Figura 10: Níveis de maturidade do CMMC



PROCESSES	PROCESSOS
Optimizing	Otimizar
Reviewed	Revistos
Managed	Geridos
Documented	Documentados
Performed	Realizados
PRACTICES	PRÁTICAS
Advanced/Progressive	Avançadas/Progressivas
Proactive	Proativas
Good Cyber Hygiene	Boa Ciber-higiene
Intermediate Cyber Hygiene	Ciber-higiene Intermédia
Basic Cyber Hygiene	Ciber-higiene Básica
Level 5	Nível 5
Level 4	Nível 4
Level 3	Nível 3
Level 2	Nível 2
Level 1	Nível 1

- **Nível 1**
  - **Processos – Realizados**: porque a organização apenas pode realizar estas práticas de uma forma *ad hoc* e pode ou não apoiar-se em documentação. A maturidade do processo não é avaliada para o Nível 1;
  - **Práticas – Ciber-higiene Básica**: o nível 1 incide sobre a proteção de ICF (Informações Contratuais Federais) e consiste apenas em práticas que correspondem aos requisitos de salvaguarda básicos;
- **Nível 2**
  - **Processos – Documentados**: o nível 2 requer que uma organização estabeleça e documente práticas e políticas para orientar a implementação dos seus esforços em matéria de CMMC. A documentação de práticas permite que as pessoas as executem de um modo repetível. As organizações desenvolvem capacidades maduras documentando os respetivos processos e exercendo-as conforme documentado;
  - **Práticas – Ciber-higiene Intermédia**: o nível 2 serve como uma progressão do Nível 1 para o Nível 3 e consiste num subconjunto de requisitos de segurança especificados na NIST SP 800-171, bem como em práticas de outras normas e referências;
- **Nível 3**
  - **Processos – Geridos**: o nível 3 requer que uma organização estabeleça, mantenha e atribua os recursos a um plano que demonstre a gestão de atividades para implementação de práticas. O plano pode incluir informações sobre missões, objetivos, planos de projetos, atribuição de recursos, formação necessária e envolvimento de partes interessadas relevantes;
  - **Práticas – Boa Ciber-higiene**: o nível 3 incide sobre a proteção de CUI e engloba todos os requisitos de segurança especificados na NIST SP 800-171, bem como práticas adicionais de outras normas e referências para mitigar ameaças;
- **Nível 4**
  - **Processos – Revistos**: o nível 4 requer que uma organização reveja e meça práticas em relação à eficácia. Além de medir práticas em relação à eficácia, as organizações neste nível são capazes de tomar medidas corretivas quando necessário e informar a direção de alto nível sobre o estado ou problemas de uma forma recorrente;
  - **Práticas – Proativas**: o nível 4 incide sobre a proteção de CUI (Informações Não Classificadas Controladas) e engloba um subconjunto dos requisitos de

segurança reforçados. Estas práticas melhoram as capacidades de deteção e resposta de uma organização para fazer face e adaptar-se às táticas, técnicas e procedimentos em mutação;

- **Nível 5**
  - **Processos – Otimização**: o nível 5 requer que uma organização normalize e otimize a implementação de processos na organização; e
  - **Práticas – Avançadas/Proativas**: o nível 5 incide sobre a proteção de CUI. As práticas adicionais aumentam a profundidade e a sofisticação das capacidades em matéria de cibersegurança.

Método de avaliação

O CMMC é um modelo relativamente jovem, concluído no primeiro trimestre de 2020. Por enquanto, não foi implementado em nenhuma organização. Todavia, os contratantes do DdD esperam alcançar examinadores terceiros certificados para realizarem auditorias. O DdD espera que os seus contratantes implementem boas práticas para promover a cibersegurança e a proteção de informações sensíveis.

A.6 O Modelo Comunitário de Maturidade em matéria de Cibersegurança (CCSMM)

O Modelo Comunitário de Maturidade em matéria de Cibersegurança (CCSMM) foi desenvolvido pelo Centro para a Garantia e Segurança de Infraestruturas da Universidade do Texas. O objetivo do CCSMM é definir melhor métodos para determinar o estado atual de uma comunidade na sua preparação no domínio da cibersegurança e proporcionar um roteiro para as comunidades seguirem nos seus esforços de preparação. As comunidades visadas pelo CCSMM são essencialmente administrações locais ou estaduais. O CCSMM foi concebido em 2007.

Atributos/Dimensões

Os níveis de maturidade são definidos seguindo **6 dimensões principais** que abrangem os diferentes aspetos da cibersegurança nas comunidades e organizações. Essas dimensões são claramente definidas para cada nível de maturidade (especificado na Figura 11: Síntese das dimensões **do** CCSMM). As 6 dimensões são:

i Ameaças Combatidas;
ii Métricas;
iii Partilha de Informações;
iv Tecnologia;
v Formação; e
vi Teste.

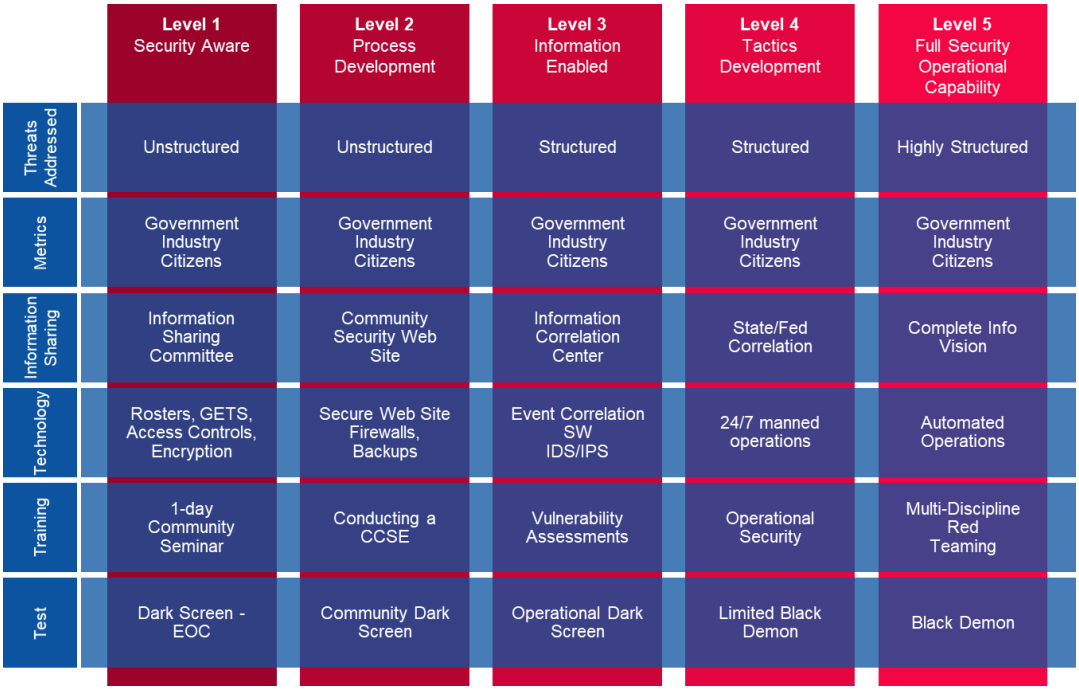
Níveis de maturidade

O CCSMM assenta em **5 níveis de maturidade** com base nos principais tipos de ameaças e atividades abordadas no nível:

- **Nível 1: Conscientização para a Segurança**
  O tema principal de atividades neste nível é sensibilizar as pessoas e organizações para as ameaças, problemas e questões relacionados com a cibersegurança;
- **Nível 2: Desenvolvimento de Processos**
  Nível concebido para ajudar as comunidades a criarem e melhorarem processos de segurança necessários para resolver eficazmente problemas de cibersegurança;
- **Nível 3: Possibilitado pelas Informações**
  Concebido para melhorar os mecanismos de partilha de informações na comunidade a fim de permitir à comunidade correlacionar eficazmente elementos de informação supostamente díspares.

- **Nível 4: Desenvolvimento de Táticas**
  Os elementos deste nível estão concebidos para desenvolver métodos melhores e mais proativos para detetar e responder a ataques. Neste nível, a maioria dos métodos de prevenção devem estar implementados.
- **Nível 5: Capacidade Operacional de Segurança Plena**
  Este nível representa os elementos que devem estar implementados para qualquer organização se considerar plenamente preparada operacionalmente para combater qualquer tipo de ciberameaça.

Figura 11: Síntese das dimensões do CCSMM por nível



Level 1 Security Aware	Nível 1 Conscientização para a Segurança
Level 2 Process Development	Nível 2 Desenvolvimento de Processos
Level 3 Information Enabled	Nível 3 Possibilitado pelas Informações
Level 4 Tactics Development	Nível 4 Desenvolvimento de Táticas
Level 5 Full Security Operational Capability	Nível 5 Capacidade Operacional de Segurança Plena
Threats Addressed	Ameaças Combatidas
Metrics	Métricas
Information sharing	Partilha de informações
Technology	Tecnologia
Training	Formação
Test	Teste
Unstructured	Não estruturado
Governement Industry Citizens	Governo Indústria Cidadãos
Information Sharing Committee	Comité de Partilha de Informações
Rosters, GETS, Assess Controls, Encryption	Listas, GETS, Controlos de Acesso, Encriptação
1-dat Community Seminar	Seminário para a comunidade de 1 dia
Dark Screen – EOC	Ecrã Negro - EOC
Unstructured	Não estruturado
Governement Industry Citizens	Governo Indústria Cidadãos

Community Security Web site	Sítio Web de Segurança da Comunidade
Secure Web Site Firewalls, Backups	Barreiras de segurança, Cópias de segurança de Sítio Web seguro
Conudcting a CCSE	Realização de um CCSE
Community Dark Screen	Community Dark Screen
Structured	Estruturado
Governement Industry Citizens	Governo Indústria Cidadãos
Information Correlation Center	Centro de Correlação de Informações
Event Correlation SW IDS/IPS	Correlação de Evento SW IDS/IPS
Vulnerability Assessment	Avaliação da Vulnerabilidade
Operational Dark Screen	Operational Dark Screen
Structured	Estruturado
Governement Industry Citizens	Governo Indústria Cidadãos
State/Fed Correlation	Correlação Estado/Fed
24/7 manned operations	Operações providas de pessoal 24/7
Operational Security	Segurança Operacional
Limited Black Demon	Limited Black Demon
Highly Structured	Altamente estruturado
Complete Info Vision	Visão completa das informações
Automated Operations	Operações automatizadas
Multi-Discipline Red Teaming	Red teaming multidisciplinar
Black Demon	Black Demon

Método de avaliação

O CCSMM enquanto uma metodologia de avaliação destina-se a ser implementado pelas comunidades com contributos de agências de aplicação da lei estaduais e federais. Visa ajudar a comunidade a definir o que é mais importante, quais os alvos mais prováveis e o que precisa ser protegido (e em que grau). Com esses objetivos em mente, podem ser elaborados planos para trazer cada aspeto da comunidade para o respetivo nível necessário de maturidade de cibersegurança. As informações específicas geradas pelo CCSMM ajudam a definir os objetivos dos vários testes e exercícios que podem ser usados para medir a eficácia de programas criados.

A.7 Modelo de maturidade da segurança da informação para o Quadro de cibersegurança do Instituto Nacional de Normas e Tecnologia (NIST) (ISMM)

O Modelo de Maturidade da Segurança da Informação (ISMM) foi desenvolvido na Faculdade de Ciências e Engenharia da Computação da Universidade King Fahd de Petróleo e Minerais na Arábia Saudita. Propõe um novo modelo de maturidade da capacidade para medir a implementação de medidas de cibersegurança. O objetivo do ISMM é permitir às organizações medir o seu progresso em matéria de implementação ao longo do tempo usando a mesma ferramenta de medição regularmente para garantir que a postura de segurança pretendida é mantida. O ISMM foi desenvolvido em 2017.

Atributos/Dimensões

O ISMM tem por base os domínios existentes avaliados do quadro NIST e acrescenta uma dimensão sobre avaliação da conformidade. Tal confere ao modelo **23 domínios avaliados** em relação à postura de segurança de uma organização. Os 23 domínios avaliados são:

i Gestão de Ativos;
ii Ambiente Empresarial;
iii Governação;
iv Avaliação dos Riscos;
v Estratégia de Gestão de Riscos;
vi Avaliação da Conformidade;
vii Controlo do Acesso;
viii Sensibilização e Formação;
ix Segurança dos Dados;
x Processos e Procedimentos de Proteção da Informação;
xi Manutenção;
xii Tecnologia de Proteção;
xiii Anomalias e Eventos;
xiv Monitorização Contínua da Segurança;
xv Processos de Deteção;
xvi Planeamento da Resposta;
xvii Comunicações de Resposta;
xviii Análise da Resposta;
xix Mitigação;
xx Melhorias da Resposta;
xxi Plano de Recuperação;
xxii Melhorias da Recuperação; e
xxiii Comunicações da Recuperação.

Níveis de maturidade

O ISMM assenta em **5 níveis de maturidade**, os quais, infelizmente, não estão especificados na documentação disponível.

- **Nível 1:** Processo Realizado;
- **Nível 2:** Processo Gerido;
- **nível 3:** Processo Estabelecido;
- **nível 4:** Processo Previsível; e
- **Nível 5:** Processo de Otimização.

Método de avaliação

O ISMM não propõe nenhuma metodologia específica para realizar a avaliação para organizações.

A.8 Modelo de Capacidade de Auditoria Interna (IA-CM) para o Setor Público

O Modelo de Capacidade de Auditoria Interna (IA-CM) foi desenvolvido pelo «Institute of Internal Auditors Research Foundation» com o intuito de criar capacidades e apoio através da autoavaliação no setor público. Destinado aos profissionais de auditoria, o IA-CM proporciona uma panorâmica do próprio modelo juntamente com um Guia de Aplicação para prestar assistência na utilização do modelo enquanto uma ferramenta de autoavaliação.

Apesar de o IA-CM estar concentrado na capacidade de Auditoria Interna, em vez da criação de capacidades em matéria de cibersegurança, o modelo está criado como uma ferramenta de autoavaliação destinada a entidades do setor público que pode ser aplicada globalmente para melhorar os processos e a eficácia. Uma vez que o âmbito não incide sobre a cibersegurança, os atributos não será analisados. O IA-CM foi concluído em 2009.

Níveis de maturidade

O Modelo de Capacidade de Auditoria Interna (IA-CM) inclui **5 níveis de maturidade**, cada um dos quais descreve as características e capacidades de uma atividade de Auditoria Interna

nesse nível. Os níveis de capacidade do modelo proporcionam um roteiro para melhoria contínua.

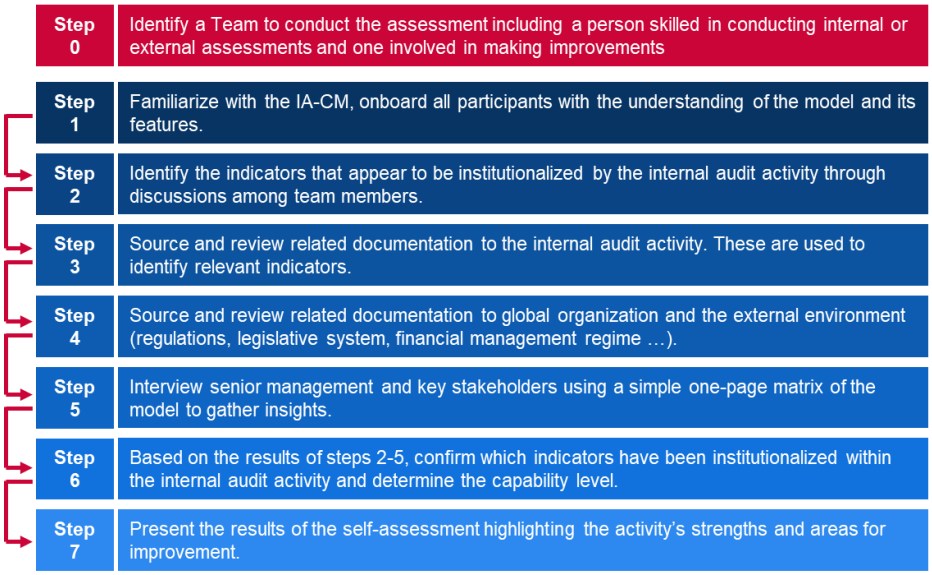
- **Nível 1: Inicial**
  Capacidades não sustentáveis, repetíveis – dependentes de esforços individuais
  - *Ad hoc* ou não estruturadas.
  - Auditorias únicas isoladas ou exames de documentos e transações relativamente à exatidão e conformidade.
  - Resultados dependentes das competências da pessoa específica no exercício do cargo.
  - Não há práticas profissionais estabelecidas além das prestadas por associações profissionais.
  - Aprovação de financiamento pela direção, consoante necessário.
  - Ausência de infraestruturas.
  - Auditores provavelmente parte de uma unidade organizacional maior.
  - Não está desenvolvida capacidade institucional.
- **Nível 2: Infraestruturas**
  Práticas e procedimentos sustentáveis e repetíveis
  - A principal questão ou desafio para o Nível 2 é como criar e manter a repetibilidade de processos e, assim, uma capacidade repetível.
  - Estão a ser criadas relações de relatório de auditoria interna, infraestruturas de gestão e administrativas e práticas e processos profissionais (orientação, processos e procedimentos de auditoria interna).
  - Planeamento de auditoria principalmente baseado nas prioridades de gestão.
  - Confiança continuada essencialmente nas aptidões e competências de pessoas específicas.
  - Conformidade parcial com as normas.
- **Nível 3: Integrado**
  Práticas de gestão e profissionais uniformemente aplicadas
  - Políticas, processos e procedimentos de auditoria interna estão definidos, documentados e integrados uns nos outros e na infraestrutura da organização.
  - Encontram-se bem estabelecidas práticas profissionais e de gestão de auditoria interna e são uniformemente aplicadas na atividade de auditoria interna.
  - A auditoria interna começa a alinhar-se com a atividade da organização e os riscos que enfrenta.
  - A auditoria interna evolui de realizar apenas auditoria interna tradicional para se integrar como agente de colaboração prestando aconselhamento sobre desempenho e gestão de riscos.
  - A tónica está na formação de equipas e na capacidade da atividade de auditoria interna e a sua independência e objetividade.
  - Conformidade de um modo geral com as normas.
- **Nível 4: Gerido**
  Integra informação na organização para melhorar a governação e a gestão de riscos
  - A auditoria interna e as expectativas das principais partes interessadas estão alinhadas.
  - As métricas de desempenho estão criadas para medir e monitorizar os processos e resultados de auditoria interna.
  - A auditoria interna é reconhecida como proporcionando contribuições significativas à organização.
  - As funções de auditoria interna enquanto parte integrante da governação e gestão de riscos da organização.
  - A auditoria interna é uma unidade de negócio bem gerida.
  - Os riscos são medidos e geridos quantitativamente.
  - As aptidões e competências exigidas estão criadas com capacidade para renovação e partilha de conhecimentos (na auditoria interna e na organização).
- **Nível 5: Otimização**
  Aprender dentro e fora da organização para melhoria contínua
  - A auditoria interna é uma organização de aprendizagem com melhorias e inovação contínuas do processo.

- A auditoria interna usa informações de dentro e fora da organização para contribuir para a consecução de objetivos estratégicos.
- Desempenho de classe mundial/recomendado/de acordo com boas práticas.
- A auditoria interna é uma parte crítica da estrutura de governação da organização.
- Competências especializadas e profissionais de topo.
- As medições do desempenho individual, da unidade e organizacional estão plenamente integradas para
- impulsionar melhorias do desempenho.

Método de avaliação

O Modelo de Capacidade de Auditoria Interna está claramente criado para autoavaliação. Fornece passos pormenorizados a seguir para usar o IA-CM e um conjunto de diapositivos de amostra para adaptar. Antes do início da autoavaliação, deve ser identificada uma equipa específica, incluindo, no mínimo, uma pessoa com competências na realização de avaliações internas ou externas de auditorias internas e uma pessoa que esteja envolvida na introdução de melhorias nesta área.

Figura 12: Etapas de autoavaliação do IC-AM



Step 0	Etapa 0
Step 1	Etapa 1
Step 2	Etapa 2
Step 3	Etapa 3
Step 4	Etapa 4
Step 5	Etapa 5
Step 6	Etapa 6
Step 7	Etapa 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Identificar uma equipa para realizar a avaliação, incluindo uma pessoa com competências na realização de avaliações internas e externas e uma pessoa envolvida na introdução de melhorias.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Familiarizar com o IA-CM, familiarizar todos os participantes com a compreensão do modelo e as suas funcionalidades.

Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Identificar os indicadores que parecem estar institucionalizados pelo atividade de auditoria interna através de debates entre membros da equipa.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Fornecer e rever documentação relacionada à atividade de auditoria interna. Estes são usados para identificar indicadores relevantes.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Fornecer e rever documentação relacionada à organização global e ao ambiente externo (regulamentação, sistema legislativo, regime de gestão financeira...).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Entrevistar a direção de topo e partes interessadas principais usando uma matriz simples de uma página do modelo para recolher opiniões.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Com base nos resultados das etapas 2-5, confirmar que indicadores foram institucionalizados na atividade de auditoria interna e determinar o nível de capacidade.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Apresentar os resultados da autoavaliação salientando os pontos fortes da atividade e áreas para melhoria.

A.9 O Índice Global de Cibersegurança (IGC)

O Índice Global de Cibersegurança (IGC) é uma iniciativa da União Internacional das Telecomunicações (UIT) destinada a analisar o compromisso e a situação em matéria de cibersegurança em todas as regiões da ITU: África, Américas, Estados Árabes, Ásia-Pacífico, CEI e Europa, e coloca em destaque países com elevado compromisso e práticas recomendáveis. O objetivo do IGC é ajudar os países a identificarem áreas para melhoria no domínio da cibersegurança, bem como motivá-los para adotarem medidas destinadas a melhorar a sua classificação ajudando, assim, a aumentar o nível global de cibersegurança em todo o mundo.

Uma vez que o IGC se trata de um índice e não de um modelo de maturidade, não utiliza níveis de maturidade, mas sim uma pontuação para classificar e comparar o compromisso em matéria de cibersegurança global das nações e regiões.

Atributos/Dimensões

O Índice Global de Cibersegurança (IGC) baseia-se nos cinco pilares da Agenda Global para a Cibersegurança (AGC). Esses pilares formam os cinco subíndices do IGC e cada um inclui um conjunto de indicadores. Os cinco pilares e indicadores são os seguintes:

i **Jurídico**: medições com base na existência de instituições e quadros jurídicos que tratam da cibersegurança e da cibercriminalidade.
   - Legislação em matéria de cibercriminalidade;
   - Regulamentação da cibersegurança; e
   - Legislação em matéria de contenção/restrição de *spam*.

ii **Técnico**: Medições com base na existência de instituições e quadros técnicos que tratam da cibersegurança.
   - CERT/CIRT/CSRIT;
   - Quadro de Implementação de Normas;
   - Organismo de Normalização;
   - Mecanismos técnicos e capacidades implementados para combater o *spam*;
   - Utilização da nuvem para efeitos de cibersegurança; e
   - Mecanismos de proteção em linha das crianças.

iii **Organizacional**: Medições com base na existência de instituições de coordenação de políticas e estratégias para o desenvolvimento de cibersegurança a nível nacional.
- Estratégia Nacional de Cibersegurança;
- Agência Responsável; e
- Cibersegurança.

iv **Criação de capacidades**: Medições com base na existência de programas de investigação e desenvolvimento, educação e formação, profissionais certificados e agências do setor público que promovam a criação de capacidades.
- Campanhas de sensibilização do público;
- Quadro para a certificação e acreditação de profissionais de cibersegurança;
- Curso de formação profissional em cibersegurança;
- Programas educativos ou currículos académicos em cibersegurança;
- Programas de I&D em cibersegurança; e
- Mecanismos de incentivo.

v **Cooperação**: Medições com base na existência de parcerias, quadros cooperativos e redes de partilha de informações.
- Acordos bilaterais;
- Acordos multilaterais;
- Participação em fóruns/associações internacionais;
- Parcerias público-privadas;
- Parcerias interagência/intra-agência; e
- Melhores práticas.

Método de avaliação

O IGC é uma ferramenta de autoavaliação criada através de um inquérito[30] de perguntas binárias, pré-codificadas e de resposta aberta. A utilização de respostas binárias elimina a avaliação baseada em opiniões e qualquer eventual enviesamento para certos tipos de resposta. As respostas pré-codificadas poupam tempo e permitem uma análise de dados mais exata. Além disso, uma escala dicotómica simples permite uma avaliação mais célere e mais complexa, uma vez que não requer respostas longas, o que acelera e simplifica o processo de dar respostas e avaliação subsequente. O inquirido deverá apenas confirmar a presença ou falta de certas soluções de cibersegurança pré-identificadas. Um mecanismo de inquérito em linha, que é usado para recolher respostas e carregar material relevante, permite a extração de boas práticas e um conjunto de avaliações qualitativas temáticas por um painel de peritos.

O processo global do IGC é implementado do seguinte modo:

- É enviada uma carta de convite a todos os participantes, informando-os da iniciativa e solicitando um ponto focal responsável pela recolha de todos os dados relevantes e pela realização do questionário IGC em linha. Durante o inquérito em linha, o ponto focal aprovado é oficialmente convidado pela ITU a responder ao questionário;
- Recolha de dados primários (para países que não respondem ao questionário):
  - a ITU elabora um projeto de resposta inicial ao questionário utilizando dados disponíveis publicamente e investigação em linha;
  - O projeto de questionário é enviado para os pontos focais para exame;
  - Os pontos focais melhoram a exatidão e devolvem o projeto de questionário;
  - O projeto de questionário corrigido é enviado para cada ponto focal para aprovação final; e
  - O questionário validado é usado para análise, pontuação e classificação.
- Recolha de dados secundários (para países que respondem ao questionário):
  - A ITU identifica quaisquer respostas, documentos de apoio, hiperligação, etc. em falta;
  - O ponto focal melhora a exatidão das respostas conforme necessário;

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

- O projeto de questionário corrigido é enviado para cada ponto focal para aprovação final; e
- O questionário validado é usado para análise, pontuação e classificação.

A.10 O Índice de Ciberpotência (CPI)

O Índice de Ciberpotência (CPI) foi criado pelo programa de investigação da «Economist Intelligence Unit» patrocinado por Booz Allen Hamilton em 2011. O CPI é um «modelo dinâmico quantitativo e qualitativo, […] que mede atributos específicos do ciberespaço em quatro motores da ciberpotência: quadro jurídico e regulamentar; contexto económico e social; infraestruturas de tecnologia; e aplicação na indústria, que examina o progresso digital em indústrias-chave» [31]. O objetivo do Índice de Ciberpotência é fazer uma avaliação comparativa da capacidade dos países do G20 para suportar ciberataques e implementar as infraestruturas digitais necessárias para uma economia próspera e segura. O valor de referência fornecido pelo CPI incide sobre 19 países do G20 (excluindo a UE). O índice fornece depois uma classificação dos países para cada indicador.

Atributos/Dimensões

O Índice de Ciberpotência (CPI) tem por base quatro motores da ciberpotência. Cada categoria é depois medida através de vários indicadores para atribuir a cada país uma pontuação específica. As categorias e os pilares são os seguintes:

i **Quadro jurídico e regulamentar**
- Compromisso do governo em relação ao ciberdesenvolvimento
- Políticas de proteção contra ciberataques
- Cibercensura (ou falta dela)
- Eficácia política
- Proteção da propriedade intelectual

ii **Contexto económico e social**
- Níveis educacionais
- Competências técnicas
- Abertura do comércio
- Grau de inovação no ambiente empresarial

iii **Infraestruturas de tecnologia**
- Acesso a tecnologias da informação e da comunicação
- Qualidade das tecnologias da informação e da comunicação
- Acessibilidade dos preços das tecnologias da informação e da comunicação
- Despesa em tecnologias da informação
- Número de servidores seguros

iv **Aplicação na indústria**
- Redes inteligentes
- Saúde em linha
- Comércio eletrónico
- Transporte inteligente
- Administração pública em linha

Método de avaliação

O CPI é um modelo de pontuação quantitativo e qualitativo. A avaliação foi realizada pela «The Economist Intelligence Unit» usando indicadores das fontes estatísticas disponíveis e fazendo estimativas quando faltavam dados. As principais fontes usadas são a «Economist Intelligence Unit», a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO); a União Internacional das Telecomunicações (UIT) ; e o Banco Mundial.

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

A.11 O Índice de Ciberpotência (CPI)

Esta secção sintetiza as principais conclusões da análise dos modelos de maturidade existentes. O Quadro 5: Panorâmica dos modelos de **maturidade** analisados fornece uma panorâmica das principais características de cada modelo de acordo com o modelo de Becker modificado. O Quadro 6 Comparação de Níveis de Maturidade as definições de alto nível dos níveis de maturidade dos modelos analisados. O Quadro 7 fornece uma panorâmica das dimensões ou dos atributos usados em cada modelo.

Quadro 5: Panorâmica dos modelos de maturidade analisados

Designação do modelo	Instituição fonte	Finalidade	Alvo	N.º de Níveis	N.º de Atributos	Método de avaliação	Representação dos Resultados
Modelo de Maturidade da Capacitação de Cibersegurança para as Nações (CMM)	Global Cybersecurity Capacity Centre Universidade de Oxford	Aumenta a escala e eficácia da criação de capacidades em matéria de cibersegurança a nível internacional	Países	5	5 dimensões principais	Colaboração com uma organização local para aperfeiçoar o modelo antes de o aplicar ao contexto nacional	Radar de 5 secções
Modelo de Maturidade da Capacitação de Cibersegurança (C2M2)	Departamento da Energia dos EUA (DdE)	Ajuda as organizações a avaliar e fazer melhorias aos seus programas de cibersegurança e a reforçar a sua resiliência operacional	Organizações de todos os setores, tipos e dimensões	4	10 domínios principais	Metodologia de autoavaliação e conjunto de ferramentas	Cartão de pontuação com gráficos circulares
Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas	Instituto Nacional de Normas e Tecnologia (NIST)	Quadro destinado a orientar atividades de cibersegurança e gerir riscos no seio das organizações	Organizações	N/A (4 Patamares)	5 funções principais	Autoavaliação	-
Modelo de Maturidade da Capacitação de Cibersegurança Catar (Q-C2M2)	Faculdade de Direito da Universidade do Catar	Proporcionar um modelo viável que pode ser usado para fazer uma avaliação comparativa, medir e desenvolver o quadro de cibersegurança do Catar	Organizações catarianas	5	5 domínios principais	-	-
Certificação do Modelo de Maturidade da Cibersegurança (CMMC)	Departamento da Defesa dos EUA (DdD)	Promover boas práticas em matéria de cibersegurança para salvaguardar as informações	Organizações do setor da Base Industrial de Defesa (BID)	5	17 domínios principais	Avaliação por auditores externos	-
O Modelo Comunitário de Maturidade em matéria de Cibersegurança (CCSMM)	Centro para a Garantia e Segurança de Infraestruturas da Universidade do Texas	Determinar o estado atual de uma comunidade na sua preparação no domínio da cibersegurança e proporcionar um roteiro para as comunidades seguirem nos seus esforços de preparação	Comunidades (governos locais ou estaduais)	5	6 dimensões principais	Avaliação dentro das comunidades com contributos de agências de aplicação da lei do Estado e federais	-
Modelo de maturidade da segurança da informação para o Quadro de cibersegurança do Instituto Nacional de Normas e Tecnologia (NIST) (ISMM)	Faculdade de Ciências e Engenharia da Computação Universidade de Petróleo e Minerais King Fahd, Dhahran, Arábia Saudita	Permitir às organizações medir o respetivo progresso de implementação ao longo do tempo, para garantir que estão a manter a postura de segurança pretendida	Organizações	5	23 domínios avaliados	-	-
Modelo de Capacidade de Auditoria Interna (IA-CM) para o Setor Público	o «Institute of Internal auditors Research Foundation»	Criar capacidade de auditoria interna e apoio através da autoavaliação no setor público	Organizações do setor público	5	6 elementos	Autoavaliação	-
O Índice Global de Cibersegurança (IGC)	União Internacional das Telecomunicações (ITU)	Analisar o compromisso e a situação em matéria de cibersegurança e ajudar os países a identificarem áreas para melhoria no domínio da cibersegurança	Países	N/A	5 pilares	Autoavaliação	Tabela de classificação

O Índice de Ciberpotência (CPI)	A «Economist Intelligence Unit» e Booz Allen Hamilton	Fazer uma avaliação comparativa da capacidade dos países do G20 para suportar ciberataques e implementar as infraestruturas digitais necessárias para uma economia próspera e segura.	Países do G20	N/A	4 categorias	Avaliação comparativa pela *Economist Intelligence Unit*	Tabela de classificação

Quadro 6 Comparação de Níveis de Maturidade

Modelo	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
Modelo de Maturidade da Capacitação de Cibersegurança para as Nações (CMM)	**Arranque** Não existe maturidade em matéria de cibersegurança, ou tem um caráter muito embrionário. Poderão existir discussões iniciais sobre criação de capacidades em matéria de cibersegurança, mas não foram adotadas ações concretas. Há uma ausência de dados observáveis nesta fase.	**Formativa** Algumas características dos aspetos começaram a crescer e a serem formuladas, mas podem ser *ad hoc*, desorganizadas, definidas deficientemente ou simplesmente «novas». Contudo, os dados desta atividade podem ser claramente demonstrados.	**Estabelecida** Os elementos do aspeto estão criados e a funcionar. Não há, porém, uma consideração bem planeada da afetação relativa de recursos. Há pouca tomada de decisões de compromisso no que diz respeito ao investimento «relativo» nos vários elementos do aspeto. No entanto, o aspeto está funcional e definido.	**Estratégica** Foram feitas escolhas sobre que partes do aspeto são importantes e quais são menos importantes para a organização ou nação em causa. A fase estratégica reflete o facto de que estas escolhas foram feitas, subordinadas às circunstâncias da nação ou organização.	**Dinâmica** Existem mecanismos claros para alterar a estratégia dependendo das circunstâncias prevalecentes, tais como a tecnologia do ambiente de ameaças, conflito mundial ou uma mudança significativa num domínio de preocupação (por exemplo, cibercriminalidade ou privacidade). Organizações dinâmicas desenvolveram métodos para alterar estratégias a passos largos. Tomada de decisões célere, reafectação de recursos e atenção constante ao ambiente em mutação são características desta fase.
Modelo de Maturidade da Capacitação de Cibersegurança (C2M2)	**NIM0** Não são realizadas práticas.	**NIM1** São realizadas práticas iniciais, mas podem ser *ad hoc*.	**NIM2** Características de gestão: As práticas estão documentadas; São prestados recursos adequados para apoiar o processo; O pessoal que realiza as práticas possui competências e conhecimento adequados; e São atribuídas responsabilidade e autoridade para a realização das práticas. Característica de abordagem: As práticas são mais completas ou avançadas do que no NIM1.	**NIM3** Características de gestão: As atividades são orientadas por políticas (ou outras diretivas organizacionais); São estabelecidos e monitorizados objetivos de desempenho para atividades do domínio para acompanhar as realizações; e São normalizadas e melhoradas práticas documentadas para atividades do domínio na empresa. Característica de abordagem: As práticas são mais completas ou avançadas do que no NIM2.	-
Modelo de maturidade da segurança da informação para o Quadro de cibersegurança do	**Processo Realizado**	**Processo Gerido**	**Processo Estabelecido**	**Processo Previsível**	**Processo de Otimização**

Instituto Nacional de Normas e Tecnologia (NIST) (ISMM)					
Modelo de Maturidade da Capacitação de Cibersegurança Catar (Q-C2M2)	**Inicial** Emprega práticas e processos de cibersegurança *ad hoc* ao abrigo de alguns dos domínios.	**Em desenvolvimento** Políticas e práticas implementadas para desenvolver e melhorar atividades em matéria de cibersegurança ao abrigo dos domínios com o objetivo de sugerir novas atividades a implementar.	**Em implementação** Políticas adotadas para implementar todas as atividades em matéria de cibersegurança ao abrigo dos domínios com o propósito de concluir a implementação num determinado período.	**Adaptativo** Revisita e revê atividades em matéria de cibersegurança e adota práticas baseadas em indicadores preditivos resultantes de experiências e medições anteriores.	**Ágil** Continua a exercer a fase adaptativa com uma ênfase adicional na agilidade e rapidez aquando da implementação de atividades nos domínios.
Certificação do Modelo de Maturidade da Cibersegurança (CMMC)	**Processos: Realizados** Porque a organização apenas pode realizar estas práticas de uma forma *ad hoc* e pode ou não apoiar-se em documentação. A maturidade do processo não é avaliada para o Nível 1. **Práticas: Ciber-higiene Básica** O nível 1 incide sobre a proteção de ICF (Informações Contratuais Federais) e consiste apenas em práticas que correspondem aos requisitos de salvaguarda básicos.	**Processos: Documentados** O nível 2 requer que uma organização estabeleça e documente práticas e políticas para orientar a implementação dos seus esforços em matéria de CMMC. A documentação de práticas permite que as pessoas as executem de um modo repetível. As organizações desenvolvem capacidades maduras documentando os respetivos processos e exercendo-as conforme documentado. **Práticas: Ciber-higiene Intermédia** O nível 2 serve como uma progressão do Nível 1 para o Nível 3 e consiste num subconjunto de requisitos de segurança especificados na NIST SP 800-171, bem como em práticas de outras normas e referências.	**Processos: Geridos** O nível 3 requer que uma organização estabeleça, mantenha e atribua os recursos a um plano que demonstre a gestão de atividades para implementação de práticas. O plano pode incluir informações sobre missões, objetivos, planos de projetos, atribuição de recursos, formação necessária e envolvimento de partes interessadas relevantes. **Práticas: Boa Ciber-higiene**. O nível 3 incide sobre a proteção de CUI (Informações Não Classificadas Controladas) e engloba todos os requisitos de segurança especificados na NIST SP 800-171, bem como práticas adicionais de outras normas e referências para mitigar ameaças.	**Processos: Revistos.** O nível 4 requer que uma organização reveja e meça práticas em relação à eficácia. Além de medir práticas em relação à eficácia, as organizações neste nível são capazes de tomar medidas corretivas quando necessário e informar a direção de alto nível sobre o estado ou problemas de uma forma recorrente. **Práticas: Proativas** O nível 4 incide sobre a proteção de CUI (Informações Não Classificadas Controladas) e engloba um subconjunto dos requisitos de segurança reforçados. Estas práticas melhoram as capacidades de deteção e resposta de uma organização para fazer face e adaptar-se às táticas, técnicas e procedimentos em mutação.	**Processos: Otimizar** O nível 5 requer que uma organização normalize e otimize a implementação de processos na organização. **Práticas: Avançadas/Proativas** O nível 5 incide sobre a proteção de CUI (Informações Não Classificadas Controladas). As práticas adicionais aumentam a profundidade e a sofisticação das capacidades em matéria de cibersegurança.
O Modelo Comunitário de Maturidade em matéria de Cibersegurança (CCSMM)	**Conscientização para a Segurança** O tema principal de atividades neste nível é sensibilizar as pessoas e organizações para as ameaças, problemas e questões relacionados com a cibersegurança	**Desenvolvimento de Processos** Nível concebido para ajudar as comunidades a criarem e melhorarem processos de segurança necessários para resolver eficazmente problemas de cibersegurança.	**Possibilitado pelas Informações** Concebido para melhorar os mecanismos de partilha de informações na comunidade a fim de permitir à comunidade correlacionar eficazmente elementos de informação supostamente díspares.	**Desenvolvimento e Táticas** Os elementos deste nível estão concebidos para desenvolver métodos melhores e mais proativos para detetar e responder a ataques. Neste nível, a maioria dos métodos de prevenção devem estar implementados.	**Capacidade Operacional de Segurança Plena** Este nível representa os elementos que devem estar implementados para qualquer organização se considerar plenamente preparada operacionalmente para combater qualquer tipo de ciberameaça.
Modelo de Capacidade de Auditoria Interna (IA-CM) para o Setor Público	**Inicial** Capacidades não sustentáveis, repetíveis – dependentes de esforços individuais	**Infraestruturas** Práticas e procedimentos sustentáveis e repetíveis	**Integrado** Práticas de gestão e profissionais uniformemente aplicadas	**Geridos** Integra informação na organização para melhorar a governação e a gestão de riscos	**Otimizar** Aprender dentro e fora da organização para melhoria contínua

Quadro 7: Comparação de Atributos/Dimensões

	Modelo de Maturidade da Capacitação de Cibersegurança para as Nações (CMM)	Modelo de Maturidade da Capacitação de Cibersegurança (C2M2)	Modelo de Maturidade da Capacitação de Cibersegurança Catar (Q-C2M2)	Certificação do Modelo de Maturidade da Cibersegurança (CMMC)	Certificação do Modelo de Maturidade da Cibersegurança (CMMC)	Modelo de maturidade da segurança da informação para o Quadro de cibersegurança do Instituto Nacional de Normas e Tecnologia (NIST) (ISMM)	Quadro para Melhorar a Cibersegurança de Infraestruturas Críticas	O Índice Global de Cibersegurança (IGC)	O Índice de Ciberpotência (CPI)
Níveis	Cinco dimensões divididas em vários fatores que incluem eles próprios vários aspetos e indicadores (Figura 4)	Dez domínios, incluindo objetivo de gestão único e vários objetivos de abordagem (Figura 6)	Cinco domínios divididos em subdomínios	Dezassete domínios pormenorizados em processos e uma a várias capacidades que são depois detalhadas em Práticas (Figura 9).	6 dimensões principais	Vinte e três domínios avaliados	Cinco funções com categorias principais e subcategorias subjacentes (Figura 8).	Cinco pilares incluindo vários indicadores	Quatro categorias com vários indicadores
Atributos/Dimensões	i Dividir a política e estratégia de cibersegurança; ii Encorajar uma cultura de cibersegurança responsável na sociedade; iii Desenvolver conhecimentos em matéria de cibersegurança; iv Criar quadros jurídicos e regulamentares eficazes; e v Controlar os riscos através de normas, organizações e tecnologias.	i Gestão de Riscos; ii Gestão de ativos, mudança e configuração; iii Gestão de Identidades e Acessos; iv Gestão de Ameaças e Vulnerabilidades; v Conhecimento da Situação; vi Resposta a Eventos e Incidentes; vii Gestão da Cadeia de Abastecimento e das Dependências Externas; viii Gestão Mão-de-Obra; ix Arquitetura de Cibersegurança; x Gestão de Programa de Cibersegurança.	i Compreender (Cibergovernação, Ativos, Riscos e Formação); ii Proteger (Segurança dos Dados, Segurança da Tecnologia, Segurança do Controlo do Acesso, Segurança das Comunicações e Segurança do Pessoal); iii Expor (Monitorizar, Gestão de Incidentes, Deteção, Análise e Exposição); iv Responder (Planeamento da Resposta, Mitigação e Comunicação da Resposta); v Sustentar (Planeamento da Recuperação, Gestão da Continuidade, Melhoria e Dependências Externas).	i Controlo do Acesso; ii Gestão de Ativos; iii Auditoria e Prestação de Contas; iv Sensibilização e Formação; v Gestão da Configuração; vi Identificação e Autenticação; vii Resposta a Incidentes; viii Manutenção; ix Proteção dos Meios; x Segurança do Pessoal; xi Proteção Física; xii Recuperação; xiii Gestão de Riscos; xiv Avaliação da Segurança; xv Conhecimento da Situação; xvi Proteção do Sistema e das Comunicações; xvii Integridade do Sistema e da Informação.	i Ameaças Combatidas; ii Métricas; iii Partilha de Informações; iv Tecnologia; v Formação; vi Teste.	i Gestão de Ativos; ii Ambiente Empresarial; iii Governação; iv Avaliação dos Riscos; v Estratégia de Gestão de Riscos; vi Avaliação da Conformidade; vii Controlo do Acesso; viii Sensibilização e Formação; ix Segurança dos Dados; x Processos e Procedimentos de Proteção da Informação; xi Manutenção; xii Tecnologia de Proteção; xiii Anomalias e Eventos; xiv Monitorização Contínua da Segurança; xv Processos de Deteção; xvi Planeamento da Resposta; xvii Comunicações de Resposta; xviii Análise da Resposta; xix Mitigação da Resposta; xx Melhorias da Resposta; xxi Plano de Recuperação; xxii Melhorias da Recuperação; xxiii Comunicações da Recuperação.	i Identificar; ii Proteger; iii Detetar; iv Responder; v Recuperar.	i Jurídico; ii Técnico; iii Organizacional; iv Criação de capacidades; v Cooperação.	i Quadro Jurídico e Regulamentar; ii Contexto Económico e Social; iii Infraestruturas de Tecnologia; iv Aplicação na Indústria.

ANEXO B – BIBLIOGRAFIA DA INVESTIGAÇÃO DOCUMENTAL

Almuhammadi, S. e Alsaleh, M. (2017) «Information Security Maturity Model for Nist Cyber Security Framework», em Computer Science & Information Technology (CS & IT). Sexta Conferência Internacional sobre Convergência e Serviços das Tecnologias da Informação, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. e Alsaleh, M. (2017) «Information Security Maturity Model for Nist Cyber Security Framework», em Computer Science & Information Technology (CS & IT). Disponível em: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) «Stocktaking, analysis and recommendations on the protection of CIIs. Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) «Developing Maturity Models for IT Management – A Procedure Model and its Application.» Disponível em: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Governo belga (2012) Estratégia para a Cibersegurança. Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) «Developing Cybersecurity Capacity: A proof-of-concept implementation guide.» RAND Corporation. Disponível em: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) «Introduction to Return on Security Investment».

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) «Cybersecurity Capability Maturity Model (C2M2) Version 2.0.» Disponível em https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) «National Cybersecurity Strategies in Comparison – Challenges for Switzerland.» Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Conselho de Ministros (2019) Diário da República n.º 108/2019, Série I - Resolução do Conselho de Ministros n.º 92/2019. Disponível em: https://dre.pt/application/conteudo/122498962

Creese, S. (2016) «Cybersecurity Capacity Maturity Model for Nations (CMM).» Universidade de Oxford.

«CSIRT Maturity - Self-assessment Tool» (sem data). Disponível em: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Projeto CyberCrime@IPA do Conselho da Europa e da União Europeia, Projeto Global sobre a Cibercriminalidade do Conselho da Europa e da Task Force da União Europeia para a Cibercriminalidade (2011) Unidades especializadas em cibercriminalidade - Estudo sobre boas práticas. Disponível em: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

«Cybersecurity Incident Report and Analysis System – Visual Analysis Tool» (sem data). Disponível em: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017)« Public Private Partnerships (PPP).»

Darra, E. (sem data) «Welcome to the NCSS Training Tool».

Dekker, M. A. C. (2014) «Technical Guideline on Incident Reporting.» Disponível em: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) «Technical Guideline on Security Measures.» Disponível em: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) «Guideline on Threats and Assets.» Disponível em: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016) Estratégia para a cibersegurança. Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) «*Privacy and data protection by design - from policy to engineering.*» Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Comissão Europeia (2012) Regulamento do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012PC0238&from=PT

Agência Europeia para a Segurança das Redes e da Informação (2012) «NCSS: Practical Guide on Development and Execution.» Heraklion: ENISA.

Agência Europeia para a Segurança das Redes e da Informação (2012) «NCSS: Setting the course for national efforts to strengthen security in cyberspace.» Heraklion: ENISA.

Agência Europeia para a Segurança das Redes e da Informação (2016) «Guidelines for SMEs on the security of personal data processing.»

Agência Europeia para a Segurança das Redes e da Informação (2016) «NCSS good practice guide: designing and implementing national cyber security strategies.» Heraklion: ENISA.

Agência Europeia para a Segurança das Redes e da Informação (2017) «Handbook on security of personal data processing.» Disponível em: http://dx.publications.europa.eu/10.2824/569768

Agência Europeia para a Segurança das Redes e da Informação (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Disponível em: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Gabinete Executivo do Presidente (2015) «Memorandum for Heads of Executive Departments and Agencies.» Disponível em: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Chancelaria Federal da República da Áustria (2013) «Austrian Cyber Security Strategy.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-

map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Ministério Federal do Interior (2011) «Cyber Security Strategy for Germany.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016) Diretiva SIR e Nacional (2015) «Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.» Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., União Europeia e Agência Europeia para a Segurança das Redes e da Informação (2015) «The 2015 report on national and international cyber security exercises: survey, analysis and recommendations.» Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Gabinete do primeiro-ministro francês (2014) «French National Digital Security Strategy.» Disponível em: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015) «Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.» Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Universidade de Gand et al. (2017) «Evaluating Business Process Maturity Models', Journal of the Association for Information Systems.» Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Governo da Bulgária (2015) «National Cyber Security Strategy - Cyber-resistant Bulgaria 2020.»

Governo da Croácia (2015) «The National Cyber Security Strategy of The Republic of Croatia.» Disponível em: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Governo da Grécia (2017) «National Cyber Security Strategy.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Governo da Hungria (2018) «Strategy for the Security of Network and Information Systems.» Disponível em: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Governo da Irlanda (2019) «National Cyber Security Strategy.» Disponível em: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Governo de Espanha (2019) «National Cyber Security Strategy.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Instituto de Auditores Internos (ed.) (2009) «Internal audit capability model (IA-CM) for the public sector: overview and application guide.» Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

União Internacional das Telecomunicações (ITU) (2018) «The Global Cybersecurity Index. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

União Internacional das Telecomunicações (ITU) (2018) «Guide to developing a national cybersecurity strategy.» Disponível em: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) «Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework», International Review of Law.

Governo letão (2014) «Cyber Security Strategy of Latvia.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) «An evaluation framework for national cyber security strategies.» Heraklion: ENISA. Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.* (2014) «*Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.*» Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministério da Competitividade e da Economia Digital, Marítima e dos Serviços (2016) «Malta Cyber Security Strategy. Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ministério dos Assuntos Económicos e das Comunicações (2019) «Cybersecurity Strategy – Republic of Estonia.» Disponível em: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministério da Defesa Nacional da República da Lituânia (2018) «National Cyber Security Strategy»

Centro Nacional de Cibersegurança (2015) «National Cyber Security Strategy of the Czech Republic.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Estratégias Nacionais de Cibersegurança - Mapa Interativo (sem data). Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

«National Cybersecurity Strategies Evaluation Tool» (2018). Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Instituto Nacional de Normas e Tecnologia (2018) «Framework for Improving Critical Infrastructure Cybersecurity», Versão 1.1. Gaithersburg, MD: Instituto Nacional de Normas e Tecnologia. Disponível em: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) «Business Process Maturity Model.» Disponível em: https://www.omg.org/spec/BPMM/1.0/PDF

OCDE, União Europeia e Centro Comum de Investigação (2008) «Handbook on Constructing Composite Indicators: Methodology and User Guide.» OCDE. Disponível em: https://www.oecd.org/sdd/42495745.pdf.

Gabinete do comissários das Comunicações Eletrónicas e dos Regulamentos Postais (2012) «Cybersecurity Strategy of the Republic of Cyprus.»

Jornal Oficial da União Europeia (2008) DIRETIVA 2008/114/CE DO CONSELHO, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114&from=PT

Organização de Cooperação e de Desenvolvimento Económicos (OCDE) (2012) «Cybersecurity policy making at a turning point.» Disponível em: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) «National Cyber Security Strategies - Practical Guide on Development and Execution».

Ouzounis, E. (2012) «Good Practice Guide on National Exercises.»

Portesi, S. (2017) «Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects»

Presidência do Conselho de Ministros (2017) «The Italian Cybersecurity Action Plan.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019) «Dziennik Urzędowy Rzeczypospolitej Polskiej.» Disponível em: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Governo romeno (2013) «Cyber Security Strategy of Romania.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. e Agência da União Europeia para a Cibersegurança (2019) «Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies.» Disponível em: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Secretariado do Comité de Segurança (2019) «Finland's Cyber Security Strategy 2019.» Disponível em: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Governo eslovaco (2015) «Cyber Security Concept of the Slovak Republic.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015) Diretiva 2016/1148/UE do Parlamento Europeu e do Conselho, de 7 de julho de 2010

Smith, R. (2016) «Diretiva 2016/1148/UE do Parlamento Europeu e do Conselho, de 7 de julho de 2010», em Smith, R., legislação nuclear da UE. Londres: Macmillan Education. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT.

Stavropoulos, V. (2017) Mês Europeu da Cibersegurança 2017.

Governo sueco (2017) «Nationell strategi för samhällets informations- och cybersäkerhet.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Governo dinamarquês - Ministério das Finanças (2018) «Danish Cyber and Information Security Strategy.» Disponível em: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Conselho Federal (2018) «National strategy for the protection of Switzerland against cyber risks.»

Conselho do Governo luxemburguês (2018) «National Cybersecurity Strategy.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Governo dos Países Baixos (2018) «National Cyber Security Agenda.» Disponível em: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Casa Branca (2018) «National Cyber Strategy of the United States of America.» Disponível em: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011) «Cyber Europe Report.» Disponível em: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. e Agência Europeia para a Segurança das Redes e da Informação (2013) «*National-level risk assessments: an analysis report.*» Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) «Report on cyber-crisis cooperation and management.» Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015) «Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises.» Disponível em: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016-2021 (2016). Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Universidade de Innsbruck et al. (2009) «Understanding Maturity Models.»

Wamala, D. F. (2011) «ITU National Cybersecurity Strategy Guide.» Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) «The Community Cyber Security Maturity Model», em 2007 40.ª Conferência Internacional do Havai sobre Ciências de Sistema S'07)

ANEXO C – OUTROS OBJETIVOS ESTUDADOS

Os objetivos especificados a seguir foram estudados enquanto parte da fase de investigação documental e das entrevistas realizadas pela ENISA. Os objetivos que se seguem não fazem parte do Quadro de Avaliação das Capacidades Nacionais, mas elucidam sobre tópicos sobre os quais vale a pena discutir. Cada um dos seguintes subcapítulos fornecerá uma explicação da razão pela qual o objetivo foi descartado.

- Desenvolver estratégias de cibersegurança setoriais;
- Combater as campanhas de desinformação;
- Proteger tecnologias de ponta (5G, IA, computação quântica, etc.);
- Assegurar a soberania em matéria de dados; e
- Proporcionar incentivos para o desenvolvimento da indústria dos ciberseguros.

Desenvolver estratégias de cibersegurança setoriais

A adoção de estratégias setoriais que visam intervenções e incentivos num setor introduz sem dúvida uma capacidade descentralizada. É particularmente oportuno para os Estados-Membros cujos OSE têm de lidar com diferentes quadros e regulamentação e onde existem muitas dependências devido à natureza transversal da cibersegurança. Com efeito, em vários Estados-Membros, é comum contar dezenas de autoridades nacionais e organismos regulamentares com conhecimento das especificidades de cada setor que detêm um mandato para aplicar regulamentação específica para cada setor.

A Dinamarca, por exemplo, lançou seis estratégias específicas que abordam os esforços cibersegurança e de segurança da informação dos setores mais críticos para desenvolver uma capacidade mais robusta descentralizada na cibersegurança e segurança da informação. Cada «unidade setorial» contribuirá para avaliação das ameaças a nível setorial, monitorização, exercício de preparação, criação de sistemas de segurança, partilha de conhecimento e instruções, entre outros. As estratégias setoriais abrangem os seguintes setores:

- Energia;
- Cuidados de saúde;
- Transportes;
- Telecomunicações;
- Finanças; e
- Marítimo.

Outros Estados-Membros manifestaram interesse em considerar estratégias de cibersegurança setoriais para refletir todos os requisitos regulamentares. Contudo, cumpre salientar que um tal objetivo poderá não ser adequado para todos os Estados-Membros, dependendo da sua dimensão, políticas nacionais e maturidade. A grande dificuldade para garantir que o quadro pode ter em conta todas as especificidades levou a ENISA a não incluir este objetivo no quadro.

Combater as campanhas de desinformação

Os Estados-Membros integram a proteção dos princípios fundamentais como os direitos humanos, a transparência e a confiança pública nas respetivas estratégias nacionais de

cibersegurança. Trata-se de algo muito importante sobretudo no que toca à desinformação que é disseminada através dos meios de comunicação noticiosos tradicionais ou das plataformas de redes sociais. Além disso, a cibersegurança representa atualmente um dos maiores desafios eleitorais. Com efeito, atividades como a propagação de informações falsas ou a propaganda negativa foram observadas em vários países no período que medeia até eleições importantes. Esta ameaça tem o potencial de comprometer o processo democrático da UE. A nível europeu, a Comissão delineou um Plano de Ação[32] para intensificar esforços para combater a desinformação na Europa: este plano incide sobre domínios-chave (deteção, cooperação, colaboração com plataformas em linha e sensibilização) e serve para criar as capacidades da UE e reforçar a cooperação entre Estados-Membros.

4 de 19 países entrevistados manifestaram a sua intenção de combater o problema da desinformação e propaganda na sua ENC.

Por exemplo, a ENC francesa[33] observa que: «é da responsabilidade do Estado informar os cidadãos sobre os riscos de técnicas de manipulação e de propaganda usadas por agentes maliciosos na Internet. Por exemplo, após os ataques terroristas contra França em janeiro de 2015, o governo criou uma plataforma de informação sobre os riscos relacionados com a radicalização islâmica através de redes de comunicação eletrónica: “Stop-djihadisme.gouv.fr”.» Esta abordagem poderá ser alargada para responder a outros fenómenos de propaganda ou destabilização.

Noutro exemplo, a ENC 2019-2024 da Polónia[34] indica que: «contra atividades manipuladoras como campanhas de desinformação, são necessárias ações sistémicas para desenvolver a sensibilização dos cidadãos no contexto de verificar a autenticidade das informações e responder a tentativas de distorcê-las.»

No entanto, durante as entrevistas realizadas pela ENISA, vários Estados-Membros afiançaram que não abordam o problema enquanto parte da sua ENC como uma ameaça de cibersegurança, abordando, em vez disso, o problema a um nível social mais vasto, por exemplo, através de iniciativas políticas.

Proteger tecnologias de ponta (5G, IA, computação quântica...)

Dado que o cenário atual de ciberameaças continua a expandir-se, o desenvolvimento de novas tecnologias irá muito provavelmente resultar num aumento da intensidade e do número de ciberataques e na diversificação dos métodos, meios e alvos utilizados pelos autores de ameaças. Entretanto, estas novas soluções tecnológicas na forma de tecnologias de ponta têm o potencial de se tornarem nos elementos constitutivos do Mercado Digital Europeu. A fim de salvaguardar a dependência digital crescente dos Estados-Membros e o surgimento de novas tecnologias, devem ser criados incentivos e verdadeiras políticas para apoiar o desenvolvimento e implementação seguros e fiáveis dessas tecnologias na UE.

Durante a fase de investigação documental realizada sobre as ENC dos Estados-Membros, as seguintes tecnologias de ponta foram apresentados como sendo de interesse para os Estados-Membros: 5G, IA, computação quântica, criptografia, computação periférica, veículos

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

conectados e autónomos, grandes volumes de dados e dados inteligentes, cadeia de blocos (*blockchain*), robótica e IdC.

Mais concretamente, no início de 2020, a Comissão Europeia publicou uma comunicação convidando os Estados-Membros a tomarem medidas para implementar o conjunto de medidas recomendadas nas conclusões sobre o conjunto de instrumentos para as redes 5G[35]. Este conjunto de instrumentos da para as redes 5G surge na sequência da Recomendação (UE) 2019/534 sobre a cibersegurança das redes 5G adotada pela Comissão em 2019, que apelou a uma abordagem europeia unificada da segurança das redes 5G[36].

Durante as entrevistas realizadas pela ENISA, foi salientado que este tópico se trata de um tópico mais transversal que é abordado na ENC ao invés de um objetivo específico propriamente dito.

Assegurar a soberania em matéria de dados

Por um lado, o ciberespaço pode ser encarado como um espaço comum formidável, que está facilmente acessível, proporcionando um elevado grau de conectividade e capaz de gerar grandes oportunidades para crescimento socioeconómico. Por outro lado, o ciberespaço também se caracteriza por uma jurisdição débil, dificuldade em atribuir ações, ausência de fronteiras e sistemas interconectados que podem ser porosos e cujos dados podem ser roubados ou até mesmo acedidos por governos estrangeiros. Além destas duas perspetivas, o ecossistema digital é marcado pela concentração de plataformas e infraestruturas de serviços em linha nas mãos de muito poucas partes interessadas. Todos os aspetos supracitados levam os Estados-Membros a promoverem a soberania digital. Alcançar a soberania digital significa que os cidadãos e as empresas são capazes de prosperar plenamente usando serviços digitais e produtos TIC que sejam confiáveis sem qualquer receio relativamente aos dados pessoais de alguém , ou aos ativos digitais, à autonomia económica de alguém ou à influência política de alguém.

A soberania em matéria de dados ou soberania digital é defendida pelos Estados-Membros a nível nacional e a nível europeu. Embora os Estados-Membros não pareçam abordar a questão diretamente na respetiva ENC como um tópico específico, abordam-na como um princípio transversal ou indicam a sua intenção de assegurar a soberania digital a nível nacional em publicações *ad hoc* concentrando-se em tecnologias-chave. Por exemplo, na revisão estratégica francesa da ciberdefesa de 2018, é indicado que «controlar as seguintes tecnologias reveste-se da maior importância para assegurar a soberania digital: encriptação das comunicações, deteção de ciberataques, rádio móvel profissional, computação em nuvem e inteligência artificial[37].

A nível europeu, os Estados-Membros estão a participar ativamente na definição da estratégia europeia para os dados (COM/2020/66 final) e na criação do enquadramento europeu para a certificação de produtos, serviços e processos digitais TIC estabelecido pelo Regulamento Cibersegurança da UE (2019/881), para assegurar uma autonomia digital estratégica a nível da UE.

A fase de entrevistas com os Estados-Membros revelou que o tópico da soberania digital é amiúde considerado uma questão mais vasta do que uma que está restringida à cibersegurança. Por conseguinte, os Estados-Membros não abrangem o tópico nas respetivas

[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019H0534
[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

ENC e, em relação aos poucos que o fazem, não o abrangem como um objetivo específico propriamente dito.

Proporcionar incentivos para o desenvolvimento da indústria dos ciberseguros

A situação atual da indústria de ciberseguros mostra que o mercado global cresceu inquestionavelmente. Contudo, ainda é muito incipiente uma vez que os dados devem ser recolhidos e ainda estão por definir muitos precedentes (por exemplo, cobertura omissa, ciberriscos sistémicos...). Além disso, as perdas agregadas estimadas resultantes dos ciberataques em todo o mundo têm diferentes ordens de grandeza superiores à capacidade de cobertura atual da indústria de ciberseguros (Documento de trabalho do FMI - «Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143»). Contudo, o desenvolvimento da indústria de ciberseguros pode seguramente produzir benefícios e lançar os alicerces para mecanismos virtuosos. Com efeito, os mecanismos de ciberseguros podem ajudar a:

- Sensibilizar para os riscos de em matéria de cibersegurança em empresas;
- Avaliar a exposição aos ciberriscos de um modo quantitativo;
- Melhorar a gestão de riscos de cibersegurança;
- Prestar apoio a organizações que sejam vítimas de ciberataques; e
- Cobrir os danos (materiais ou não) induzidos por um ciberataque.

Alguns Estados-Membros começaram a trabalhar neste tópico. Por exemplo:

- A Estónia adotou uma abordagem «esperar para ver» na sua ENC: «A fim de mitigar os ciberriscos no setor privado em geral, a procura e a oferta de serviços de ciberseguros na Estónia será analisada e nessa base, serão acordados princípios cooperativos para partes relacionadas, nomeadamente a partilha de informações, preparação de avaliação dos riscos, etc. Atualmente, os fornecedores de serviços de cibersegurança são poucos no mercado estónio e é necessário cartografar em primeiro lugar quem oferece o quê. A complexidade da proteção dos seguros é amiúde considerada um entrave ao desenvolvimento do mercado de ciberseguros.»
- O Luxemburgo apoia especificamente o desenvolvimento da indústria de ciberseguros na sua ENC: «Objetivo 1: Criar novos produtos e serviços. Reunir riscos e encorajar as vítimas de ciberincidentes digitais a procurarem ajuda de peritos para gerir o incidente e restaurar um sistema afetado por um ato malicioso, as companhias de seguro serão encorajadas a criarem produtos específicos para o domínio dos ciberseguros.»

Os retornos de informação dos inquiridos foram bastante diversos sobre este tópico: alguns Estados-Membros indicaram que o tópico dos ciberseguros tornou-se recentemente um tópico de discussão, ao passo que outros afiançaram que embora o tópico seja promissor, a indústria ainda não está suficientemente madura. Todavia, um grande número de inquiridos declarou que o tópico não é abordado enquanto parte da ENC, porque era considerado demasiado específico ou porque não se inseria no âmbito de aplicação da ENC.

TP-02-21-253-PT-N

Sobre a Agência da União Europeia para a Cibersegurança

A Agência da União Europeia para a Cibersegurança, ENISA, é a agência da União dedicada à obtenção de um elevado nível comum de cibersegurança na Europa. Estabelecida em 2004 e reforçada pelo Regulamento Cibersegurança da UE, a Agência da União Europeia para a Cibersegurança contribui para a ciberpolítica da UE, reforça a fiabilidade dos produtos, serviços e processos de TIC com sistemas de certificação da cibersegurança, coopera com os Estados-Membros e os organismos da UE e ajuda a Europa a preparar-se para os desafios cibernéticos do futuro. Através da partilha de conhecimentos, do reforço das capacidades e da sensibilização, a Agência trabalha em colaboração com as suas principais partes interessadas para reforçar a confiança na economia conectada, aumentar a resiliência das infraestruturas da União e, em última análise, manter a segurança digital da sociedade e dos cidadãos europeus. Para mais informações, consultar www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-493-0
DOI: 10.2824/88591