CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Cybersecurity policy initiatives in the Portuguese maritime sector

2nd ENISA Maritime Cybersecurity Conference
European Maritime Safety Agency, Lisbon
14th October 2022

Vasco Vaz
Regulation, Supervision and Certification Department
Centro Nacional de Cibersegurança

2nd ENISA Maritime Cybersecurity Conference

European Maritime Safety Agency, Lisbon

14th October 2022

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

10h15	Portuguese cybersecurity legislative framework and initiatives
15’	Development of supplementary cybersecurity provisions for the maritime sector
	Maritime sector ISAC

Portuguese cybersecurity legislative framework and initiatives

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Law n.º 46/2018, 13th August

ASSEMBLEIA DA REPÚBLICA

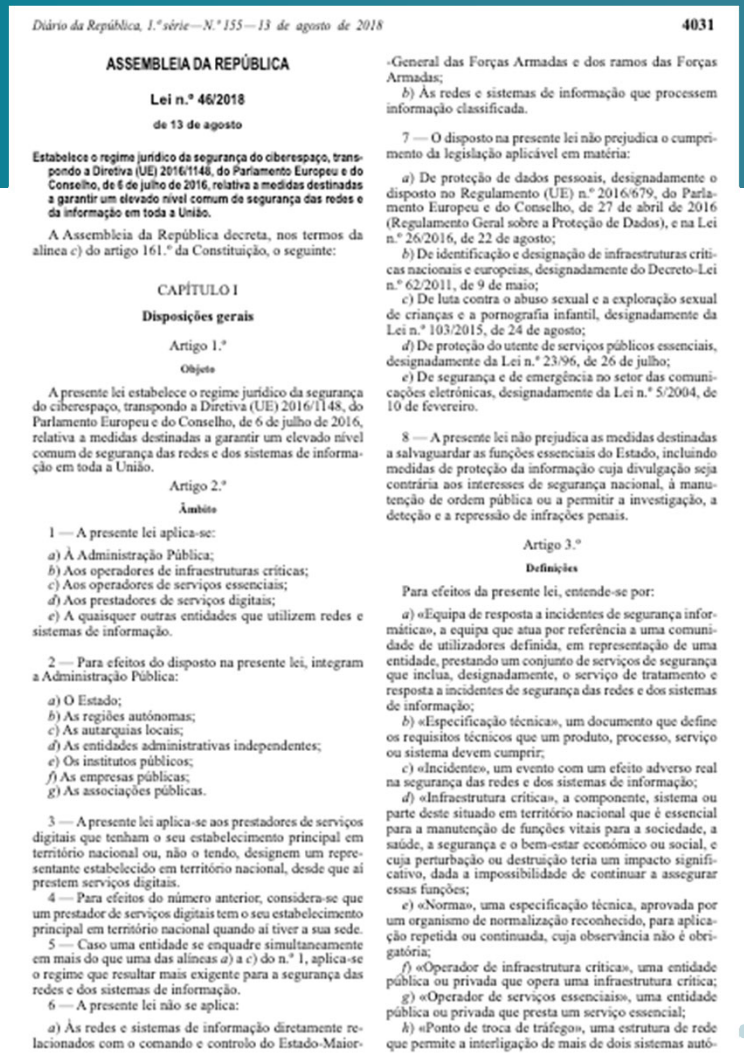
- Establishes the **Legal Framework for Cyberspace Security,** transposing Directive (EU) 2016/1148

- **National Strategy for Cyberspace Security**. The 2019-2023 strategy was approved by the Council of Ministers' Resolution n.º 92/2019 (as per article 6)

- The **Higher Council for Cyberspace Security** ensures strategic-political coordination for the security of cyberspace (as per Article 5)

- **National Cyber Security Centre** is the **National Cyber Security Authority [**as per Article 7(1) and (3)], and the national single point of contact

- **CERT.PT** established as the National Computer Security Incident Response Team (as per Articles 8 and 9)



Diário da República, 1.ª série — N.º 155 — 13 de agosto de 2018 **4031**

ASSEMBLEIA DA REPÚBLICA

Lei n.º 46/2018

de 13 de agosto

Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

A Assembleia da República decreta, nos termos da alínea *c*) do artigo 161.º da Constituição, o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

A presente lei estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

Artigo 2.º

Âmbito

1 — A presente lei aplica-se:

a) À Administração Pública;
b) Aos operadores de infraestruturas críticas;
c) Aos operadores de serviços essenciais;
d) Aos prestadores de serviços digitais;
e) A quaisquer outras entidades que utilizem redes e sistemas de informação.

2 — Para efeitos do disposto na presente lei, integram a Administração Pública:

a) O Estado;
b) As regiões autónomas;
c) As autarquias locais;
d) As entidades administrativas independentes;
e) Os institutos públicos;
f) As empresas públicas;
g) As associações públicas.

3 — A presente lei aplica-se aos prestadores de serviços digitais que tenham o seu estabelecimento principal em território nacional ou, não o tendo, designem um representante estabelecido em território nacional, desde que aí prestem serviços digitais.

4 — Para efeitos do número anterior, considera-se que um prestador de serviços digitais tem o seu estabelecimento principal em território nacional quando aí tiver a sua sede.

5 — Caso uma entidade se enquadre simultaneamente em mais do que uma das alíneas *a*) a *c*) do n.º 1, aplica-se o regime que resultar mais exigente para a segurança das redes e dos sistemas de informação.

6 — A presente lei não se aplica:

a) Às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas;
b) Às redes e sistemas de informação que processem informação classificada.

7 — O disposto na presente lei não prejudica o cumprimento da legislação aplicável em matéria:

a) De proteção de dados pessoais, designadamente o disposto no Regulamento (UE) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados), e na Lei n.º 26/2016, de 22 de agosto;
b) De identificação e designação de infraestruturas críticas nacionais e europeias, designadamente do Decreto-Lei n.º 62/2011, de 9 de maio;
c) De luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, designadamente da Lei n.º 103/2015, de 24 de agosto;
d) De proteção do utente de serviços públicos essenciais, designadamente da Lei n.º 23/96, de 26 de julho;
e) De segurança e de emergência no setor das comunicações eletrónicas, designadamente da Lei n.º 5/2004, de 10 de fevereiro.

8 — A presente lei não prejudica as medidas destinadas a salvaguardar as funções essenciais do Estado, incluindo medidas de proteção da informação cuja divulgação seja contrária aos interesses de segurança nacional, à manutenção de ordem pública ou a permitir a investigação, a deteção e a repressão de infrações penais.

Artigo 3.º

Definições

Para efeitos da presente lei, entende-se por:

a) «Equipa de resposta a incidentes de segurança informática», a equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação;
b) «Especificação técnica», um documento que define os requisitos técnicos que um produto, processo, serviço ou sistema devem cumprir;
c) «Incidente», um evento com um efeito adverso real na segurança das redes e dos sistemas de informação;
d) «Infraestrutura crítica», a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções;
e) «Norma», uma especificação técnica, aprovada por um organismo de normalização reconhecido, para aplicação repetida ou continuada, cuja observância não é obrigatória;
f) «Operador de infraestrutura crítica», uma entidade pública ou privada que opera uma infraestrutura crítica;
g) «Operador de serviços essenciais», uma entidade pública ou privada que presta um serviço essencial;
h) «Ponto de troca de tráfego», uma estrutura de rede que permite a interligação de mais de dois sistemas autó-

CNCS Centro Nacional de Cibersegurança PORTUGAL

Law n.º 46/2018, 13th August

Art. 12.º — Security requirements are defined under the conditions laid down in specific legislation

Incident notification requirements are defined under the conditions laid down in specific legislation — Art. 13.º, 15.º, 19.º e 20.º

Art. 21.º ss — Supervision and sanctions

Public Admi

- State
- Autonomous r
- Local Authoriti
- Independent a
- Public institute
- Public compar
- Public associa

Operators o

- Energy – Elec
- Transport – ai
- Banking
- Financial mark
- Health sector -
- Drinking water
- Digital Infrastr

Operators o

Digital servi providers

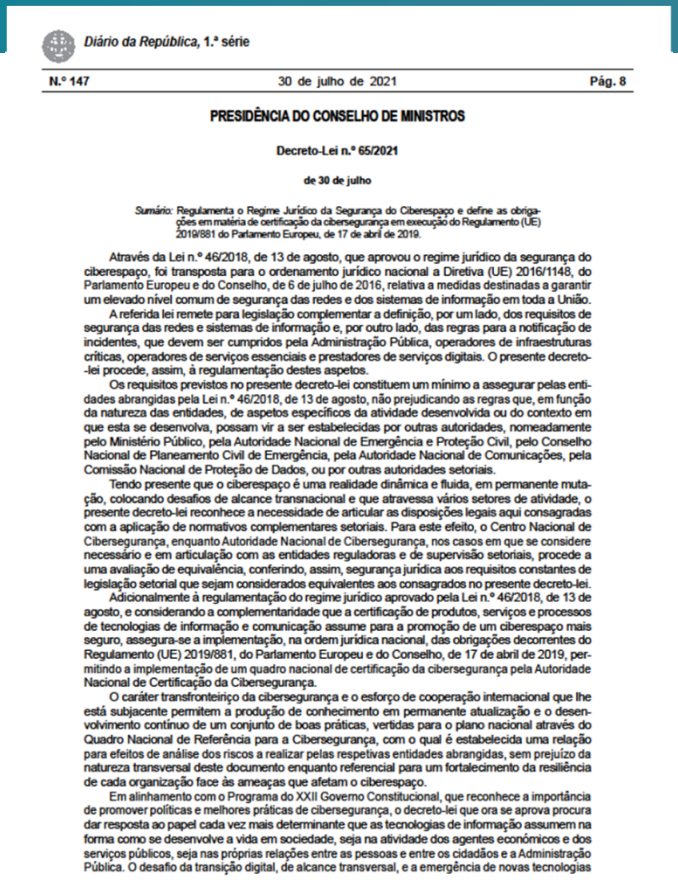
- Online marketplace
- Online search engine
- Cloud computing service

CNCS Centro Nacional de Cibersegurança PORTUGAL

Decree-Law n.º 65/2021 – Context

Decree-Law n.º 65/2021, of 30 July

- Regulates the Legal Framework for Cyberspace Security, approved by Law n.º46/2018, of 13 August
- Sets out the obligations concerning cybersecurity certification in application of Regulation (Eu) 2019/881 of The European Parliament and of the Council of 17 April 2019



Diário da República, 1.ª série

N.º 147 — 30 de julho de 2021 — Pág. 8

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Decreto-Lei n.º 65/2021

de 30 de julho

Sumário: Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Através da Lei n.º 46/2018, de 13 de agosto, que aprovou o regime jurídico da segurança do ciberespaço, foi transposta para o ordenamento jurídico nacional a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

A referida lei remete para legislação complementar a definição, por um lado, dos requisitos de segurança das redes e sistemas de informação e, por outro lado, das regras para a notificação de incidentes, que devem ser cumpridos pela Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais. O presente decreto-lei procede, assim, à regulamentação destes aspetos.

Os requisitos previstos no presente decreto-lei constituem um mínimo a assegurar pelas entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, não prejudicando as regras que, em função da natureza das entidades, de aspetos específicos da atividade desenvolvida ou do contexto em que esta se desenvolva, possam vir a ser estabelecidas por outras autoridades, nomeadamente pelo Ministério Público, pela Autoridade Nacional de Emergência e Proteção Civil, pelo Conselho Nacional de Planeamento Civil de Emergência, pela Autoridade Nacional de Comunicações, pela Comissão Nacional de Proteção de Dados, ou por outras autoridades setoriais.

Tendo presente que o ciberespaço é uma realidade dinâmica e fluida, em permanente mutação, colocando desafios de alcance transnacional e que atravessa vários setores de atividade, o presente decreto-lei reconhece a necessidade de articular as disposições legais aqui consagradas com a aplicação de normativos complementares setoriais. Para este efeito, o Centro Nacional de Cibersegurança, enquanto Autoridade Nacional de Cibersegurança, nos casos em que se considere necessário e em articulação com as entidades reguladoras e de supervisão setoriais, procede a uma avaliação de equivalência, conferindo, assim, segurança jurídica aos requisitos constantes de legislação setorial que sejam considerados equivalentes aos consagrados no presente decreto-lei.

Adicionalmente à regulamentação do regime jurídico aprovado pela Lei n.º 46/2018, de 13 de agosto, e considerando a complementaridade que a certificação de produtos, serviços e processos de tecnologias de informação e comunicação assume para a promoção de um ciberespaço mais seguro, assegura-se a implementação, na ordem jurídica nacional, das obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, permitindo a implementação de um quadro nacional de certificação da cibersegurança pela Autoridade Nacional de Certificação da Cibersegurança.

O caráter transfronteiriço da cibersegurança e o esforço de cooperação internacional que lhe está subjacente permitem a produção de conhecimento em permanente atualização e o desenvolvimento contínuo de um conjunto de boas práticas, vertidas para o plano nacional através do Quadro Nacional de Referência para a Cibersegurança, com o qual é estabelecida uma relação para efeitos de análise dos riscos a realizar pelas respetivas entidades abrangidas, sem prejuízo da natureza transversal deste documento enquanto referencial para um fortalecimento da resiliência de cada organização face às ameaças que afetam o ciberespaço.

Em alinhamento com o Programa do XXII Governo Constitucional, que reconhece a importância de promover políticas e melhores práticas de cibersegurança, o decreto-lei que ora se aprova procura dar resposta ao papel cada vez mais determinante que as tecnologias de informação assumem na forma como se desenvolve a vida em sociedade, seja na atividade dos agentes económicos e dos serviços públicos, seja nas próprias relações entre as pessoas e entre os cidadãos e a Administração Pública. O desafio da transição digital, de alcance transversal, e a emergência de novas tecnologias

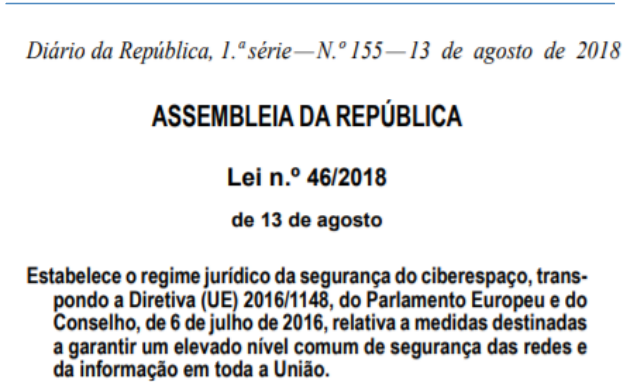
https://dre.pt/web/guest/home/-/dre/168697988/details/maximized

Decree-Law n.º 65/2021 – Context

Decree-Law n.º 65/2021, of 30 July

Regulates the Legal Framework for Cyberspace Security, approved by Law n.º46/2018, of 13 August

- Network and information systems security requirements
- Incident notification rules



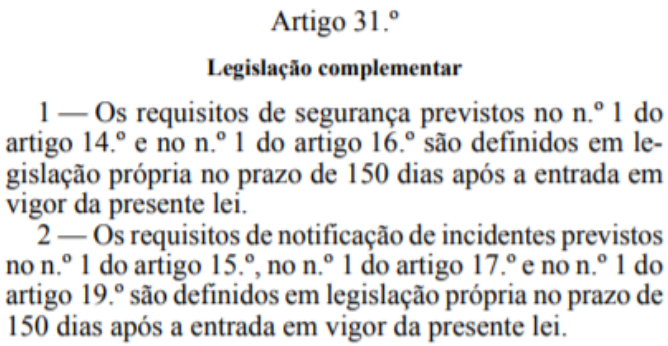
Diário da República, 1.ª série — N.º 155 — 13 de agosto de 2018

ASSEMBLEIA DA REPÚBLICA

Lei n.º 46/2018

de 13 de agosto

Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.



Artigo 31.º

Legislação complementar

1 — Os requisitos de segurança previstos no n.º 1 do artigo 14.º e no n.º 1 do artigo 16.º são definidos em legislação própria no prazo de 150 dias após a entrada em vigor da presente lei.

2 — Os requisitos de notificação de incidentes previstos no n.º 1 do artigo 15.º, no n.º 1 do artigo 17.º e no n.º 1 do artigo 19.º são definidos em legislação própria no prazo de 150 dias após a entrada em vigor da presente lei.

https://dre.pt/web/guest/home/-/dre/168697988/details/maximized

CNCS Centro Nacional de Cibersegurança PORTUGAL

Entities to which the Decree-law is applicable

Public Administration

- State
- Autonomous regions
- Local Authorities
- Independent administrative authorities
- Public institutes
- Public companies
- Public associations

Operators of essential services

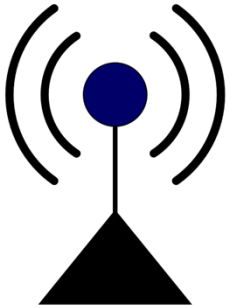
- Energy – Electricity, oil, gas
- Transport – air, rail, **water – sea and inland waterways -** and road transport
- Banking
- Financial market infrastructures
- Health sector – Health care settings
- Drinking water supply and distribution
- Digital Infrastructure

Operators of critical infrastructures

Digital service providers

- Online marketplace
- Online search engine
- Cloud computing service

DL 65/2021 – Obligations of the Entities – Common provisions



Permanent point of contact – to ensure the information flow with CNCS at an operational and technical level

Drawing up and periodic updating of a **security plan**, properly documented and signed by the security manager

Security manager – to manage the set of adopted security requirements and incident reporting measures

Drawing up and periodic updating of an **inventory of all assets which are essential** for the provision of their services, duly signed by the security manager

Production of an **annual report**

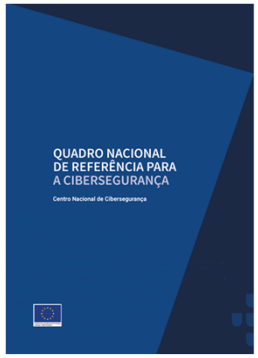
DL 65/2021 – Obligations of the Entities – Security of network and information systems

- To take the appropriate **technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations**
  - ➢ to that end, perform a **risk analysis** on all the assets that ensure the continued operation of the networks and information systems they use
  - As regards Operators of Essential Services, also on those assets which ensure the provision of essential services

- **Global** scope risk analysis to be performed 1x year or at the request of CNCS

- **Partial** scope risk analysis

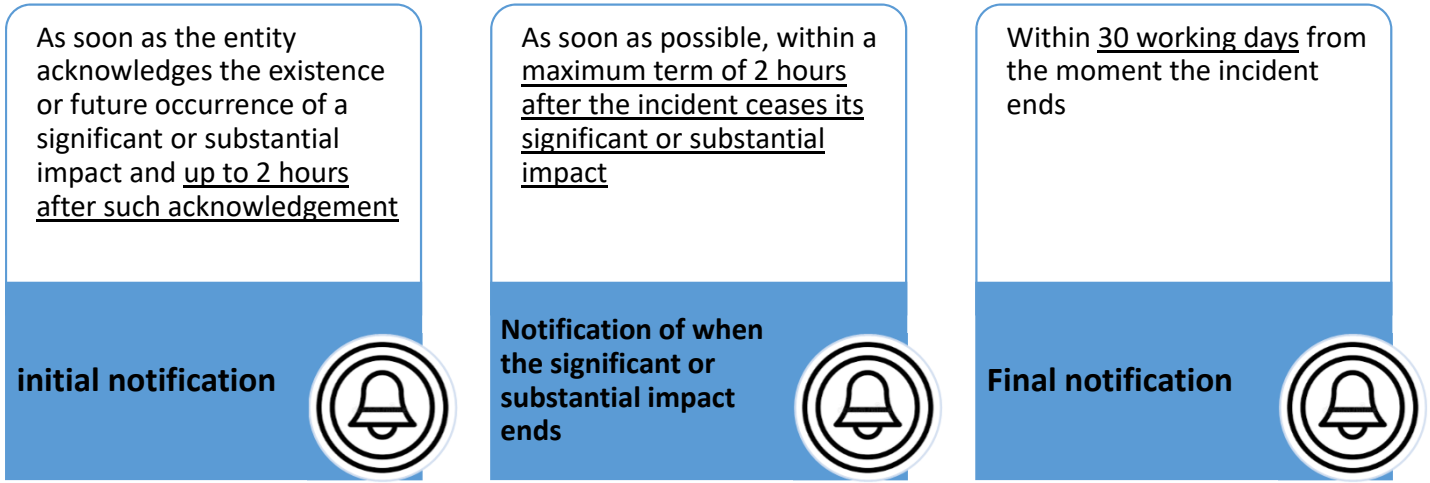
- ❑ From CNCS-approved **sectorial supplementary provisions**
- ❑ From the **National Cybersecurity Reference Framework**, produced by CNCS



QNRCS

DL 65/2021 – Obligations of the Entities – Incident notification

- To take all the necessary measures for the detection, impact assessment and notification of **incidents with a significant or substantial impact**



When the incident is resolved within 2 hours from its detection, entities may send a single, final, notification

DL 65/2021 – Supplementary provisions

- CNCS may **issue supplementary technical instructions** on security requirements and incident notification, namely sectorial supplementary provisions


Energy


Transport


Drinking water supply and distribution


Digital Infrastructure


Bank


Health sector

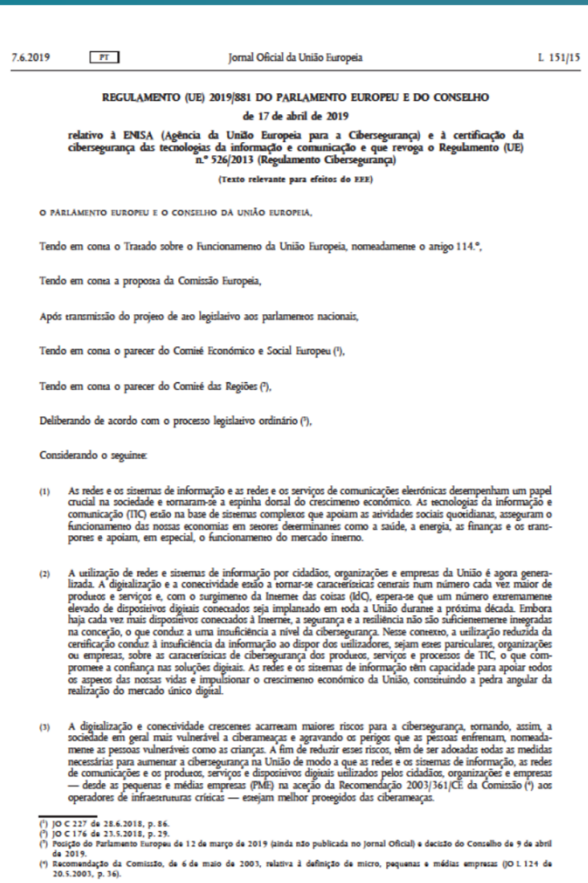

Financial market infrastructures

- Lay down specific conditions for **Public Administration** entities**,** in an adequate and proportionate manner with regard for their dimensions and organisational complexities

DL 65/2021 – Cybersecurity certification

Decree-Law n.º 65/2021, of 30 July

Sets out the obligations concerning cybersecurity certification in application of Regulation (Eu) 2019/881 of The European Parliament and of the Council of 17 April 2019



7.6.2019 PT Jornal Oficial da União Europeia L 151/15

REGULAMENTO (UE) 2019/881 DO PARLAMENTO EUROPEU E DO CONSELHO
de 17 de abril de 2019
relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança)
(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu (1),

Tendo em conta o parecer do Comité das Regiões (2),

Deliberando de acordo com o processo legislativo ordinário (3),

Considerando o seguinte:

(1) As redes e os sistemas de informação e as redes e os serviços de comunicações eletrónicas desempenham um papel crucial na sociedade e tornaram-se a espinha dorsal do crescimento económico. As tecnologias da informação e comunicação (TIC) estão na base de sistemas complexos que apoiam as atividades sociais quotidianas, asseguram o funcionamento das nossas economias em setores determinantes como a saúde, a energia, as finanças e os transportes e apoiam, em especial, o funcionamento do mercado interno.

(2) A utilização de redes e sistemas de informação por cidadãos, organizações e empresas da União é agora generalizada. A digitalização e a conectividade estão a tornar-se características centrais num número cada vez maior de produtos e serviços e, com o surgimento da Internet das coisas (IdC), espera-se que um número extremamente elevado de dispositivos digitais conectados seja implantado em toda a União durante a próxima década. Embora haja cada vez mais dispositivos conectados à Internet, a segurança e a resiliência não são suficientemente integradas na conceção, o que conduz a uma insuficiência a nível da cibersegurança. Nesse contexto, a utilização reduzida da certificação conduz à insuficiência da informação ao dispor dos utilizadores, sejam esses particulares, organizações ou empresas, sobre as características de cibersegurança dos produtos, serviços e processos de TIC, o que compromete a confiança nas soluções digitais. As redes e os sistemas de informação têm capacidade para apoiar todos os aspetos das nossas vidas e impulsionar o crescimento económico da União, constituindo a pedra angular da realização do mercado único digital.

(3) A digitalização e conectividade crescentes acarretam maiores riscos para a cibersegurança, tornando, assim, a sociedade em geral mais vulnerável a ciberameaças e agravando os perigos que as pessoas enfrentam, nomeadamente as pessoas vulneráveis como as crianças. A fim de reduzir esses riscos, têm de ser adotadas todas as medidas necessárias para aumentar a cibersegurança na União de modo a que as redes e os sistemas de informação, as redes de comunicações e os produtos, serviços e dispositivos digitais utilizados pelos cidadãos, organizações e empresas — desde as pequenas e médias empresas (PME) na ação da Recomendação 2003/361/CE da Comissão (4) aos operadores de infraestruturas críticas — estejam melhor protegidos das ciberameaças.

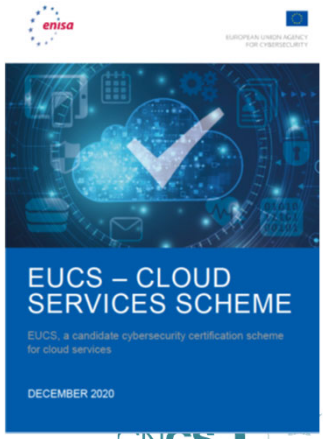
(1) JO C 227 de 28.6.2018, p. 86.
(2) JO C 176 de 23.5.2018, p. 29.
(3) Posição do Parlamento Europeu de 12 de março de 2019 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 9 de abril de 2019.
(4) Recomendação da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

Cybersecurity Act

CNCS Centro Nacional de Cibersegurança PORTUGAL

DL 65/2021 – Cybersecurity certification

- CNCS is the **National Cybersecurity Certification Authority** (NCCA)
- Establishment of a **National Cybersecurity Certification Framework**
  - Develop and implement <u>specific cybersecurity certification schemes</u> for domains not covered by other European schemes
- Carry out its tasks within the **European cybersecurity certification schemes**
  - Supervision
  - Certification



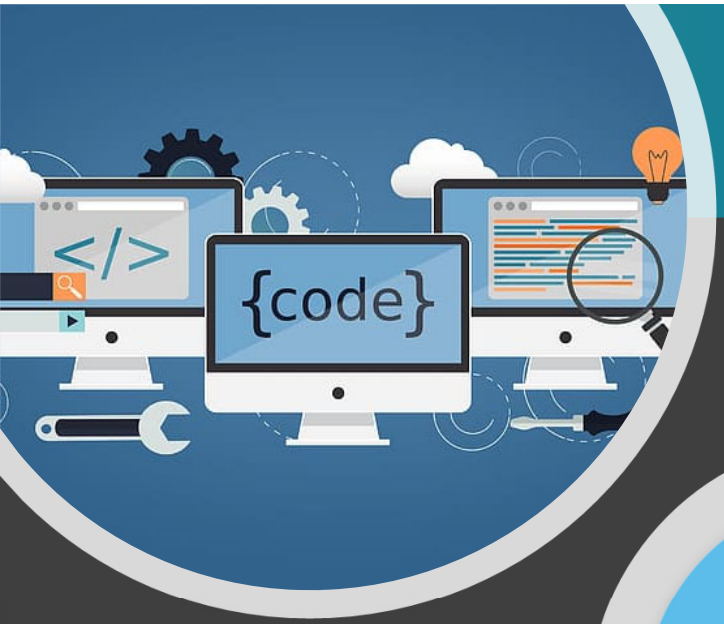
CNCS
Centro Nacional de Cibersegurança
PORTUGAL

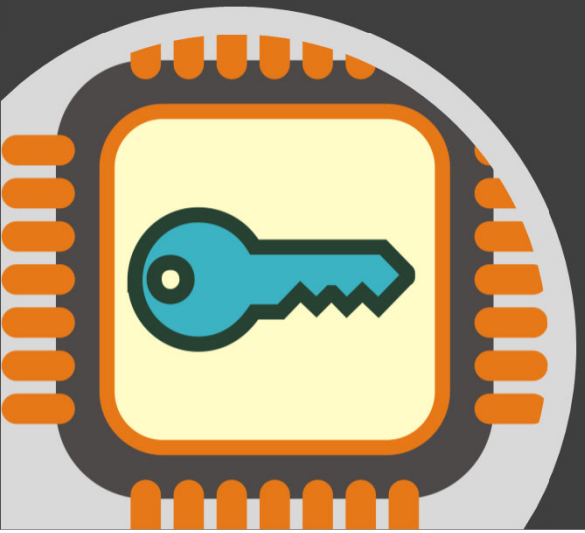
NCRF certification scheme – generic properties

- **Scheme owner and supervisory body – CNCS**
- **Certificate** obtained after successful certification process lead by a NAB (IPAC) – accredited **Certification Body**
- **3 certification levels**
  - **Basic, Substantial, High**
  - **Complementary** and **cumulative levels**
- Certificate **validity** – 3 years
- Focus on **risk analysis** and **management** for the **applicable certification scope**
  - **Main activity** and **related** activities which are **essential**
  - **NCRF mandatory measures** and measures that **may be excluded under certain conditions**

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Regulation n.º 183/2022, of 21 February





The **communication channels** and **procedures** with CNCS and the **required content and formats** for delivering the information to comply with the legal requirements

- **communication channels** and **procedures**
  - Email
  - API
    - Webpage form also to be made available
  - Use of cryptography

Regulation n.º 183/2022, of 21 February

Required content and formats formats for delivering the information to comply with the legal requirements

Permanent point of contact

ANEXO I

(a que se refere o artigo 2.º)

Ponto de contacto permanente

Nome da entidade	Nome do ponto ou pontos de contacto permanente/ serviço disponível ou equipa operacional	Endereço de correio eletrónico principal	Endereço de correio eletrónico alternativo	Número de telefone fixo principal (se aplicável)	Número de telefone móvel principal	Número de telefone fixo alternativo (se aplicável)	Número de telefone móvel alternativo	Outros contactos alternativos

Regulation n.º 183/2022, of 21 February

Required content and formats formats for delivering the information to comply with the legal requirements

Security manager

ANEXO II

(a que se refere o artigo 3.º)

Responsável de segurança

Nome da entidade	Nome do responsável de segurança	Cargo do responsável de segurança	Endereço de correio eletrónico	Número de telefone fixo (se aplicável)	Número de telefone móvel

Regulation n.º 183/2022, of 21 February

Required content and formats formats for delivering the information to comply with the legal requirements

Asset inventory

ANEXO III

(a que se refere o artigo 4.º)

Lista de ativos

Serviço Suportado	Nome do equipamento/ Nome do software	Modelo/Versão	Endereço IP (se aplicável)	FQDN (se aplicável)	Fabricante

Regulation n.º 183/2022, of 21 February

Required content and formats formats for delivering the information to comply with the legal requirements

Annual report

ANEXO IV

(a que se refere o artigo 5.º)

Relatório anual

1 — Designação da entidade:
2 — Ano civil e período de tempo do relatório:
3 — Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação:
4 — Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes:
5 — Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre:
5.1 — Número de utilizadores afetados pela perturbação do serviço
5.2 — Duração dos incidentes
5.3 — Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço
6 — Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação:
7 — Problemas identificados e medidas implementadas na sequência dos incidentes:
8 — Qualquer outra informação relevante:

Data:
Responsável de segurança:
Assinatura do Responsável de segurança:

Cybersecurity reference documents and tools

Documents

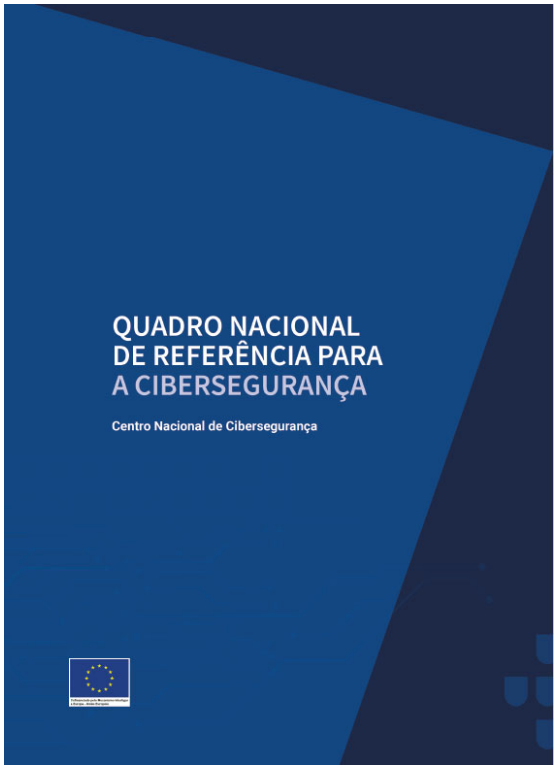
- National Cybersecurity Reference Framework
- Cybersecurity Capabilities Assessment Framework
- Risk Management Guide

Tools

- *CiberCheckUp*
- Minimum Cybersecurity Capabilities Roadmap

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

National Cybersecurity Reference Framework



https://www.cncs.gov.pt/pt/quadro-nacional/

Cybersecurity guide – organises a set of **security measures** for the most common and significant security issues

Provides a **baseline** for an organisation to meet the **minimum recommended information security requirements**

Provides for **examples** and **guidance**

Contributes to the fulfilment of the **National Strategy for Cyberspace Security**

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

National Cybersecurity Reference Framework

Cybersecurity **Standard**

Checklist of actions to be performed

(!) **Mandatory** implementation

Reference and support to cybersecurity **risk management**

Takes into account **human, technological and procedural** dimensions

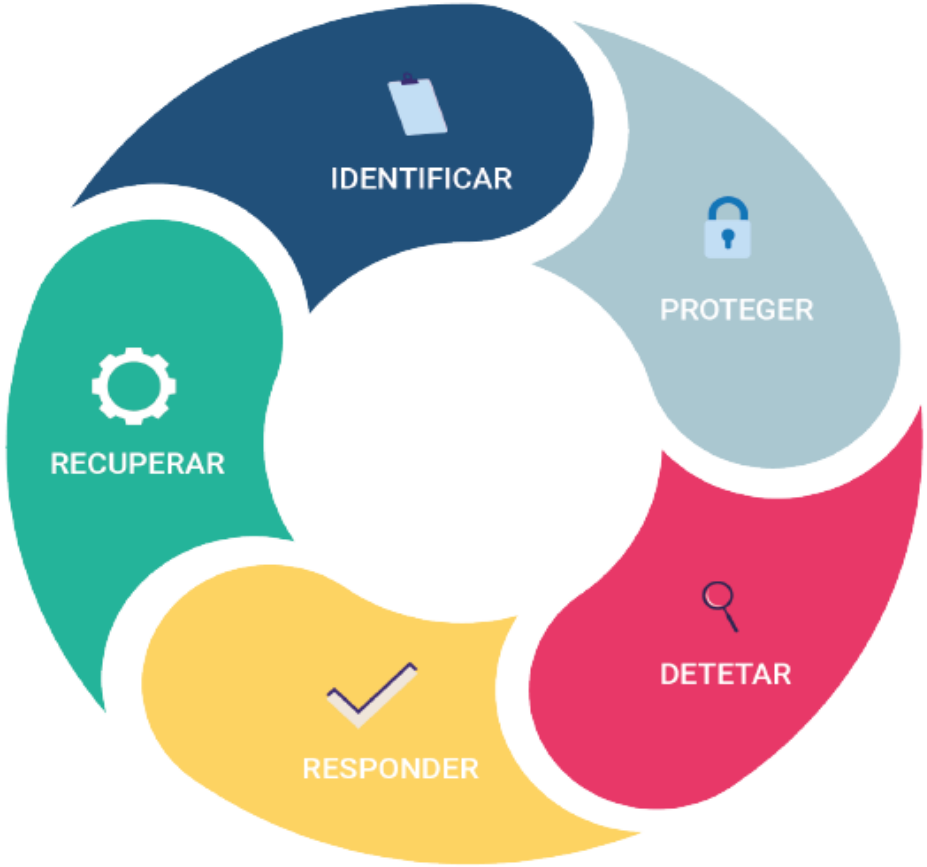
- ✓ **Review of cybersecurity practices**
- ✓ **Systematisation of processes or improvement of existing ones**
- ✓ **Communication of cybersecurity requirements**

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

National Cybersecurity Reference Framework – Structure

Security measures

Cybersecurity goals to be achieved



National Cybersecurity Reference Framework – Example

R.N. CIS CSC, 16; COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03; ISO/IEC 27001:2013, A.7.1.1, A.9.2.1; NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3.

PR.GA-6 - A organização deve verificar a identidade dos colaboradores e vinculá-las às respetivas credenciais

Descrição

A identidade dos colaboradores deve ser vinculada, revista e as suas credenciais confirmadas interativamente, quando necessário.

A verificação de antecedentes deve ser efetuada respeitando a legislação laboral aplicável.

Implementação Técnica

1 Gestão de Identidades e Acessos.

Implementação Processual

A organização deve:

1 Efetuar a verificação de credenciais e referências dos novos colaboradores nos termos permitidos por lei e de forma adequada às funções que o mesmo irá exercer;

2 Implementar um processo formal de registo de novos colaboradores (onde é associado um utilizador único e nominal);

3 Implementar um processo formal de cancelamento de registo de ex-colaboradores;

4 Implementar um processo formal de gestão de acessos.

Evidências

1 Registos das verificações de antecedentes efetuadas;

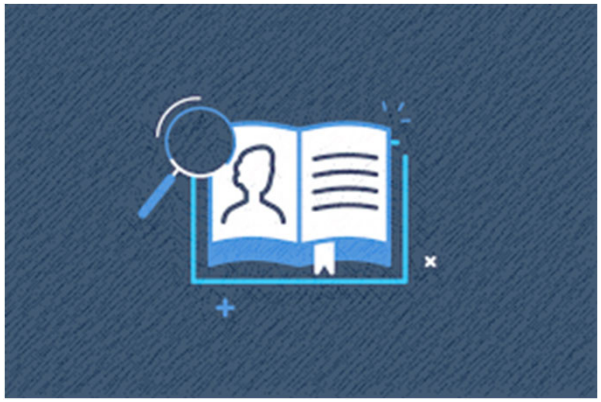
2 Documentos de suporte ao processo de gestão de acessos;

3 Documentos de suporte ao processo de entrada e saída de colaboradores;

4 Registos de funcionamento do processo de entrada e saída de colaboradores e do processo de gestão de acessos.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Reference documents



- **[CIS CSC 7.0]**

  Critical Security Controls catalogue published by the *Center for Internet Security* (CIS)

- **[COBIT 5]**

  ISACA's overarching business and management framework for the governance and management of enterprise IT

- **[ISO/IEC 27001:2013]**

  Standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation

- **NIST SP-800-53 Rev4**

  Set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations, published by NIST

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

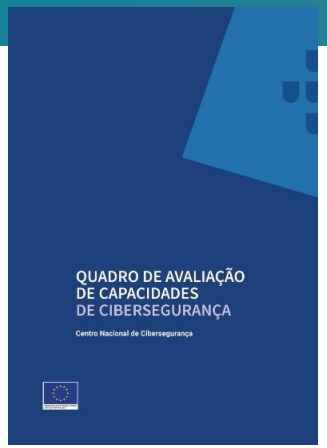
Other tools to improve organisational cybersecurity maturity levels

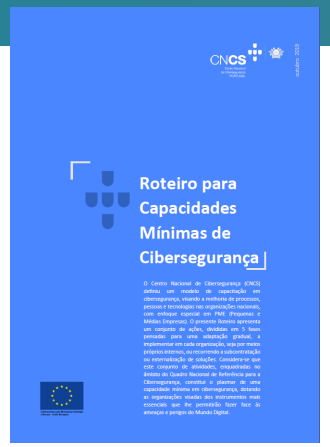
1. **Cybersecurity Capabilities Assessment Framework –** targeted at organisations to support their cybersecurity capacity building; complementary document to the NCRF, implementing CNCS's strategy to provide supporting reference documents and tools

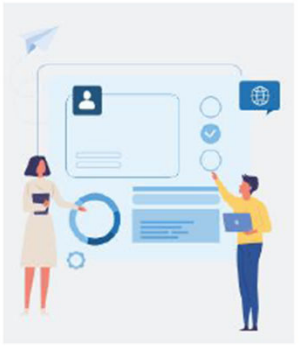
2. **CiberCheckUp** – online tool to assess the cybersecurity maturity of an organisation, considering the NCR and CCA frameworks'

3. **Minimum Cybersecurity Capabilities Roadmap** – guide for cybersecurity capacity building, aimed at improving processes, people and technologies in national organisations, with a particular focus on SMEs

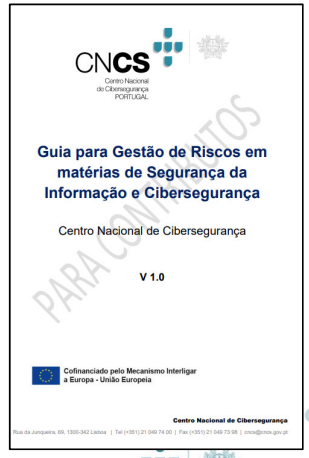
4. **Risk Management Guide –** includes a systematic and coherent approach to the process of analysis, assessment and periodic treatment of risks and how they relate to the scope of provision of a service or production of goods







CIBERCHECKUP



CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Cybersecurity Capabilities Assessment Framework Example

PR.GA-6 - A organização deve verificar a identidade dos colaboradores e vinculá-las às respetivas credenciais

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Inicial	• Os colaboradores têm as suas credenciais e identidades registadas e vinculadas.	• Registo da atribuição de credenciais nominais aos colaboradores.
2 – Intermédio	• Os procedimentos de validação das identidades são registados em políticas; • A organização conta com o apoio sistémico na gestão dos acessos e, quando necessário, na validação interativa das credenciais; • Existe um processo de gestão de identidades e acessos estabelecido, com base na identificação dos colaboradores.	• Documentos com a política e procedimentos que suportam o processo de gestão de identidades e acessos.
3 – Avançado	• A gestão de acessos é revista e avaliada com recorrência e os resultados são utilizados para a melhoria do processo; • Os antecedentes são igualmente revistos com uma determinada periodicidade.	• Existem registos de revisão dos procedimentos de concessão de acessos, suportados pela verificação de antecedentes; • Existe uma equipa dedicada a validar e atribuir identidades.

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Identification of Operators of Essential Services – annual update

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Identification of Operators of Essential Services – annual update

Sector	Subsector	Type of entity
Transport	Water transport	Inland, sea and coastal passenger and freight water transport companies, not including the individual vessels operated by those companies
		Managing bodies of ports, including their port facilities and entities operating works and equipment contained within ports
		Operators of vessel traffic services

Presently: 9 OES

Development of supplementary cybersecurity provisions for the maritime sector

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Supplementary provisions–definition of sectorial security requirements

Reference framework

- ISM CODE – International Safety Management Code 2018
- GCOS – The Guidelines on Cyber Security Onboard Ships
- CoP-Ports – Cyber security for ports and port systems code of practice

5. Estabelecer políticas e procedimentos para o controlo do acesso remoto aos sistemas de TI e TO a bordo. Devem ser estabelecidas diretrizes claras sobre quem tem permissão para aceder, quando pode aceder e o que podem aceder. Quaisquer procedimentos para acesso remoto devem incluir uma coordenação estreita com o capitão do navio e outro pessoal-chave do navio.

Grupo: Gestão de identidades e acessos

Objetivo: Proteger

QNRCS: PR.GA-3

Referências setoriais: GCOS 5.3, CoP-Ports Section 5

12. Disponibilizar os planos de recuperação a bordo e em terra. O objetivo de um plano de recuperação é apoiar a recuperação dos sistemas afetados e dados necessários para restaurar os ativos de TI e TO para um estado operacional. Para ajudar a garantir a segurança do pessoal de bordo, a operação e a navegação do navio devem ser priorizadas no plano. Os detalhes e a complexidade de um plano de recuperação irão depender do tipo de navio e da TI, TO e outros sistemas instalados a bordo.

Grupo: Proteção de Informação

Objetivo: Proteger, Recuperar

QNRCS: PR.PI-4, RC.PR-1, PR.PI-10

Referências setoriais: GCOS 7.2, CoP-Ports Section 5

- Work internally done by CNCS to get acquainted with sectorial best practices
- Inspiration for the joint definition of sectorial security requirements with the Directorate-General for Natural Resources, Safety and Maritime Services (DGRM)

Supplementary provisions–definition of sectorial notification thresholds and procedures

Setor	Subsetor	Tipos de entidades	Parâmetros
Transportes	Transporte marítimo e por vias navegáveis interiores	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, tal como definidas, para o transporte marítimo, no anexo I do Regulamento (CE) 725/2004, não incluindo os navios explorados por essas companhias.	Incidente que resulte em 50% dos transportes previstos serem cancelados ou sofrerem atrasos durante 3 horas ou mais.
		Entidades gestoras dos portos na aceção do artigo 3, ponto 1, da Diretiva 2005/65/CE, incluindo as respetivas instalações portuárias na aceção do artigo 2, ponto 11, do Regulamento (CE) 725/2004, e as entidades que gerem as obras e o equipamento existentes dentro dos portos.	Incidente que resulte em: i) no encerramento de porto por duas horas ou mais; ou ii) no cancelamento ou atraso dos transportes previstos para saída ou chegada a porto durante duas horas ou mais; ou iii) na suspensão de atividade do porto para cargas específicas durante duas horas ou mais.
		Operadores de serviços de tráfego marítimo na aceção do artigo 3, alínea o), da Diretiva 2002/59/CE.	Incidente que resulte em i) disrupção de sistema VTS que cause atrasos de duas horas ou mais no movimento de navios num período de 24 horas; ou ii) encerramento de porto por duas horas ou mais.

Standard Operating Procedures (SOP)

Standard Operating Procedures for joint external communication in case of a cyber incidents or crisis

Standard Operating Procedures *(to be further developed)*

Authorities agree that a statement should be issued and notify the concerned entity, in accordance with pre-determined criteria

Coordination with the concerned entity and consolidation of the statement

CNCS and DGRM issue joint statement in their respective institutional websites

Information Sharing and Analysis Centre for the Port Sector – PortosPT

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PortosPT

- **Terms of Reference**
  - Mission – ***"to increase the resilience of its Members to cyber incidents through consistent information and experience sharing on the basis of mutual trust"***
  - Objectives
  - Principles
  - Organisation and Management
  - Information sharing procedures
- **Concerned parties**
  - **Promoter: CNCS** *(non-member)*
  - **Founding members: 5 entities** representatives of the **Port sector** and of **competent authorities**
  - *… more expected to come*

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt | (+351) 210 497 400