SGMAI
SECRETARIA GERAL
MINISTÉRIO DA ADMINISTRAÇÃO INTERNA

DOSSIER TEMÁTICO

CIBERSEGURANÇA E RESILIÊNCIA DE INFRAESTRUTURAS CRÍTICAS E SERVIÇOS ESSENCIAIS

FICHA TÉCNICA

Título: Cibersegurança e Resiliência de Infraestruturas Críticas e Serviços Essenciais (NIS2/CER)

Dezembro, 2025

Administração Interna / Secretaria-Geral

Direcção de Serviços de Documentação e Relações-Públicas

Divisão de Documentação e Arquivo

SUMÁRIO

Introdução 5

1. Organizações Nacionais de Cibersegurança e Resiliência de Infraestruturas Críticas .. 6

1.1. Estrutura institucional de resiliência **6**

1.2. Estratégia Nacional para a Resiliência das Entidades Críticas e a Avaliação Nacional de Risco **7**

1.3. Organismos Centrais de Coordenação e Segurança **8**

1.4. Órgãos de Coordenação e Consulta (Conselhos Interministeriais e Centros Técnicos) **10**

1.5. Entidades Reguladoras e Autoridades Setoriais **11**

1.6. Iniciativas e Redes estruturantes **14**

2. Organizações e entidades da UE em cibersegurança e infraestruturas críticas 15

2.1. Agências europeias **15**

2.2. Grupos de cooperação **15**

2.3. Entidades reguladoras setoriais **15**

2.4. Iniciativas e redes estruturantes da UE **16**

2.5. Outras estruturas da Comissão Europeia **17**

3. Organizações internacionais extraeuropeias relevantes 18

3.1. Organizações onde Portugal está representado **18**

3.2. Organizações onde Portugal não está representado **19**

4. Enquadramento jurídico e normativo aplicável 21

4.1. Legislação da União Europeia **21**

4.1.1. Legislação Europeia de Base **21**

4.1.2. Regulamentos **22**

4.2. Legislação nacional portuguesa **23**

4.3. Instrumentos não vinculativos da União Europeia **25**

4.4. Acordos e compromissos internacionais de Portugal (UE e NATO) **26**

5. Literatura técnica 27

6. Relatórios, Formação e Capacitação 31

6.1. Incidentes Significativos e Relatórios de Investigação **31**

6.2. Exercícios Práticos de Cibersegurança **36**

6.3. Formação, Treino e Sensibilização **38**

7. Literatura científica 40

7.1. Infraestruturas Críticas no Contexto da Segurança e da Resiliência **40**

7.2. Conformidade com NIS2/CER **41**

7.3. Continuidade de negócios (BCP/DRP) **43**

7.4. Resposta a incidentes e playbooks operacionais **45**

7.5. Avaliação de riscos e auditorias **48**

Introdução

A cibersegurança e a resiliência das infraestruturas críticas e dos serviços essenciais assumiram, na última década, uma centralidade estratégica sem precedentes, em resultado da crescente digitalização e interdependência de setores vitais para o funcionamento da sociedade. Áreas como a energia, a água, os transportes, as comunicações, a saúde, os serviços de emergência (incluindo o 112) e a administração pública dependem hoje de sistemas digitais complexos, interligados e expostos a um conjunto alargado de ameaças cibernéticas, híbridas e físicas. Incidentes recentes, a nível nacional e internacional, demonstram que ataques cibernéticos ou falhas digitais podem provocar interrupções significativas de serviços essenciais, com impactos económicos, sociais e, em alguns casos, na segurança nacional.

Neste contexto, a União Europeia e os Estados-Membros reforçaram de forma substancial o quadro jurídico, institucional e operacional aplicável à proteção e resiliência destas entidades, destacando-se a Diretiva (UE) 2022/2555 (NIS2), a Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas (CER) e o Regulamento (UE) 2022/2554 (DORA). Estes instrumentos elevam o nível de exigência em matéria de gestão de riscos, continuidade de negócio, resposta e reporte de incidentes, impondo às organizações obrigações concretas, verificáveis e sujeitas a supervisão. Paralelamente, organismos internacionais como a NATO, as Nações Unidas, a OCDE e diversas agências especializadas têm vindo a reforçar orientações, exercícios e mecanismos de cooperação, reconhecendo a resiliência das infraestruturas críticas como um pilar essencial da segurança coletiva.

A pertinência deste dossier decorre, assim, da necessidade de sistematizar informação atual, rigorosa e multidisciplinar sobre cibersegurança e resiliência, num período particularmente relevante (2020–2025), marcado por alterações legislativas profundas, pelo aumento da ameaça cibernética e por uma crescente integração entre segurança digital, continuidade operacional e proteção civil. O dossier destina-se sobretudo a técnicos, responsáveis de cibersegurança, decisores e titulares de responsabilidades legais e regulatórias, mas reveste igualmente interesse para um público mais alargado, dado o impacto direto da resiliência das infraestruturas críticas no quotidiano dos cidadãos.

Em termos de estrutura, o dossier organiza-se em oito capítulos: (1) enquadramento nacional, abrangendo entidades, coordenação e regulação; (2) quadro e mecanismos da União Europeia; (3) organizações internacionais relevantes; (4) enquadramento jurídico e normativo, incluindo normas da UE e nacionais, instrumentos não vinculativos e compromissos internacionais; (5–6) literatura técnica e relatórios, com foco em incidentes, exercícios e formação, treino e sensibilização; e (7) literatura científica, organizada por eixos temáticos como infraestruturas críticas no contexto da segurança e da resiliência, conformidade com NIS2/CER, continuidade de negócio (BCP/DRP), resposta a incidentes e playbooks operacionais, e avaliação de riscos e auditorias.

A informação reunida neste dossier baseia-se predominantemente em fontes oficiais, nomeadamente legislação da União Europeia, diplomas legais nacionais, comunicações e relatórios de organismos públicos, agências reguladoras, autoridades nacionais e instituições internacionais (como a Comissão Europeia, a ENISA, a NATO, a OCDE, a ONU e autoridades governamentais de vários países). No que respeita à componente académica, a literatura científica foi selecionada, essencialmente, de bases de dados de conhecimento com, incluindo revistas científicas internacionais reconhecidas (como *International Journal of Critical Infrastructure Protection* e a *Computer Law & Security Review*), bem como publicações indexadas de editoras académicas e associações científicas.

1. Organizações Nacionais de Cibersegurança e Resiliência de Infraestruturas Críticas

1.1. Estrutura institucional de resiliência

- **CNPCE, Conselho Nacional de Planeamento Civil de Emergência e Comissões Setoriais Técnicas**

Natureza: Órgão interministerial de planeamento de emergências civis, criado para cumprir a Diretiva 2008/114/CE, substituída pela atual Diretiva (UE) 2022/2555 e coordenar a proteção de infraestruturas críticas. É presidido pelo Presidente da ANEPC (Proteção Civil) e integrado no Sistema Nacional de Planeamento Civil de Emergência (SNPCE).

Composição: Inclui um vice-presidente (designado pelo Governo), representantes de: Estado-Maior-General das Forças Armadas; Regiões Autónomas Açores e Madeira; Secretário-Geral do Sistema de Segurança Interna; Autoridade Marítima Nacional; GNR; PSP; membro do Governo da área das Finanças; INEM; Agência Portuguesa do Ambiente; os Presidentes das Comissões de Planeamento de Emergência Setoriais.

Competências: Identificação, designação e proteção de infraestruturas críticas nacionais e europeias, bem como promoção da resiliência dessas infraestruturas. O CNPCE avalia as propostas dos vários setores sobre quais instalações devem ser consideradas críticas e aprova a lista final de Infraestruturas Críticas Nacionais (ICN). Comunica depois aos operadores designados a sua classificação e supervisiona que estes elaborem os Planos de Segurança das Infraestruturas Críticas e os Planos de Emergência Internos. O CNPCE aprova também os critérios de identificação de infraestruturas críticas que os setores devem seguir. Em termos de proteção, o CNPCE, em conjunto com o Secretário-Geral do SSI, promove exercícios estratégicos de gestão de crises envolvendo operadores de infraestruturas críticas e autoridades setoriais. Se uma infraestrutura crítica nacional tiver impacto noutro Estado membro, o CNPCE coordena os contactos bilaterais ou multilaterais com esse Estado e com a Comissão Europeia. Além disso, o CNPCE pode propor legislação ou medidas de política ao Governo para colmatar lacunas na resiliência de setores específicos.

Comissões Setoriais de Planeamento de Emergência: São nove comissões técnicas permanentes sob a égide do CNPCE, cada uma dedicada a um setor ou subsetor crítico:
(1)Água e Resíduos; (2)Agricultura e Alimentação; (3)Cibersegurança; (4)Comunicações; (5)Energia; (6)Saúde;(7)Transporte Aéreo; (8)Transporte Marítimo; (9)Transportes Terrestres.
Cada comissão é tipicamente coordenada pelo organismo setorial competente (por ex., Comissão de Energia pelo Ministério da Energia/DGEG, Comissão de Cibersegurança pelo CNCS/GNS, Comissão de Saúde pelo Ministério da Saúde/INFARMED, etc.), e envolve os principais operadores e reguladores desse setor. Essas comissões reúnem-se para elaborar planos setoriais de emergência, partilhar boas práticas de resiliência e articular medidas preventivas. Os presidentes de cada comissão reportam ao CNPCE. Em situações de crise nacional, os coordenadores setoriais do CNPCE podem ser integrados em estruturas de apoio direto ao Primeiro-Ministro na gestão da crise, garantindo que o conhecimento específico de cada setor informa as decisões estratégicas.

Ligação a Entidades Europeias: O CNPCE é, por função, o ponto de contacto nacional para a Diretiva de Infraestruturas Críticas Europeias (2008/114/CE) e agora para a nova Diretiva (UE) 2022/2557 de resiliência de entidades críticas. Interage com a Comissão Europeia reportando as ICN (Infraestruturas Críticas Nacionais) e ICE (Infraestruturas Críticas Europeias) designadas, e coopera na troca de informações sensíveis de forma classificada por via do GNS (que fornece as

credenciações de segurança necessárias). Assim, Portugal está representado no ECC (Critical Entities Resilience Group) previsto na nova diretiva, onde os Estados trocam experiências sobre avaliação de riscos e boas práticas setoriais. Através das comissões setoriais, liga-se a redes europeias específicas, por exemplo, a Comissão de Comunicação irá interagir com o NIS Cooperation Group na vertente telecom, a de Saúde com o Health Security Committee da UE, etc. Em resumo, o CNPCE é o mecanismo que permite a Portugal falar a "uma só voz" no contexto europeu de proteção de infraestruturas críticas.

- **SSI, Secretário-Geral do Sistema de Segurança Interna**

Natureza: O Serviço de Informações de Segurança (SSI) é um serviço integrado no Sistema de Informações da República Portuguesa (SIRP), com natureza civil e âmbito nacional. Tem como missão principal assegurar a produção de informações necessárias à garantia da segurança interna, à defesa da ordem constitucional e à salvaguarda dos interesses fundamentais do Estado, incluindo a prevenção de ameaças que possam afetar infraestruturas críticas e serviços essenciais, nomeadamente no domínio cibernético.

Composição: O SSI, sob a tutela do Primeiro-Ministro, atua em estreita articulação com o Serviço de Informações Estratégicas de Defesa (SIED), bem como com outras entidades nacionais com competências nas áreas da segurança interna, da cibersegurança e da proteção de infraestruturas críticas.

Competências: O SSI recolhe, analisa e produz informações sobre ameaças à segurança interna, incluindo cibernéticas, híbridas e terroristas, avaliando riscos para infraestruturas críticas e para a continuidade de serviços essenciais. Apoia a prevenção de espionagem, sabotagem e ataques com impacto na segurança nacional e coopera com as entidades nacionais competentes, designadamente o Centro Nacional de Cibersegurança, na partilha de informação e na mitigação de riscos. Em articulação com as entidades responsáveis pela resiliência, contribui para uma estrutura coordenada de reforço da resiliência, incluindo a aprovação e acompanhamento de planos, receção de notificações de incidentes, realização de auditorias/inspeções e aplicação de sanções, quando aplicável, com execução setorial assegurada pelas entidades competentes e forças de segurança.

Ligação a Entidades Europeias: O SSI coopera com serviços de informações e entidades de segurança dos Estados-Membros da União Europeia, no respeito pelos enquadramentos legais nacionais e europeus. Participa em mecanismos de cooperação e partilha de informação relevantes para a segurança interna, contribuindo para iniciativas europeias no domínio da proteção e resiliência das entidades críticas, bem como para a prevenção e resposta a ameaças transnacionais, incluindo no ciberespaço.

1.2. Estratégia Nacional para a Resiliência das Entidades Críticas e a Avaliação Nacional de Risco

A Estratégia Nacional para a Resiliência das Entidades Críticas e a Avaliação Nacional de Risco devem ser aprovadas **até 17 de janeiro de 2026**, mantendo-se em vigor, até lá, os instrumentos previstos no Decreto-Lei n.º 20/2022, de 28 de janeiro. Será igualmente criada uma plataforma eletrónica de registo de informação sobre entidades e infraestruturas críticas, que poderá integrar informação classificada. Plataforma Nacional para a Redução do Risco de Catástrofes

1.3. Organismos Centrais de Coordenação e Segurança

- **Centro Nacional de Cibersegurança (CNCS)**

Tutela: Funciona no âmbito do **Gabinete Nacional de Segurança (GNS)**, sob a tutela da Presidência do Conselho de Ministros (Ministro da Presidência). O coordenador do CNCS é simultaneamente subdiretor-geral do GNS.

Competências: Autoridade Nacional de Cibersegurança responsável por promover o uso livre, confiável e seguro do ciberespaço em Portugal, através do desenvolvimento de capacidades de prevenção, monitorização, deteção, reação e recuperação face a incidentes ou ciberataques. O CNCS é a entidade designada pela Lei n.º 46/2018, de 13 de agosto como autoridade nacional para a segurança do ciberespaço, coordenando a implementação da Diretiva NIS2. Integra o CERT.PT, a equipa nacional de resposta a incidentes de segurança informática. Também emite instruções técnicas e recebe notificações de incidentes das entidades obrigadas (Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais).

Setores Abrangidos: Todos os setores da Administração Pública e da economia abrangidos pelo regime de segurança do ciberespaço, incluindo infraestruturas críticas, serviços essenciais (energia, águas, transportes, saúde, financeiro, etc.) e prestadores digitais. Atua transversalmente como autoridade central, em articulação com autoridades setoriais quando existam.

Ligações Europeias: Representa Portugal nos organismos europeus de cibersegurança, participa no Grupo de Cooperação NIS da UE e na rede de equipas CSIRT (Computer Security Incident Response Team) europeias. Coopera estreitamente com a ENISA (Agência da UE para a Cibersegurança) em exercícios, formações e desenvolvimento de capacidades nacionais. O CNCS foi também designado Centro de Coordenação Nacional no âmbito do Centro Europeu de Competências em Cibersegurança.

- **Gabinete Nacional de Segurança (GNS)**

Tutela: Presidência do Conselho de Ministros (atualmente sob o Ministro da Presidência). É um serviço central da administração direta do Estado, com autonomia administrativa, dependente do Primeiro-Ministro ou membro do Governo em quem ele delegar.

Competências: É a Autoridade Nacional de Segurança (ANS), responsável em exclusivo pela proteção e salvaguarda da informação classificada no âmbito nacional e das organizações internacionais de que Portugal faz parte (NATO, UE, etc.). Exerce funções de credenciação de segurança de pessoas e empresas para acesso a matéria classificada e funções de autoridade credenciadora e fiscalizadora no âmbito do Sistema de Certificação Eletrónica do Estado, Infraestrutura de Chaves Públicas. No GNS está integrado o CNCS, pelo que o GNS também intervém na estratégia nacional de cibersegurança. O diretor-geral do GNS é por inerência a Autoridade Nacional de Segurança.

Setores Abrangidos: Abrange transversalmente todos os setores do Estado que lidam com informação classificada (defesa, diplomacia, segurança interna, etc.), garantindo procedimentos uniformes de segurança. Participa na coordenação da segurança de infraestruturas críticas quando envolvam informação classificada ou matérias de alto sigilo.

Ligações Europeias e Internacionais: Atua como ponto de contacto nacional para segurança da informação no âmbito da NATO e da UE. Participa em fóruns internacionais de autoridades de segurança e coopera com as congéneres dos países aliados.

- **Autoridade Nacional de Emergência e Proteção Civil (ANEPC)**

Tutela: Ministério da Administração Interna. É um serviço central da administração direta do Estado, com autonomia administrativa e financeira.

Competências: Planear, coordenar e executar as políticas de proteção civil e emergência, incluindo a prevenção, preparação, resposta e recuperação face a acidentes graves ou catástrofes. Coordena os agentes de proteção civil (bombeiros, forças de segurança, Forças Armadas quando ativas, INEM, etc.) e assegura o funcionamento do Sistema Integrado de Operações de Proteção e Socorro em cenários de emergência. No domínio específico do planeamento civil de emergência, a ANEPC assegura e coordena as necessidades nacionais de planeamento para fazer face a situações de crise ou guerra, incluindo a proteção de infraestruturas críticas. A ANEPC preside ao Conselho Nacional de Planeamento Civil de Emergência (CNPCE), órgão que identifica e designa oficialmente as infraestruturas críticas nacionais. No âmbito do CNPCE, a ANEPC coordena as Comissões de Planeamento de Emergência Setoriais (ver secção consultiva abaixo) para os setores de energia, transportes, comunicações, água, saúde, etc. Também elabora planos de emergência (nacional e distritais) e promove exercícios de teste à resiliência.

Setores Abrangidos: Todos os setores considerados nos planos de emergência e critério de "serviços vitais", nomeadamente Proteção Civil geral (incêndios, cheias, sismos, etc.), e nas infraestruturas críticas abrange energia, comunicações, transportes (rodoviário, ferroviário, aéreo, marítimo), água e resíduos, alimentação, saúde, financeiro, órgãos de soberania, etc. através das respetivas comissões setoriais. Em situações de crise graves, a ANEPC e o CNPCE articulam a resposta nacional junto do Primeiro-Ministro e do Sistema de Segurança Interna .

Ligações Europeias: Representa Portugal no Mecanismo de Proteção Civil da União Europeia, participando no Centro de Coordenação de Resposta de Emergência da UE e em equipas europeias de proteção civil. Coordena a participação nacional em missões internacionais de proteção civil. No âmbito da Diretiva (UE) 2022/2557 (Resiliência de Entidades Críticas), a ANEPC tem responsabilidade na implementação nacional (identificação de entidades críticas através do CNPCE e supervisão dos planos de resiliência). Também coopera com a NATO na área do Planeamento Civil de Emergência (Civil Emergency Planning).

- **Polícia Judiciária,Unidade Nacional de Combate ao Cibercrime (UNC3T)**

Sigla e Nome: PJ, Polícia Judiciária, através da UNC3T (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica)

Tutela: Ministério da Justiça. A Polícia Judiciária é a polícia de investigação criminal de competência genérica, com autonomia técnica. A UNC3T é uma unidade especializada da PJ.

Competências: Prevenção, deteção e investigação criminal de crimes informáticos e ciberataques de alto impacto, bem como de crimes cometidos com recurso a meios tecnológicos. Por lei, a PJ detém competência reservada para investigar a criminalidade informática grave (Lei do Cibercrime - Lei n.º 109/2009, de 15 de setembro) e outros crimes tecnológicos. A **UNC3T** dá resposta preventiva e repressiva ao fenómeno do cibercrime a nível nacional. Investiga crimes previstos na Lei do Cibercrime (acesso ilegítimo, dano em programas ou dados, sabotagem informática, etc.), crimes informáticos contra dados pessoais, fraudes informáticas e nas comunicações, ataques a meios de pagamento eletrónico, espionagem informática (APT) e ciberterrorismo, entre outros. Compete-lhe centralizar informação criminal sobre cibercrime e elaborar análises estratégicas sobre estas ameaças. Importa salientar que a PJ, através da UNC3T, colabora diretamente com as entidades nacionais de cibersegurança,

designadamente o **CNCS**, em ações de prevenção, deteção e investigação de incidentes que afetem a segurança nacional do ciberespaço. A UNC3T articula-se com o CNCS na elaboração do Plano Nacional de Prevenção e Combate ao Cibercrime e participa em fóruns de partilha de informação técnico-científica sobre cibersegurança.

Setores Abrangidos: Atua transversalmente em todos os setores em que ocorram crimes cibernéticos. Tem particular relevância na resposta a incidentes que atingem infraestruturas críticas ou serviços essenciais, como ataques a redes de energia, telecomunicações, sistema financeiro, saúde, administração pública, etc., sempre que constituam ilícitos criminais. Nesses casos, a PJ conduz a investigação para identificar autores e os levar à justiça, ao mesmo tempo que colabora com as entidades setoriais e de cibersegurança para mitigar o incidente.

Ligações Europeias: A PJ é o ponto de contacto nacional para a Europol/EC3 (European Cybercrime Centre) e para a rede de unidades de cibercrime da UE, facilitando cooperação policial internacional em investigações transnacionais. Participa em equipas conjuntas de investigação de cibercrime e troca informação através da Interpol e outras redes. A UNC3T integra ainda o grupo *Joint Cybercrime Action Taskforce* (J-CAT) da Europol. Adicionalmente, a PJ representa Portugal no CSIRT Network europeu através da UNC3T sempre que necessário (a PJ possui um CERT interno e integra a Rede Nacional de CSIRTs como observador, para melhor articular a resposta a incidentes).

1.4. Órgãos de Coordenação e Consulta (Conselhos Interministeriais e Centros Técnicos)

- **Conselho Superior de Segurança do Ciberespaço (CSSC)**

Natureza: Órgão específico de consulta e coordenação estratégica do Primeiro-Ministro para assuntos de segurança do ciberespaço. Criado pela Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto funciona como um *"conselho nacional de cibersegurança"* de alto nível.

Composição: [Ver: Despacho n.º 1195/2018, de 2 de fevereiro]. Reúne os principais responsáveis governamentais e técnicos ligados à segurança digital: Primeiro-Ministro (que preside) ou Ministro designado; a Autoridade Nacional de Segurança (Dir. Geral do GNS, vice-presidente); Secretário-Geral do SSI (Segurança Interna); Secretário-Geral do SIRP (informações da República); Diretor do SIS; Coordenador do CNCS; Embaixador para a diplomacia digital; Presidente da AMA (Administração Digital); Diretor da AT (Autoridade Tributária); representante das Forças Armadas (Dir. Comunicações do EMGFA); representantes das forças de segurança (Rede Nacional de Segurança Interna); Diretor do IGFEJ (Justiça); Diretor da UNC3T da PJ; representante do Ministério Público; Presidente da FCT (Ciência e Tecnologia); Diretor-Geral da Educação; Presidente do Conselho de Administração dos SPMS (Saúde); Presidente executivo da Infraestruturas de Portugal; Presidente do IAPMEI (PME); um representante da Rede Nacional de CSIRTs. Pode convidar também entidades privadas e peritos. Esta composição ampla abrange governo, segurança, defesa, academia e operadores de infraestruturas, assegurando uma abordagem 360º.

Competências: Apoiar o Primeiro-Ministro na definição da estratégia nacional de cibersegurança e na coordenação das políticas setoriais. O CSSC emite pareceres e recomendações sobre matérias de cibersegurança de âmbito nacional, por exemplo, deliberou critérios de risco de fornecedores 5G, recomendando restrições a equipamentos de alto risco. Elabora relatórios anuais de avaliação da execução da Estratégia Nacional de Segurança do Ciberespaço. Em caso de grandes incidentes de cibersegurança nacionais, pode ser convocado

para aconselhar medidas de resposta e recuperação (embora a resposta operacional caiba ao CNCS/CERT.PT e outras autoridades). O CSSC promove a articulação interministerial, ex.: garante que as orientações estratégicas de cibersegurança são coerentes com a Estratégia Digital, com os planos setoriais TIC de cada ministério, etc. Serve ainda de fórum para partilha de informação de alto nível entre os diversos domínios (civil, militar, interno, privado). Sua existência reforça a unidade de esforços face a ameaças cibernéticas.

Ligação a Entidades Europeias: Embora o CSSC seja interno, pelos seus membros ele conecta-se aos fóruns europeus. Por exemplo, as deliberações do CSSC podem informar a posição portuguesa no NIS Cooperation Group e reuniões de ministros. Além disso, o facto de nele participarem diplomacia (Embaixador, diplomacia digital) e economia (IAPMEI) demonstra alinhamento com estratégias da UE (Estratégia de Cibersegurança da UE) e iniciativa de Diplomacia Digital. O CSSC também acolhe discussões sobre cumprimento de diretivas UE (NIS/NIS2, CER) transversalmente.

1.5. Entidades Reguladoras e Autoridades Setoriais

- **ANAC, Autoridade Nacional da Aviação Civil**

A ANAC é uma autoridade administrativa independente com atribuições de regulador técnico e económico no setor da aviação, sob a tutela do Ministério das Infraestruturas. Supervisiona segurança da aviação civil. Coordena planos de cibersegurança para aeroportos e sistemas de navegação aérea, em articulação com a EASA, promovendo a resiliência digital na aviação.

- **ANACOM, Autoridade Nacional de Comunicações**

Autoridade administrativa independente, com estatuto de regulador para as comunicações. Tem autonomia administrativa e financeira [Decreto-Lei n.º 39/2015, de 16 de março]. A ANACOM assume, ainda, as atribuições e competências de Autoridade Nacional Sectorial de Cibersegurança, no que respeita à matéria das comunicações eletrónicas e do serviço postal, ao abrigo do Decreto-Lei n.º 125/2025, de 4 de dezembro

- **ASF, Autoridade de Supervisão de Seguros e Fundos de Pensões**

Entidade administrativa independente, sob alçada genérica do Ministério das Finanças. Regula seguros e fundos de pensões. Avalia ciber-riscos nas seguradoras, exige planos de contingência e participa na coordenação europeia - EIOPA - de resiliência digital do setor financeiro.

- **BANCO DE PORTUGAL, Autoridade Supervisora Financeira e Banco Central**

É o banco central da República Portuguesa, parte integrante do Eurosistema do Banco Central Europeu (BCE). Tem estatuto de independência definido nos tratados da UE e na Lei Orgânica do Banco de Portugal. Em termos nacionais, embora independente funcionalmente, relaciona-se com o Ministério das Finanças para certos efeitos (o Governador do BdP participa no Conselho Nacional de Supervisores Financeiros junto do Ministério).

Supervisiona infraestruturas críticas do sistema financeiro e aplica o regulamento DORA. Exige planos de continuidade, resposta a incidentes cibernéticos e realiza testes de resiliência digital a bancos e sistemas de pagamentos.

- **CMVM, Comissão do Mercado de Valores Mobiliários**

Autoridade administrativa independente, sujeita a supervisão genérica do Ministério das Finanças. A CMVM supervisiona os mercados de capitais em Portugal. Supervisiona infraestruturas de mercado financeiro. Atua na ciber-resiliência através de auditorias digitais, testes de continuidade e requisitos técnicos para plataformas críticas, alinhados com DORA e a ESMA.

- **DGEG, Direção-Geral de Energia e Geologia**

A Direção-Geral de Energia e Geologia (DGEG) é um serviço da administração central direta do Estado e tem como missão Contribuir para a conceção, promoção e avaliação das políticas energéticas e dos recursos geológicos nacionais Supervisiona infraestruturas energéticas e elabora planos de emergência energética. No domínio da ciber-resiliência, coordena com ERSE e ENSE a preparação para falhas digitais e a aplicação de requisitos NIS2 no setor da energia.

- **ENSE, Entidade Nacional para o Setor Energético, E.P.E.**

A ENSE é uma entidade pública empresarial cujo capital estatutário é detido pelo Estado (Direção-Geral do Tesouro e Finanças). Resultou da reestruturação da antiga ENMC em 2018, concentrando funções de fiscalização que antes cabiam à ASAE, DGEG e ENMC.
Fiscaliza a segurança operacional no setor energético e coordena respostas a emergências. Tem papel ativo na ciber-resiliência através da gestão de riscos operacionais, simulações de falhas e inspeções de segurança digital em operadores críticos de energia.

- **E-REDES, Distribuição de Eletricidade, S.A.**

Empresa privada (do Grupo EDP, antiga EDP Distribuição). Opera sob contrato de concessão pública celebrado com os Municípios (78 concelhos em baixa tensão) e sob licença do Estado (rede nacional de distribuição em alta e média tensão). É regulada pela ERSE.
Opera a distribuição elétrica nacional. Implementa medidas NIS2, possui equipa CERT interna e sistemas de monitorização contínua para garantir resiliência e recuperação rápida em caso de incidentes.

- **ERSAR, Entidade Reguladora dos Serviços de Águas e Resíduos**

Está integrada na administração indireta do Estado, sendo uma entidade administrativa independente. Embora possua autonomia funcional, técnica e financeira, exerce as suas funções sob a tutela do Ministério do Ambiente e da Ação Climática. Regula os serviços de água. Exige planos de segurança da água, avaliações de risco digital e promove resiliência em sistemas SCADA e telemetria, essenciais ao abastecimento público.

- **ERSE, Entidade Reguladora dos Serviços Energéticos**

Entidade administrativa independente (autoridade reguladora) com autonomia orgânica, funcional e financeira. A ERSE rege-se pelos seus Estatutos (aprovados pelo Decreto-Lei n.º 97/2002, de 12 de abril e atualizados), com dever de prestação de contas ao Governo (Ministério do Ambiente e Ação Climática/Energia) e à Assembleia da República.
Regula o setor energético (eletricidade e gás) com foco na continuidade e segurança do fornecimento. No âmbito da ciber-resiliência, exige planos de segurança e continuidade dos operadores, acompanha a implementação de medidas NIS2 e coordena com a ACER e a ENTSO-E respostas a riscos digitais.

- **IMT, Instituto da Mobilidade e dos Transportes, I.P. / AMT, Autoridade da Mobilidade e dos Transportes**

O IMT é um instituto público, tutelado pelo Ministério das Infraestruturas, que exerce funções executivas e regulamentares no setor dos transportes terrestres e marítimos. A AMT é uma pessoa coletiva de direito público com a natureza de entidade administrativa independente, dotada de autonomia administrativa, financeira e de gestão, bem como de património próprio, sob a tutela do Ministério das Infraestruturas. Tem como missão regular e fiscalizar os transportes terrestres, fluviais, ferroviários, marítimos e respetivas infraestruturas, promovendo a concorrência e protegendo os direitos dos consumidores através de poderes de regulamentação, supervisão e sancionamento.

Avaliam riscos operacionais e cibernéticos nos setores de transporte terrestre, ferroviário e marítimo. Colaboram com entidades europeias (ERA, EMSA) na aplicação de requisitos de ciber-resiliência a operadores e infraestruturas críticas.

- **INFARMED, Autoridade Nacional do Medicamento e Produtos de Saúde, I.P.**

O Infarmed é um instituto público com autonomia administrativa e financeira, integrado na administração indireta do Estado. Atua sob tutela do Ministério da Saúde e é responsável por funções atribuídas a este ministério na área do medicamento e produtos de saúde. Atua na ciber-resiliência através da monitorização de sistemas críticos de logística de medicamentos, integrando redes de alerta sanitário e partilha de incidentes de cibersegurança no setor da saúde.

- **INFRAESTRUTURAS de Portugal, S.A. (IP)**

Empresa pública (S.A. de capitais 100% públicos, resultante da fusão REFER+EP em 2015). Está sob tutela conjunta dos Ministérios das Infraestruturas e habitação e das Finanças. Tem a responsabilidade de construir, manter e gerir as redes ferroviária e rodoviária de âmbito nacional.

Avalia vulnerabilidades digitais, protege sistemas de controlo e sinalização (ex: ERTMS) e colabora com forças de segurança em protocolos de ciberproteção de infraestruturas físicas e digitais.

- **NAV Portugal, Navegação Aérea de Portugal, E.P.E.**

Entidade pública empresarial (E.P.E.) tutelada pelo Ministério das Infraestruturas e Habitação e o Ministério das Finanças. A NAV é o prestador do serviço público de navegação aérea no espaço aéreo português, cobrindo as Regiões de Informação de Voo (FIR) de Lisboa e Santa Maria (Açores). Fornece os serviços de controlo de tráfego aéreo (ATC), controlo de área (centro de Lisboa e Santa Maria), controlo de aproximação e controlo de aeródromo (torres nos principais aeroportos); assim como serviços de informação de voo e alerta. Também opera os sistemas e equipamentos de auxílio à navegação (radares, comunicações ar-terra, sistemas de gestão ATM).

Responsável pela navegação aérea. Tem centros de contingência e planos de falha para continuidade operacional. Implementa medidas avançadas de cibersegurança no controlo do tráfego aéreo, articulando com Eurocontrol e projetos SESAR.

- **REN, Redes Energéticas Nacionais, S.A.**

Empresa privada (sociedade anónima cotada em bolsa), com participação significativa de capitais nacionais e estrangeiros. Embora privada, é concessionária de serviços públicos de transporte de energia sob regulação do Estado (ERSE).
Opera redes de transporte de eletricidade e gás. Possui planos robustos de cibersegurança, segmentação de redes OT/IT, redundância operacional e protocolos de resposta rápida a incidentes cibernéticos. Participa em exercícios europeus (ENTSO-E).

- **SPMS, EPE Serviços Partilhados do Ministério da Saúde**

Desenvolve atividades de cibersegurança no âmbito do Serviço Nacional de Saúde (SNS) para proteger a informação, os sistemas e as infra-estruturas digitais do setor da saúde. O seu trabalho inclui a gestão de incidentes através da equipa CSIRT-SPMS (Computer Security Incident Response Team), participação em redes nacionais e internacionais de resposta a incidentes, promoção de boas práticas de segurança digital, formação de profissionais e gestores, sensibilização dos utilizadores, e cooperação com outras entidades em exercícios, workshops e iniciativas específicas de segurança. A SPMS também apoia ações como simulações de phishing e a adoção de medidas técnicas de proteção, reforçando a cultura de cibersegurança no SNS face à crescente sofisticação das ameaças digitais.

1.6. Iniciativas e Redes estruturantes

- **Aliança para a Cibersegurança**.

A Aliança para a Cibersegurança é uma comunidade colaborativa promovida pelo CNCS que reúne entidades públicas e privadas para reforçar a cultura de cibersegurança e a partilha de informação sobre ameaças e boas práticas.

- **ISAC (Information Sharing and Analysis Centers)**

As Comunidades Setoriais de Cibersegurança (ISACs), dinamizadas pelo CNCS em parceria com operadores, são grupos de partilha e análise de informação que reúnem entidades de setores críticos para trocar, em ambiente de confiança, dados sobre ciberameaças (incluindo indicadores de comprometimento), vulnerabilidades, boas práticas e lições aprendidas, facilitando alertas precoces e coordenação durante incidentes.

- **ISAC EnergyPT**

O ISAC EnergyPT é um fórum setorial de cooperação em cibersegurança criado em Portugal e dinamizado pelo Centro Nacional de Cibersegurança (CNCS) para equipas de cibersegurança de organizações que operam no setor energético. O objetivo do ISAC é criar laços de confiança entre os seus membros, promover um ambiente colaborativo e facilitar a partilha de informação, indicadores de ameaça e melhores práticas entre operadores críticos de energia.

2. Organizações e entidades da UE em cibersegurança e infraestruturas críticas

2.1. Agências europeias

- **ENISA (Agência da União Europeia para a Cibersegurança)**

Agência da UE especializada em segurança informática. Fornece conhecimento técnico, apoio e coordenação às políticas de cibersegurança da UE, reforçando a resiliência de setores críticos (energia, telecom, finanças, etc.)

- **EU-CyCLONe (European Cyber Crisis Liaison Organisation Network)**

Rede de cooperação entre as autoridades nacionais responsáveis por gestão de crises cibernéticas. Facilita a partilha de informação e coordenação operacional em incidentes de grande escala.

2.2. Grupos de cooperação

- **NIS Cooperation Group**

Grupo estabelecido pela diretiva NIS/NIS2 que reúne Estados-Membros, Comissão e ENISA. Promove cooperação estratégica e troca de informação para elevar o nível comum de segurança em sistemas de rede e informação na EU.

- **Rede de CSIRTs da UE**

Rede operacional de equipas nacionais de resposta a incidentes informáticos (Computer Security Incident Response Teams). Estabelecida pela diretiva NIS, essa rede partilha avisos de ameaças e coordena ações técnicas em incidentes cibernéticos transfronteiriços, sob orientação do NIS Cooperation Group

2.3. Entidades reguladoras setoriais

- **ACER (Agência para a Cooperação dos Reguladores de Energia)**

Agência que coordena reguladores nacionais de eletricidade e gás. Visa integrar mercados energéticos europeus e garantir fornecimento fiável de energia. Publica diretrizes comuns, incluindo regras de cibersegurança para o setor elétrico (rede de transporte).

- **ENTSO-E (Rede Europeia de Operadores dos Sistemas de Transporte de Eletricidade)**
  Associação dos operadores de redes de transporte elétrico da UE. Tem mandato legal para garantir a segurança e fiabilidade da rede elétrica transnacional e desenvolver códigos de rede, incluindo normas de cibersegurança e planos de resposta a incidentes para o setor de eletricidade.

- **ENTSO-G (Rede Europeia de Operadores dos Sistemas de Transporte de Gás)**

Associação dos operadores de redes de transporte de gás da UE. Coordena planeamento de rede e medidas de segurança de abastecimento de gás natural ao nível europeu, contribuindo para a resiliência das infraestruturas críticas de energia.

- **ERGA (European Regulators Group for Audiovisual Media Services)**

Grupo de reguladores nacionais de serviços audiovisuais (rádio, TV, vídeo online). Assessora a Comissão na aplicação da Diretiva de Media Audiovisuais, tratando de questões de segurança online dos conteúdos (ex. proteção de menores, discursos de ódio).

- **ERA (Agência Ferroviária da UE)**

Agência que harmoniza normas técnicas e de segurança no setor ferroviário europeu. Trabalha na interoperabilidade e certificação de veículos e na segurança de sistemas críticos de sinalização (como o ERTMS), incluindo requisitos de cibersegurança para os sistemas de controle ferroviário.

- **EMSA (Agência Europeia de Segurança Marítima)**

Agência da UE para segurança marítima. Reduz riscos de acidentes e poluição nos mares europeus apoiando a fiscalização de normas de segurança de navios e portos. Emite orientações para inspeções de navios que incluem elementos de cibersegurança a bordo, reforçando a proteção das infraestruturas marítimas críticas.

- **BEREC (Body of European Regulators for Electronic Communications)**

Órgão que reúne reguladores nacionais de telecomunicações. Promove a aplicação consistente do quadro regulatório de comunicações eletrónicas na UE, assegurando mercados de telecomunicações integrados e a resiliência das redes digitais de comunicação.

- **EBA (Autoridade Bancária Europeia)**

Agência da UE que supervisiona a estabilidade do sistema bancário. Estabelece regras prudenciais, incluindo diretivas sobre gestão de riscos de TIC (como orientações de resiliência digital alinhadas com o Regulamento DORA), para proteger as infraestruturas financeiras essenciais.

- **ESMA (Autoridade Europeia dos Valores Mobiliários e dos Mercados)**

Supervisor das bolsas e mercados financeiros da UE. Regula produtos financeiros transfronteiriços e promove a resiliência digital das empresas financeiras. Em 2025, incluiu cyber-resiliência e gestão de risco TIC como prioridades estratégicas da supervisão, alinhada com a implementação do DORA.

- **EIOPA (Autoridade Europeia de Seguros e Pensões Complementares)**

Regula o setor segurador e de pensões na UE. Como parte das Autoridades Europeias de Supervisão Financeira (ESAs), destaca a necessidade de reforçar a ciberresiliência financeira. Num relatório conjunto de 2025, os ESAs (EBA, ESMA e EIOPA) alertam para riscos cibernéticos crescentes e reforçam a gestão proativa de risco em instituições financeiras.

2.4. Iniciativas e redes estruturantes da UE

- **ISACs europeus (Information Sharing and Analysis Centers)**

Plataformas público-privadas setoriais para partilha de inteligência sobre ameaças. São centros sem fins lucrativos que reúnem empresas e entidades públicas de um mesmo setor (energia, finanças, transportes, etc.) para trocar informação de segurança e melhorar a resiliência cibernética coletiva. A ENISA apoia ativamente a criação e funcionamento dessas ISACs, promovendo exercícios conjuntos e boas práticas.

- **PESCO (Cooperação Estruturada Permanente)**

Marco formal de cooperação em defesa entre Estados-Membros (26 participantes), criado em 2017. Permite desenvolver capacidades militares comuns através de projetos colaborativos. Vários projetos PESCO são dedicados à cibersegurança e resposta a incidentes (como Equipas de Resposta Rápida Cibernéticas), reforçando a segurança digital no âmbito da defesa.

- **Major Cities of Europe (MCE)**

Rede de grandes cidades europeias para cooperação em segurança urbana e tecnologia da informação. Reúne CIOs/CISOs municipais para partilhar experiências de defesa cibernética urbana. Por exemplo, o ISAC "I4C+" sob a égide da MCE permite que cidades troquem informação sensível sobre incidentes, reduzindo o risco e impacto de ataques informáticos nas infraestruturas críticas urbanas.

- **Blueprint para Gestão de Crises Cibernéticas da UE**

Iniciativa do Conselho/Comissão (recomendação de 2025) que estabelece o quadro de resposta a crises cibernéticas de larga escala na UE. Esclarece quando uma crise atinge nível europeu, define papéis de atores chave (ENISA, EU-CyCLONe, etc.) e procedimentos para detetar, responder, recuperar e aprender com incidentes massivos. Visa assegurar coordenação técnica e política em situações que ultrapassem a capacidade nacional.

2.5. Outras estruturas da Comissão Europeia

- **DG HOME (Direção-Geral Assuntos Internos)**

É responsável pelas políticas de segurança interna da UE. Desenvolve legislação e estratégias (ex. ProtectEU) contra cibercrime, terrorismo e ameaças híbridas. Coordena agências como Europol/Eu-LISA e fundos (Fundo de Segurança Interna) que financiam projetos de cibersegurança e proteção de infraestruturas críticas.

- **DG CNECT (Direção-Geral Redes de Comunicação, Conteúdo e Tecnologia)**

Departamento encarregado da agenda digital da UE. Formula políticas de infraestrutura de rede, 5G e tecnologias emergentes, e lidera o mercado digital único. Atua na cibersegurança estratégica, defendendo a UE contra ameaças cibernéticas e híbridas e coordenando iniciativas de segurança de redes digitais.

- **JRC (Centro Comum de Investigação)**

O serviço científico da Comissão Europeia. Realiza pesquisas de apoio às políticas da UE, incluindo cibersegurança. Por exemplo, o JRC mapeou normas técnicas de ciberresiliência para implementar o Regulamento de Resiliência Cibernética (CRA), e produz análises de vulnerabilidades em infraestruturas críticas para informar decisões da Comissão.

3. Organizações internacionais extraeuropeias relevantes

3.1. Organizações onde Portugal está representado

- **OCDE Organização para a Cooperação e Desenvolvimento Económico**

Organização internacional de cooperação económica que reúne 38 países, da qual Portugal faz parte. Aborda a cibersegurança na perspetiva da "segurança digital", desenvolvendo recomendações e quadros de referência para políticas públicas. O seu "Policy Framework on Digital Security" (Quadro de Políticas para a Segurança Digital) orienta os governos na gestão do risco cibernético, na definição de estratégias nacionais e na proteção de atividades críticas e de infraestruturas essenciais. Publica igualmente estudos e orientações para promover o alinhamento económico e social das políticas de segurança digital, contribuindo para o reforço da resiliência das economias face às ameaças cibernéticas.

- **OMC Organização Mundial do Comércio**

Organização multilateral que regula o comércio internacional, da qual Portugal é membro fundador. Embora o seu foco seja o comércio, a OMC aborda aspetos da economia digital e do comércio eletrónico, influenciando normas relativas aos fluxos transfronteiriços de dados e à infraestrutura digital. Em análises recentes, salienta que um enquadramento regulatório eficaz deve incluir salvaguardas como a privacidade e a cibersegurança, para reforçar a confiança no comércio digital. Deste modo, a OMC contribui indiretamente para a resiliência das infraestruturas de TIC, ao incentivar políticas que assegurem transações digitais seguras entre os seus membros.

- **NATO (OTAN) Organização do Tratado do Atlântico Norte**

Aliança militar intergovernamental composta por 32 países, da qual Portugal é membro fundador, centrada na defesa coletiva. A ciberdefesa integra as suas missões essenciais de dissuasão e defesa. A OTAN funciona também como plataforma política de consulta entre os Aliados, promovendo a partilha de informação, a cooperação e a ação coletiva contra ciberataques, incluindo medidas de proteção de infraestruturas críticas. Nas cimeiras mais recentes, os Aliados reafirmaram o compromisso de reforçar as defesas nacionais, em particular das redes e dos serviços essenciais, através da partilha mútua de recursos e da realização de exercícios conjuntos.

- **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)**

No âmbito da sua atuação em ciberdefesa, a OTAN conta com estruturas especializadas que apoiam os Aliados no desenvolvimento de capacidades, investigação e formação. Entre estas destaca-se o um centro multinacional e interdisciplinar dedicado à investigação, formação e realização de exercícios em ciberdefesa.

- **NATO Resilience Committee**

No âmbito da sua responsabilidade em matéria de cibersegurança e resiliência, a NATO coordena também a preparação civil e a continuidade de serviços essenciais através do *Resilience Committee*. Este é apoiado por seis *Planning Groups* especializados (comunicações, proteção civil, energia, alimentação/água, saúde e transportes), que fornecem aconselhamento técnico e estratégico aos Aliados para garantir a continuidade de serviços essenciais em crises. O site apresenta o enquadramento institucional e os domínios de atuação de cada grupo.

- **UIT União Internacional de Telecomunicações**

Agência especializada das Nações Unidas que coordena normas e políticas globais nas áreas das telecomunicações e das TIC, da qual Portugal é membro. Funciona como fórum multilateral para a harmonização de normas internacionais de cibersegurança, apoiando os países na definição de estratégias nacionais e na criação de equipas de resposta a incidentes (CSIRTs). A UIT promove a cooperação entre governos, indústria e academia para garantir um ecossistema de TIC interligado, fiável e seguro, através de iniciativas como a "Global Cybersecurity Agenda". Salienta que a proteção de infraestruturas críticas de TIC e a promoção de um acesso equitativo à Internet são essenciais para o desenvolvimento socioeconómico.

- **UNDRR Escritório das Nações Unidas para Redução do Risco de Desastres**

Agência das Nações Unidas responsável pela coordenação global da redução do risco de catástrofes. Atua na promoção de políticas de infraestruturas resilientes junto dos Estados-membros (incluindo Portugal), em articulação com o Sendai Framework e com os Objetivos de Desenvolvimento Sustentável. Presta apoio técnico para que os governos identifiquem vulnerabilidades em infraestruturas críticas (energia, água, transportes, entre outras) e integrem medidas de resiliência em todas as fases do ciclo de vida dos projetos. Promove padrões e orientações globais (por exemplo, os *Principles for Resilient Infrastructure*) e parcerias como a *Coalition for Disaster Resilient Infrastructure (CDRI)*. O UNDRR sublinha que o investimento em infraestruturas resilientes é determinante para reduzir perdas e assegurar a continuidade dos serviços públicos essenciais, mesmo após situações de crise.

3.2. Organizações onde Portugal não está representado

- **APEC Cooperação Económica Ásia-Pacífico**

Fórum económico intergovernamental que reúne 21 economias da região do Pacífico (Ásia e Américas). No âmbito da sua agenda para a economia digital, estabelece princípios de segurança digital de natureza não vinculativa. O "APEC Framework for Securing the Digital Economy" sublinha a importância da resiliência das Infraestruturas Críticas de Informação (CII) para assegurar o crescimento sustentável da economia digital e a prestação de serviços essenciais, incluindo serviços públicos digitais (*e-government*). Recomenda a gestão do risco cibernético e a colaboração entre os setores público e privado para proteger redes e serviços críticos. Deste modo, influencia práticas e orientações técnicas na região Ásia-Pacífico.

- **ASEAN Associação de Nações do Sudeste Asiático**

Bloco regional composto por 10 países do Sudeste Asiático. Entre os seus objetivos estratégicos inclui-se o reforço da segurança digital dos seus membros. A ASEAN promove a coordenação política e operacional em matéria de cibersegurança, desenvolvendo mecanismos como quadros de referência para a proteção de infraestruturas críticas a nível regional e redes colaborativas de CERT. Reconhece que um ciberespaço seguro é fundamental para assegurar a continuidade de serviços públicos essenciais e apoiar o desenvolvimento económico no período pós-pandemia. A estratégia comunitária enfatiza a partilha de informação sobre ameaças, a realização de exercícios conjuntos e a capacitação das equipas nacionais.

- **CDRI Coalition for Disaster Resilient Infrastructure**

Coalizão internacional lançada pela Índia, em 2019, para reforçar a resiliência dos sistemas de infraestruturas face a riscos climáticos e catástrofes naturais. Integra 53 países-membros, bem como várias organizações e agências internacionais. A CDRI disponibiliza conhecimento técnico, apoio financeiro e partilha de boas práticas para projetos de infraestruturas críticas (energia, transportes, telecomunicações, saúde, entre outros). O seu objetivo é que, até 2050, biliões em investimentos em infraestruturas sejam planeados e geridos de modo a resistirem a desastres. Atua através de relatórios, investigação e projetos-piloto, visando aumentar a capacidade dos países para enfrentar eventos extremos sem interrupções significativas dos serviços essenciais.

- **CISA Cybersecurity and Infrastructure Security Agency**

Agência federal dos Estados Unidos responsável pela proteção das infra-estruturas críticas e pelo reforço da cibersegurança nacional. As suas funções incluem a prevenção, deteção e resposta a incidentes cibernéticos, o apoio a entidades públicas e privadas na gestão de riscos, a coordenação da partilha de informação sobre ameaças e vulnerabilidades, bem como a promoção de exercícios, orientações e boas práticas para aumentar a resiliência dos sistemas de informação e das infra-estruturas essenciais. A CISA desempenha ainda um papel central na cooperação interinstitucional e internacional, contribuindo para uma resposta coordenada a ameaças cibernéticas de grande escala.

- **Cyber Expert Group,G7 Grupo dos Sete**

Coalizão informal que reúne as sete maiores economias avançadas (Canadá, França, Alemanha, Itália, Japão, Reino Unido e Estados Unidos da América). Embora atue em múltiplos domínios económicos e políticos, o G7 atribui especial relevância à cibersegurança através de fóruns especializados. Entre estes destaca-se o **Cyber Expert Group**, que congrega as autoridades financeiras dos países do G7 com o objetivo de coordenar políticas de cibersegurança no setor financeiro. Este grupo promove a partilha de informação sobre ameaças (como o ransomware), a realização de exercícios de resposta conjunta e a elaboração de orientações e boas práticas.

- NISC **National Center of Incident Readiness and Strategy for Cybersecurity**

Integrado no National Cybersecurity Office do Japão, é a entidade central responsável pela coordenação da estratégia nacional de cibersegurança e pela prontidão para resposta a incidentes. Atua ao nível da governação, promovendo a articulação entre ministérios, setores críticos e parceiros do setor privado, apoiando a definição de políticas, orientações e mecanismos de coordenação nacional. Constitui um modelo relevante de organização para resposta a incidentes e colaboração multissetorial, complementando as estruturas operacionais de tipo CSIRT.

- **OEA Organização dos Estados Americanos**

Principal fórum político das Américas, reunindo 35 países do continente. Atua no domínio da segurança multidimensional, incluindo a cooperação em cibersegurança. Através do Comité Interamericano contra o Terrorismo (CICTE), a OEA presta assistência técnica e apoia o reforço de capacidades de cibersegurança dos Estados-membros. A Secção de Cibersegurança do CICTE lidera projetos regionais, apoiando os países no desenvolvimento de estratégias nacionais e de CSIRTs (Equipas de Resposta a Incidentes de Segurança Informática), com vista a um ciberespaço aberto, seguro e resiliente no hemisfério. Estas iniciativas contribuem para a proteção de infraestruturas críticas (energia, comunicações e finanças) e de serviços essenciais nos países das Américas.

4. Enquadramento jurídico e normativo aplicável

4.1. Legislação da União Europeia

4.1.1. Legislação Europeia de Base

Comissão Europeia. (2024). *Regulamento de Execução (UE) 2024/2690 da Comissão, de 17 de outubro de 2024, que estabelece regras de execução da Diretiva (UE) 2022/2555 relativamente aos requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança e especifica os casos em que um incidente é considerado significativo para determinados prestadores de serviços digitais*. *Jornal Oficial da União Europeia*, L 2024/2690.

Resumo: O Regulamento de Execução (UE) 2024/2690 concretiza a Diretiva NIS2 ao definir requisitos técnicos e metodológicos para a gestão de riscos de cibersegurança e ao especificar, para diversos prestadores de serviços digitais e infraestruturas críticas, os critérios que determinam quando um incidente de cibersegurança é considerado significativo, promovendo uma aplicação harmonizada das obrigações de reporte e gestão de incidentes na União Europeia.

Parlamento Europeu & Conselho da União Europeia. (2022). *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148*. *Jornal Oficial da União Europeia*, L 333, 80,152.

Resumo: (em vigor desde Dez 2022) **Designada por Diretiva NIS2 (SRI2)** estabelece obrigações reforçadas de segurança para entidades essenciais e importantes em setores críticos (energia, transportes, saúde, TI, financeiro, água, 112/administração pública, etc.), impondo gestão de risco, continuidade e reporte de incidentes. Em especial, exige que tais entidades mantenham políticas de segurança e análise de risco, planos de tratamento de incidentes e de continuidade (incluindo backups e recuperação de desastres).

Parlamento Europeu & Conselho da União Europeia. (2022). *Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho.* *Jornal Oficial da União Europeia*, L 333, 164,198.

Resumo: Designada por **Diretiva CER** complementa a Diretiva (UE) 2022/2555 definindo 14 setores de "entidades críticas" (energia, transportes, bancário, água, alimentos, saúde, financeiro, TIC, etc.) e exigindo que prestadoras de serviços essenciais possam prevenir, responder e recuperar de incidentes que afetem a sociedade. É complementar à NIS2.

Parlamento Europeu & Conselho da União Europeia. (2022) *Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 e (UE) 2016/1011*. *Jornal Oficial da União Europeia*, L 333, 1-79. Versão consolidada atual: 27/12/2022

Resumo: Também conhecida como **Digital Operational Resilience Act (DORA),** o Regulamento (UE) 2022/2554 complementa a Diretiva (UE) 2022/2555 (NIS2) ao estabelecer um regime setorial específico aplicável ao setor financeiro, concretizando e aprofundando os objetivos gerais de cibersegurança e resiliência operacional previstos na NIS2. Nos domínios abrangidos pelo seu âmbito material, a DORA atua como lex specialis, prevenindo a sobreposição de obrigações e assegurando uma aplicação coerente do quadro regulatório europeu em matéria de resiliência digital.

Comissão Europeia. (2023). *Regulamento Delegado (UE) 2023/2450 da Comissão, de 25 de julho de 2023, que complementa a Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho estabelecendo uma lista de serviços essenciais*. *Jornal Oficial da União Europeia*, L 2023/2450.

Resumo: O Regulamento Delegado (UE) 2023/2450 da Comissão Europeia complementa a Diretiva (UE) 2022/2557 (CER) ao estabelecer uma lista de serviços essenciais cuja prestação é crítica para o funcionamento da sociedade e da economia, clarificando assim o âmbito de aplicação da diretiva e apoiando a identificação das entidades críticas sujeitas às obrigações de resiliência.

4.1.2. Regulamentos

Comissão Europeia. (2025). *Decisão de Execução (UE) 2025/704 da Comissão, de 10 de abril de 2025, que estabelece as normas de execução da Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho relativa a um Mecanismo de Proteção Civil da União Europeia e que revoga as Decisões de Execução 2014/762/UE e (UE) 2019/1310 da Comissão [notificada com o número C(2025) 2130].* *Jornal Oficial da União Europeia*, L 2025/704.

Parlamento Europeu, & Conselho da União Europeia. (2025, 11 de fevereiro). *Regulamento (UE) 2025/327 do Parlamento Europeu e do Conselho, de 11 de fevereiro de 2025, relativo ao Espaço Europeu de Dados de Saúde e que altera a Diretiva 2011/24/UE e o Regulamento (UE) 2024/2847 (Texto relevante para efeitos do EEE)*. *Jornal Oficial da União Europeia*, L, 5 de março de 2025.

Parlamento Europeu & Conselho da União Europeia. (2024). *Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho, de 19 de dezembro de 2024, que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ciberameaças e incidentes de cibersegurança*. *Jornal Oficial da União Europeia*. L 2025/38, 15.1.2025

Parlamento Europeu & Conselho da União Europeia. (2024). *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (Texto relevante para efeitos do EEE).* *Jornal Oficial da União Europeia*, L 2024/1689.

Parlamento Europeu & Conselho da União Europeia. (2024). *Regulamento (UE) 2024/1679 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, relativo às orientações da União para o desenvolvimento da rede transeuropeia de transportes, que altera o Regulamento (UE) 2021/1153 e o Regulamento (UE) n.º 913/2010 e revoga o Regulamento (UE) n.º 1315/2013 (Texto relevante para efeitos do EEE)*. *Jornal Oficial da União Europeia*, L 2024/1679.

Comissão Europeia. (2024). *Regulamento Delegado (UE) 2024/1366 da Comissão, de 11 de março de 2024, que completa o Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho estabelecendo um código de rede relativo a regras setoriais para os aspetos ligados à cibersegurança dos fluxos transfronteiriços de eletricidade*. *Jornal Oficial da União Europeia*, L 2024/1366.

Parlamento Europeu & Conselho da União Europeia. (2023*). Regulamento (UE) 2023/1781 do Parlamento Europeu e do Conselho, de 13 de setembro de 2023, que estabelece um regime de medidas para reforçar o ecossistema europeu dos semicondutores e que altera o Regulamento (UE) 2021/694 (Regulamento dos Circuitos Integrados) (Texto relevante para efeitos do EEE)*. *Jornal Oficial da União Europeia*, L 229, 1-53.

Parlamento Europeu & Conselho da União Europeia. (2022). *Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, que estabelece o programa Década Digital para 2030*. *Jornal Oficial da União Europeia L 323 de 19.12.2022, pp. 4-26*.

Parlamento Europeu & Conselho da União Europeia. (2022). Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.° 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência). *Jornal Oficial da União Europeia*, L 2024/2847. Versão consolidada atual: 20/11/2024

Parlamento Europeu & Conselho da União Europeia. (2021). *Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que cria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança*. *Jornal Oficial da União Europeia*. L 202 de 8.6.2021, pp. 1-31

Parlamento Europeu & Conselho da União Europeia. (2021). *Regulamento (UE) 2021/836 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que altera a Decisão n.º 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União Europeia (Texto relevante para efeitos do EEE).* *Jornal Oficial da União Europeia*, L 185**,** 1-22.

Parlamento Europeu & Conselho da União Europeia. (2021). *Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, que estabelece o Programa Europa Digital.* *Jornal Oficial da União Europeia.* L 166 de 11.5.2021, pp. 1-34

Parlamento Europeu & Conselho da União Europeia. (2019). *Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA e à certificação da cibersegurança das TIC*. *Jornal Oficial da União Europeia*. L 151 de 7.6.2019, pp. 15-69

4.2. Legislação nacional portuguesa

Lei n.º 59/2025, de 22 de outubro
Assembleia da República
Autoriza o Governo a transpor a Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União.

Decreto-Lei n.º 125/2025, de 4 de dezembro
Presidência do Conselho de Ministros
Transpõe a Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União.

Decreto-Lei n.º 22/2025, de 19 de março
Presidência do Conselho de Ministros
Transpõe a Diretiva (UE) 2022/2557 (Diretiva CER), relativa à identificação, designação e reforço da resiliência das entidades críticas.

Decreto-Lei n.º 116/2023, de 12 de dezembro
Presidência do Conselho de Ministros
Transfere para o Centro Nacional de Cibersegurança as competências de fiscalização e de instrução de contraordenações no âmbito do ECOMPENSA

Decreto-Lei n.º 34/2023, de 23 de maio
Presidência do Conselho de Ministros
Cria a «Cyber Academia and Innovation Hub»

Decreto-Lei n.º 20/2022, de 28 de janeiro
Presidência do Conselho de Ministros
Aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias

Decreto-Lei n.º 65/2021, de 30 de julho
Presidência do Conselho de Ministros
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

Decreto-Lei n.º 43/2020, de 21 de julho
Presidência do Conselho de Ministros
Estabelece o Sistema Nacional de Planeamento Civil de Emergência

Regulamento n.º 183/2022, de 21 de fevereiro
Presidência do Conselho de Ministros - Gabinete Nacional de Segurança - Centro Nacional de Cibersegurança
Regulamento que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança

Portaria n.º 163/2023, de 5 de abril
Presidência do Conselho de Ministros - Gabinete do Secretário de Estado da Digitalização e da Modernização Administrativa
Autoriza o Gabinete Nacional de Segurança a assumir todos os encargos plurianuais relativos à aquisição de serviços de produção de conteúdos e serviços de formação no âmbito da Cibersegurança C-Academy

Diretiva n.º 10/2025, de 24 de outubro
Entidade Reguladora dos Serviços Energéticos
Aprova as regras excecionais aplicáveis à liquidação do mercado de eletricidade relativa aos dias 28 e 29 de abril de 2025.

Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro
Presidência do Conselho de Ministros
Aprova a Estratégia Nacional de Ciberdefesa

Despacho n.º 8914-A/2024, de 7 de agosto
Presidência do Conselho de Ministros - Gabinete do Ministro da Presidência
Constitui um grupo de trabalho para elaborar texto legislativo que proceda à transposição da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, à execução do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, e à certificação da cibersegurança das tecnologias da informação e comunicação.

4.3. Instrumentos não vinculativos da União Europeia

Comissão Europeia. (2025). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre o ProtectEU: uma Estratégia Europeia de Segurança Interna* (COM/2025/148 final).

> **Resumo:** A Comunicação ProtectEU apresenta uma nova Estratégia Europeia de Segurança Interna para reforçar a capacidade da UE de antecipar, prevenir e responder a ameaças. Assenta num reforço do quadro jurídico, numa cooperação mais profunda entre Estados-Membros e numa maior partilha de informação e coordenação com as agências da UE. Dá destaque à resiliência face a ameaças híbridas, incluindo ciberataques e perturbações de infraestruturas críticas, e ao combate à criminalidade organizada e ao terrorismo. Propõe uma abordagem "whole-of-society", integrando considerações de segurança nas políticas e iniciativas europeias relevantes.

Conselho da União Europeia. (2024). *Recomendação do Conselho, de 25 de junho de 2024, sobre um plano de ação para a coordenação da resposta a nível da União a perturbações em infraestruturas críticas com importante relevância transfronteiriça* (C/2024/4371). *Jornal Oficial da União Europeia*, *C, C/2024/4371, 5.7.2024*

Comissão Europeia. (2024). *Recomendação (UE) 2024/779 da Comissão, de 26 de fevereiro de 2024, sobre infraestruturas de cabos submarinos seguras e resilientes*. *Jornal Oficial da União Europeia*. L, 2024/779.

Conselho da União Europeia. (2022, 8 de dezembro). *Recomendação do Conselho de 8 de dezembro de 2022 relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas (Texto relevante para efeitos do EEE) (2023/C 20/01)*. *Jornal Oficial da União Europeia*, C 20, 20 de janeiro de 2023, 1-11.

Conselho da União Europeia. (2022). *Recomendação do Conselho, de 8 de dezembro de 2022, relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas* (2023/C 20/01). *Jornal Oficial da União Europeia*, C 20, 1-11

Conselho da União Europeia. (2022). *Proposta de recomendação do Conselho relativa a uma abordagem coordenada da União para reforçar a resiliência das infraestruturas críticas* (ST 13713/2022 INIT). *Conselho da União Europeia*.

Comissão Europeia. (2022). *Proposta de recomendação do Conselho relativa a uma abordagem coordenada da União para reforçar a resiliência das infraestruturas críticas* (COM/2022/551 final). *Comissão Europeia*.

Conselho da União Europeia. (2023). *Anexo da proposta de Recomendação do Conselho sobre um plano de ação para a coordenação da resposta a nível da União a perturbações em infraestruturas críticas com importante relevância transfronteiriça* (ST 12485/2023 ADD 1). *Conselho da União Europeia*.

Comissão Europeia & Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança. (2021). *Comunicação conjunta ao Parlamento Europeu e ao Conselho: Relatório sobre a aplicação da Estratégia de Cibersegurança da UE para a Década Digital* (JOIN(2021) 28 final). *Comissão Europeia*.

Comissão Europeia & Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança. (2020). *Comunicação conjunta ao Parlamento Europeu e ao Conselho: Estratégia de cibersegurança da UE para a década digital* (JOIN(2020) 18 final). *Comissão Europeia*.

4.4. Acordos e compromissos internacionais de Portugal (UE e NATO)

Declaração Conjunta de Nova Iorque sobre Segurança e Resiliência dos Cabos Submarinos num Mundo Globalmente Digitalizado = Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World. (2024, 26 de setembro). Shaping Europe's Digital Future : Policy and Legislation. https://digital-strategy.ec.europa.eu/pt/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world

Resumo: Declaração conjunta endossada por EUA, Austrália, Canadá, União Europeia, Estados Federados da Micronésia, Finlândia, França, Japão, Ilhas Marshall, Países Baixos, Nova Zelândia, Portugal, República da Coreia, Singapura, Tonga, Tuvalu e Reino Unido. Reconhece a dependência global de cabos submarinos e os riscos para a segurança nacional/económica, defendendo políticas para infraestruturas robustas, redundantes, resilientes e seguras. Estabelece princípios: conceção "security-by-design"; cooperação para selecionar fornecedores verificáveis e diversificar rotas; coordenação governo, indústria para implantação/manutenção; planeamento espacial para reduzir riscos e estrangulamentos; transparência de propriedade; avaliações regulares de risco (técnicas e geopolíticas); mitigação de riscos de dados; e conformidade com o Direito Internacional (UNCLOS) e leis domésticas. [também publicado em https://www.gov.uk/government/publications/new-york-joint-statement-on-the-security-and-resilience-of-undersea-cables ; https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/]

Ministry of Foreign Affairs. (2025, January 16). *Will ensure a safer seabed*. Government.no. https://www.regjeringen.no/en/whats-new/will-ensure-a-safer-seabed/id3083648/

Resumo: Declaração do Ministro dos Negócios Estrangeiros da Noruega, Espen Barth Eide, na qual anuncia medidas acordadas entre a Noruega, os EUA e aliados nórdico-bálticos para reforçar a segurança de infraestruturas submarinas, com foco em cabos e gasodutos. O texto regista explicitamente que em novembro de 2024 a Noruega endossou a *Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World (Declaração Conjunta de Nova Iorque sobre Segurança e Resiliência dos Cabos Submarinos num Mundo Globalmente Digitalizado)* e lista quatro linhas de ação (partilha de informação em tempo real, parcerias público-privadas para capacidade de reparação, criação de repositório de incidentes/reparações e agilização logística para reparos).

5. Literatura técnica

Agência da União Europeia para a Cibersegurança (ENISA). (2023). *Good practices for supply chain cybersecurity.* ENISA. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

Resumo: Compila boas práticas para reduzir risco de fornecedores e dependências. Apoia inventário, avaliação, monitorização contínua e cláusulas contratuais. Guia operacional para evidenciar conformidade com a Diretiva NIS2.

Agência da União Europeia para a Cibersegurança (ENISA). (2025). *ENISA NIS360 2024: ENISA cybersecurity maturity & criticality assessment of NIS2 sectors (Publication No. TP-1-25-002-EN-N).* ENISA. https://www.enisa.europa.eu/publications/enisa-nis360-2024

Resumo: O NIS360 é um novo produto da ENISA que avalia o grau de maturidade e a criticidade dos setores de elevada criticidade ao abrigo da Diretiva NIS2, fornecendo tanto uma visão comparativa como uma análise mais aprofundada de cada setor. Para apoiar os Estados-Membros e as autoridades nacionais na identificação de lacunas e na definição de prioridades na afetação de recursos.

Agência da União Europeia para a Cibersegurança (ENISA). (2025). *Handbook for cyber stress tests (Publication No. TP-1-25-009-EN-N).* ENISA. https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests

Resumo: A ENISA elaborou este manual como orientação para autoridades nacionais ou setoriais responsáveis pela cibersegurança e resiliência de setores críticos, a nível nacional, regional ou da UE, no âmbito da Diretiva NIS2. Também pode ser útil para outras autoridades de supervisão ao abrigo de regulamentação setorial, como o Regulamento DORA e a Diretiva CER.

Agência da União Europeia para a Cibersegurança (ENISA). (2025, June). *Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures* (Version 1.0). Publications Office of the European Union. https://doi.org/10.2824/2702548

Resumo: Guia técnico da ENISA que apoia o Regulamento de Execução (UE) 2024/2690. Detalha os requisitos técnicos e metodológicos das medidas de gestão de risco previstas no art. 21.º(2) da NIS2. Aplica-se sobretudo a subsetores de infraestruturas digitais e de gestão de serviços TIC com operações transfronteiriças, harmonizando exigências a nível da UE. Fornece orientação prática de implementação, exemplos de evidências para demonstrar conformidade e mapeamentos para boas práticas e normas (e.g., ISO/IEC). Na prática, ajuda as organizações a operacionalizar controlos de cibersegurança e a comprovar o seu cumprimento perante as autoridades competentes.

Australian Signals Directorate. (2025). *CI Fortify: Guidance for Australian critical infrastructure service continuity and resilience*. https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/ci-fortify

Resumo: A página CI Fortify no portal *cyber.gov.au* apresenta uma orientação do Australian Signals Directorate (ASD) e do Australian Cyber Security Centre (ACSC) para operadores de infra-estruturas críticas na Austrália, com o objetivo de melhorar a cibersegurança e a resiliência dos sistemas essenciais. A orientação fornece recomendações de alto nível para reforçar a continuidade dos serviços e a capacidade de resposta em situações de crise ou interrupção de serviço, focando-se especialmente em sistemas de tecnologia operacional (OT) que suportam serviços essenciais. Entre as recomendações estão a identificação de sistemas vitais, a planificação de medidas de isolamento que permitam manter serviços críticos mesmo quando as redes estiverem comprometidas e a capacidade de reconstruir rapidamente sistemas isolados, reduzindo o impacto de ataques sofisticados.

Common Criteria. (s.d.). *Official Common Criteria portal.* [Consultado em 8 DEZ 2025].https://www.commoncriteria.org/

Resumo: O portal oficial do *Common Criteria* reúne informação sobre o esquema internacional de avaliação e certificação de segurança de produtos e sistemas de tecnologias de informação. Disponibiliza acesso a listas de produtos certificados, perfis de proteção, documentos de enquadramento e orientações associadas ao processo de avaliação, permitindo apoiar decisões de aquisição, requisitos de conformidade e verificação de garantias de segurança em contextos regulados e de elevada criticidade

Federal Energy Regulatory Commission. (2025). *Critical Infrastructure Protection Reliability Standard CIP-015-1 (Cyber Security: Internal Network Security Monitoring)*. Federal Register.https://www.federalregister.gov/documents/2025/07/02/2025-12309/critical-infrastructure-protection-reliability-standard-cip-015-1-cyber-security-internal-network

Resumo: Formaliza requisitos de monitorização interna de rede em ambientes críticos do setor da energia, incluindo a deteção de eventos dentro do perímetro de confiança. Reforça a capacidade de auditoria, a produção de evidência e a investigação forense, reduzindo pontos cegos em sistemas de tecnologia operacional (OT). Ajuda a distinguir falhas técnicas de ataques e acelera a resposta a incidentes. Constitui um exemplo sólido de requisito exigível e auditável.

International Organization for Standardization. (2014). *ISO 28001:2007 Security management systems for the supply chain: Best practices for implementing supply chain security, assessments and plans: Requirements and guidance.* ISO. https://www.iso.org/standard/45654.html

Resumo: Guia focado em avaliações e planos de segurança da cadeia de fornecimento. Ajuda a estruturar práticas de avaliação e mitigação associadas a terceiros. É útil como complemento às orientações da ENISA para efeitos de evidência e de processo. Embora mais antigo, mantém relevância como referência de boas práticas.

International Organization for Standardization. (2018). *ISO 31000:2018 Risk management: Guidelines.* ISO. https://www.iso.org/standard/65694.html

Resumo: Enquadramento transversal de gestão de risco. Define princípios, estrutura e processo para avaliação e tratamento de risco. Ajuda a padronizar linguagem, critérios e rastreabilidade em auditorias. Referencial para integrar NIS2/CER em gestão de risco.

International Organization for Standardization. (2019). *ISO 22301:2019, Business continuity management systems, Requirements*. https://www.iso.org/standard/75106.html

Resumo: Norma de referência para implementar e manter um Sistema de Gestão da Continuidade do Negócio. Apoia a definição de processos de preparação, resposta e recuperação, incluindo testes e melhoria contínua. Suporta planos de continuidade e de recuperação auditáveis e alinhados com requisitos regulamentares. É amplamente utilizada em setores essenciais e em cadeias críticas.

International Organization for Standardization. (2023). *ISO 28000:2022 Security and resilience: Security management systems: Requirements.* ISO. https://www.iso.org/standard/79612.html

Resumo: Norma para sistemas de gestão orientada para a segurança e a resiliência (inclui o contexto logístico). Apoia a governação, a definição de responsabilidades, a fixação de objetivos e a melhoria contínua. É relevante para organizações com dependências na cadeia de fornecimento e em serviços críticos. Complementa as medidas técnicas com práticas de gestão e organização.

International Organization for Standardization. (2025). *ISO/IEC 27031:2025: Cybersecurity: ICT readiness for business continuity*. https://www.iso.org/standard/27031

Resumo: Orienta a prontidão das tecnologias de informação e comunicação para suportar a continuidade, articulando a componente tecnológica com o planeamento de continuidade do negócio. É útil para desenhar planos de recuperação, clarificando objetivos, dependências, procedimentos de retoma e medidas de prevenção de interrupções. Ajuda a definir requisitos de prontidão ao nível de pessoas, processos e tecnologia, e constitui uma boa base para evidenciar a preparação e a realização de testes de recuperação.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements.* ISO/IEC. https://www.iso.org/standard/27001

Resumo: Norma que define requisitos para um Sistema de Gestão de Segurança da Informação (SGSI/ISMS), cobrindo governação, gestão de risco, mecanismos de proteção e melhoria contínua. Facilita a produção de evidência documental auditável (políticas, processos e métricas).

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: Information security controls.* ISO/IEC. https://www.iso.org/standard/75652.html

Resumo: Catálogo de medidas para seleção e implementação num ISMS. Adequado para mapear requisitos legais (NIS2) para medidas concretas, apoiando a definição de uma linha de base e a produção de evidências de implementação. Útil para desenho de políticas e medidas técnicas e organizacionais.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection: Guidance on managing information security risks.* ISO/IEC. https://www.iso.org/standard/80585.html

Resumo: Orientação prática para identificar, analisar e tratar riscos de segurança da informação. Apoia a consistência metodológica e a manutenção de registos rastreáveis de risco residual. É particularmente útil para auditorias e para a formalização do processo de gestão de riscos no âmbito da NIS2, ajudando a relacionar activos, ameaças, vulnerabilidades e medidas.

International Society of Automation. (2010-2023). *ISA/IEC 62443 Series of Standards*. ISA. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Resumo: Referência-chave para a cibersegurança em ambientes industriais, incluindo tecnologia operacional e sistemas de automação e controlo industrial. Apoia a definição de requisitos, processos e níveis de segurança para sistemas de controlo. É particularmente relevante para os setores da energia, água, transportes e indústria com sistemas de supervisão e controlo. Muito útil em auditorias e na definição de requisitos para integradores e fornecedores de tecnologia operacional.

National Institute of Standards and Technology. (2021). Ross, R., et al. *Developing cyber-resilient systems: A systems security engineering approach (NIST Special Publication 800-160, Vol. 2, Rev. 1).* NIST. https://doi.org/10.6028/NIST.SP.800-160v2r1

Resumo: Propõe princípios e práticas de engenharia para a resiliência ao longo do ciclo de vida. Concretiza a resiliência em objetivos (antecipar, resistir, recuperar e adaptar) e em evidências. Apoia o desenho de arquitecturas e de medidas verificáveis e auditáveis, sendo particularmente útil para alinhar a conformidade com uma abordagem estruturada de engenharia da segurança.

National Institute of Standards and Technology. (2022). *Secure Software Development Framework (SSDF) Version 1.1 (NIST SP 800-218)*. NIST https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf

Resumo: Quadro de referência com práticas recomendadas para o desenvolvimento seguro ao longo do ciclo de vida do software. Apoia a definição de exigências a fornecedores, incluindo processos de desenvolvimento, medidas aplicadas, evidências e conformidade. É útil para critérios de aquisição e para a avaliação do nível de maturidade dos fornecedores, complementando o inventário de componentes de software ao reforçar práticas que reduzem o risco associado aos componentes.

National Institute of Standards and Technology. (2022). *Software Bill of Materials (SBOM) and Executive Order 14028 resources*. NIST. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

Resumo: Explica o conceito e a utilidade do inventário formal de componentes de software (*SBOM*) no contexto das cadeias de fornecimento. Apoia a transparência, o rastreio de vulnerabilidades e a gestão do risco associado a terceiros. É particularmente relevante na sequência de incidentes na cadeia de fornecimento e contribui para a operacionalização de requisitos de aquisição segura de software. É útil para contratos e auditorias a fornecedores de software e integradores, servindo de base a políticas de inventário e a processos de resposta a vulnerabilidades.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*. NIST. https://doi.org/10.6028/NIST.CSWP.29

Resumo: Quadro de referência para a gestão do risco cibernético, com a função de governação reforçada. É útil para mapear medidas, níveis de maturidade e programas de cibersegurança, ajudando a alinhar a linguagem entre o negócio, as tecnologias de informação, a gestão do risco e a conformidade. Serve como base para a definição de perfis e de planos de melhoria.

6. Relatórios, Formação e Capacitação

6.1. Incidentes Significativos e Relatórios de Investigação

Agência da União Europeia para a Cibersegurança. (2021, 26 de julho). *Telecom security incidents 2020: Annual report*. ENISA. https://www.enisa.europa.eu/publications/telecom-security-incidents-2020

Resumo. Este relatório anual da ENISA agrega informação sobre incidentes de segurança em telecomunicações ocorridos em 2020**,** com base em notificações submetidas por 26 Estados-Membros da União Europeia e 2 países da EFTA**.** O documento analisa 170 incidentes, que resultaram num total estimado de 841 milhões de horas de serviço perdidas**.** O relatório identifica tendências, causas mais frequentes, impactos nos serviços e lições aprendidas, contribuindo para a melhoria da resiliência e da gestão de riscos no sector das telecomunicações.

Agência da União Europeia para a Cibersegurança. (2022, 27 de julho). *Telecom security incidents 2021: Annual report*. ENISA. https://www.enisa.europa.eu/publications/telecom-security-incidents-2021

Resumo: O relatório referente a 2021 apresenta a análise de 168 incidentes de segurança em telecomunicações, reportados por 26 Estados-Membros da UE e 2 países da EFTA**.** Apesar de um número de incidentes semelhante ao ano anterior, o impacto foi significativamente superior, com cerca de 5 106 milhões de horas de serviço perdidas. O documento evidencia um agravamento da severidade dos incidentes, destacando falhas de rede, ataques maliciosos e dependências crescentes de infraestruturas críticas, reforçando a necessidade de medidas de prevenção mais robustas.

Agência da União Europeia para a Cibersegurança. (2024, 14 de março). *Telecom security incidents 2022: Annual report*. ENISA. https://www.enisa.europa.eu/publications/telecom-security-incidents-2022

Resumo: Este relatório analisa os incidentes de segurança em telecomunicações registados em 2022**,** com base em 155 incidentes notificados por 26 Estados-Membros da UE e 2 países da EFTA**.** Apesar da redução do número total de incidentes, o impacto global aumentou substancialmente, atingindo cerca de 11 209 milhões de horas de serviço perdidas**.** O relatório sublinha a crescente complexidade das redes, a dependência de serviços digitais e a importância de estratégias de resiliência operacional para proteger infraestruturas críticas de comunicações.

Agência da União Europeia para a Cibersegurança. (2025, 15 de julho). *Telecom security incidents 2024: Annual report*. ENISA. https://www.enisa.europa.eu/publications/telecom-security-incidents-2024 ENISA

Resumo. O relatório anual da ENISA sobre incidentes de segurança em telecomunicações em 2024 apresenta um conjunto de 188 incidentes significativos reportados por autoridades nacionais de 26 Estados-Membros da União Europeia e 2 países da EFTA. Este número representa um aumento de cerca de 20,5% face aos incidentes registados em 2023. Os incidentes analisados incluem interrupções de serviços, falhas sistémicas e outros eventos que afetaram infraestruturas de telecomunicações, sendo que, no conjunto, houve variações no número total de horas de serviço perdidas quando comparado com anos anteriores. O relatório fornece dados agregados sobre as causas dos incidentes, a sua severidade e tendências observadas, servindo de base para reforçar a resiliência das redes e apoiar medidas de mitigação de riscos no sector.

Australian Signals Directorate. (2025). *Annual cyber threat report 2024:25*. Australian Cyber Security Centre. https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf

Resumo: O *Annual Cyber Threat Report 2024:25*, elaborado pelo Australian Signals Directorate através do Australian Cyber Security Centre, analisa as principais ameaças cibernéticas enfrentadas pela Austrália entre julho de 2024 e junho de 2025. O relatório destaca que atores patrocinados por Estados e cibercriminosos continuaram a visar redes governamentais, infraestruturas críticas, empresas e indivíduos, com incidentes a aumentar em número e complexidade. Durante o período de relatório, o centro recebeu dezenas de milhares de notificações de cibercrime e respondeu a mais de 1 200 incidentes, registando crescimentos em várias categorias de ataque, incluindo ransomware, denúncias de dados e ataques de negação de serviço. O documento também apresenta tendências como o uso de técnicas sofisticadas por adversários, as perdas financeiras associadas aos incidentes e recomendações para melhorar a resiliência cibernética, incluindo a adoção de melhores práticas de defesa, atualização de sistemas e gestão de riscos de terceiros. [Para os relatórios dos anos anteriores ver: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/archive]

Canadian Centre for Cyber Security. (2025, 25 de novembro). *The cyber threat to Canada's water systems: Assessment and mitigation*. Communications Security Establishment Canada. https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-water-systems-assessment-mitigation

Resumo: O documento faz uma análise às ameaças informáticas que podem afetar os sistemas de água no Canadá. Conclui que o risco mais provável vem de grupos criminosos que procuram lucro, sendo o *ransomware* o tipo de ataque com maior potencial para pôr em causa a continuidade e a fiabilidade do abastecimento, por poder afetar redes e sistemas operacionais usados no controlo e gestão da água. O relatório admite também que atores ligados a Estados podem manter acessos já preparados dentro destas redes, mas aponta que esses acessos seriam mais plausivelmente usados para causar interrupções apenas em cenários extremos, como situações de crise ou conflito. Para reduzir o risco, o documento apresenta recomendações práticas para os operadores, centradas em diminuir a exposição dos sistemas, reforçar mecanismos de controlo e melhorar rotinas de segurança e de recuperação. [Para relatórios de anos anteriores do Canadian Centre for Cyber Security ver https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessments]

Cybersecurity and Infrastructure Security Agency. (2020, 17 de dezembro). *Advanced Persistent Threat compromise of government agencies, critical infrastructure, and private sector organizations (AA20-352A)* CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

Resumo: Este aviso de segurança da Cybersecurity and Infrastructure Security Agency (CISA) relata compromissos de redes de agências governamentais dos EUA, entidades de infraestruturas críticas e organizações privadas por um ator persistente e sofisticado, identificado como ligado ao serviço de inteligência russo, desde pelo menos março de 2020. O ataque aproveitou vulnerabilidades, incluindo uma cadeia de fornecimento comprometida do software *SolarWinds Orion*, e demonstrou que remover este adversário dos sistemas afetados é altamente complexo. O alerta fornece detalhes sobre os vetores de ataque, versões de software afetadas e recomendações para detetar, mitigar e analisar os possíveis impactos nos sistemas comprometidos, sublinhando o risco grave representado por esta ameaça às infraestruturas e organizações críticas.

Comissão Europeia & Organização do Tratado do Atlântico Norte (NATO). (2023, junho). *EU-NATO Task Force on the resilience of critical infrastructure: Final assessment report*. Comissão Europeia. https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

Resumo: O relatório final da *EU-NATO Task Force on the resilience of critical infrastructure*, publicado em junho de 2023, resulta de uma colaboração entre a União Europeia e a NATO para avaliar desafios de segurança e reforçar a resiliência das infraestruturas críticas na Europa e em países aliados. O documento identifica sectores com importância transversal, como energia, transportes, infraestruturas digitais e espaço, e mapeia os riscos atuais, incluindo ataques híbridos e cibernéticos que podem afetar serviços essenciais. O relatório apresenta recomendações concretas para fortalecer a cooperação entre a UE e a NATO, promovendo a troca de informação, avaliações coordenadas de ameaças, diálogos estruturados sobre resiliência e estratégias comuns para preparar, responder e recuperar de incidentes que possam comprometer infraestruturas críticas.

Entidade Reguladora dos Serviços Energéticos (ERSE). (2025, 12 de maio). *ERSExplica: Investigação ao apagão ibérico de 28 de abril de 2025* [PDF]. https://www.erse.pt/media/0mvf005i/ersexplica-apag%C3%A3o-abril-2025.pdf

Resumo: A ERSE enquadra e descreve o processo de investigação do apagão ibérico de 28/04/2025, articulado a nível europeu (no âmbito da ENTSO-E, com participação de reguladores e da ACER) e a nível nacional no quadro regulatório da qualidade de serviço. O documento refere a reposição do sistema em Portugal (incluindo recurso a capacidades de *black start*, como Castelo de Bode e Tapada do Outeiro) e as implicações regulatórias, nomeadamente análise de qualidade de serviço e potenciais compensações. Quanto aos prazos, por se tratar de um incidente de grau 3 (ICS), o relatório factual deve ser elaborado até 6 meses após o fim do incidente, neste caso, no máximo até 28/10/2025, e o relatório final deverá ser publicado até à data de publicação do Relatório Anual dos ICS 2025 da ENTSO-E, no máximo até 30/09/2026.

E-REDES. (2020, 15 de abril). *Informação sobre incidente de cibersegurança*. Recuperado de e-redes a 2 Dez 2025 https://www.e-redes.pt/pt-pt/noticias/2020/04/15/informacao-sobre-incidente-de-ciberseguranca

Resumo do incidente: O ataque de ransomware dirigido à EDP - Energias de Portugal ocorreu a 13 de abril de 2020, quando a empresa foi alvo de um ataque informático que afetou parte da sua rede corporativa e sistemas de tecnologias de informação. Os atacantes usaram a variante de ransomware conhecida como *Ragnar Locker*, alegando ter extraído dados e exigindo o pagamento de um resgate na ordem de cerca de 10 milhões de euros. Em resposta, a EDP procedeu ao isolamento e à recuperação dos sistemas de tecnologias de informação, ativou medidas de segurança para conter o ataque e cooperou com as autoridades competentes, incluindo entidades de cibersegurança e autoridades judiciárias. Apesar do incidente, não houve interrupção no fornecimento de energia elétrica, embora alguns sistemas internos, como linhas de atendimento e serviços de informação, tenham sido temporariamente afetados. A empresa comunicou oficialmente o ataque a clientes e parceiros, confirmando os esforços de mitigação e o restabelecimento gradual dos sistemas. O caso reforçou os alertas no sector energético e nas infraestruturas críticas quanto ao risco crescente de ataques de *ransomware* a empresas de serviços essenciais na Europa.

Federal Bureau of Investigation, Cyber National Mission Force, & National Security Agency. (2024, June). *People's Republic of China-linked actors compromise routers and IoT devices for botnet operations* [Joint Cybersecurity Advisory]. https://www.ic3.gov/CSA/2024/240918.pdf

Resumo: Relatório técnico oficial (Joint Cybersecurity Advisory) destinado a alertar operadores e o público para campanhas ativas de ciberameaças, publicado por agências como o FBI, o CNMF e a NSA. Descreve uma operação atribuída a atores ligados à República Popular da China que comprometeram centenas de milhares de dispositivos de rede e de "Internet das Coisas", formando a *botnet* "IntegrityTech". Esta *botnet* é usada para ocultar identidades, lançar ataques de negação de serviço (DDoS) e infiltrar redes nos Estados Unidos e em países aliados. O documento recomenda a operadores, fabricantes e administradores a aplicação de correções, o reforço das configurações de segurança e a substituição de dispositivos vulneráveis, reduzindo os riscos para infraestruturas críticas.

Gatlan, S. (2020, 14 de abril). RagnarLocker ransomware hits EDP energy giant, asks for €10M. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/

Resumo: O artigo relata que, em abril de 2020, a multinacional portuguesa Energias de Portugal (EDP) foi alvo de um ataque de ransomware da família RagnarLocker, no qual os atacantes criptografaram sistemas informáticos da empresa e exigiram um resgate de cerca de 1 580 bitcoins (aproximadamente 10 milhões de euros) para desbloquear os ficheiros. Os operadores do ransomware alegaram também ter roubado mais de 10 terabytes de dados sensíveis da infraestrutura da EDP, ameaçando divulgar essas informações caso não fosse pago o resgate. Segundo o artigo, os atacantes publicaram provas de posse de dados, incluindo ficheiros de contas de utilizadores e credenciais, e tentaram pressionar a EDP através de um chat ao vivo da própria infraestrutura usada no ataque. Na mesma notícia, um porta-voz da EDP afirmou que o ataque não afetou o fornecimento de energia, que manteve a normalidade, e que a empresa estava a trabalhar com as autoridades para avaliar e restaurar os sistemas comprometidos.

Jornal Económico. (2024 Fev. 8). Dois anos do ciberataque à Vodafone: Teletrabalho trouxe "dos maiores desafios" de segurança informática. *O Jornal Económico* [em linha]. https://jornaleconomico.sapo.pt/noticias/dois-anos-do-ciberataque-a-vodafone-teletrabalho-trouxe-dos-maiores-desafios-de-seguranca-informatica/

Resumo: O artigo analisa o ciberataque à Vodafone Portugal ocorrido em Fevereiro de 2022, dois anos após o incidente, enquadrando-o no contexto mais amplo dos desafios de segurança informática enfrentados pelas organizações. Destaca-se o impacto do teletrabalho no aumento da superfície de ataque e na complexidade da proteção de sistemas críticos, bem como a importância do reforço das medidas de cibersegurança. O texto sublinha ainda que o ataque à Vodafone constituiu um marco relevante em Portugal, evidenciando vulnerabilidades em infraestruturas essenciais e impulsionando uma maior consciencialização para os riscos cibernéticos no sector empresarial e institucional.

NATO Cooperative Cyber Defence Centre of Excellence. (2025, 18 de julho). *Addressing state-linked threats to critical maritime port infrastructure*. CCDCOE. https://ccdcoe.org/library/publications/addressing-state-linked-cyber-threats-to-critical-maritime-port-infrastructure/

Resumo: Analise ameaças cibernéticas associadas a atores ligados a Estados que visam infraestruturas portuárias marítimas críticas. Com base em informação recolhida junto de vários países, o estudo indica que quase todos os Estados analisados reportaram incidentes cibernéticos relevantes nos últimos cinco anos, mostrando que o sector portuário é um alvo recorrente e com impacto potencial elevado. O relatório identifica como áreas particularmente expostas os sistemas de controlo de acessos e os sistemas de gestão de tráfego marítimo, bem como outras componentes digitais usadas na operação e logística portuárias. Sublinha ainda que a interligação crescente entre sistemas informáticos e sistemas operacionais aumenta a superfície de ataque e pode agravar as consequências de um incidente, afetando a continuidade das operações, a segurança e a eficiência das cadeias de abastecimento. Por fim, o documento defende uma abordagem integrada de cibersegurança para portos marítimos, com medidas de prevenção, resposta e recuperação orientadas para infraestruturas críticas, reforço da cooperação e partilha de informação, e melhoria das práticas de gestão de risco e de resiliência operacional no sector.

Satter, R., & Siddiqui, Z. (2023, August 8). MOVEit hack spawned over 600 breaches but is not done yet – cyber analysts. [notícia de imprensa] *Reuters*. https://www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/

Resumo: O artigo da Reuters descreve o impacto do ataque ao software MOVEit, uma plataforma de transferência segura de ficheiros, que resultou em mais de 600 violações de dados a nível mundial. O ataque explorou uma vulnerabilidade no software e foi atribuído a um grupo de cibercriminosos ligado a esquemas de extorsão, afetando organizações públicas e privadas de vários setores. Os analistas alertam que as consequências do ataque ainda não terminaram, uma vez que continuam a surgir novas vítimas, evidenciando os riscos associados a falhas na cadeia de fornecimento digital e a importância de uma resposta rápida e coordenada a incidentes de cibersegurança.

Vodafone Portugal alvo de ciberataque [comunicado à imprensa]. Recuperado de Vodafone Portugal 2 Dez 2025 https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html

Resumo: O ciberataque de 7 de fevereiro de 2022 à rede da Vodafone Portugal foi um incidente de grande dimensão que deixou cerca de 4 milhões de clientes sem serviços móveis (voz, SMS e dados) durante várias horas. Serviços críticos, como as comunicações de emergência (112/INEM/SIRESP), hospitais e sistemas bancários (caixas Multibanco/ATM) foram temporariamente afetados. A Vodafone classificou o incidente como um ato criminoso deliberado e ativou de imediato planos de contingência e recuperação, dando prioridade ao restabelecimento das comunicações de voz via 2G e de dados via 3G. Em poucos dias, os serviços ficaram praticamente normalizados, enquanto a Polícia Judiciária manteve a investigação em curso, sem que tenham sido identificados publicamente autores até ao momento.

6.2. Exercícios Práticos de Cibersegurança

Agência da União Europeia para a Cibersegurança (ENISA). (2010-). *Cyber Europe* [exercícios paneuropeus de crises de cibersegurança] [Consultado 2 Dez. 2025]. https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe

Resumo: A página apresenta o programa Cyber Europe, uma iniciativa da Agência da União Europeia para a Cibersegurança destinada à realização de exercícios paneuropeus de gestão de crises de cibersegurança. Estes exercícios, realizados periodicamente desde 2010, recorrem a cenários realistas para reforçar a preparação, a coordenação e as capacidades técnicas e operacionais de entidades públicas e privadas na resposta a incidentes e crises de cibersegurança, incluindo setores críticos.

Agência da União Europeia para a Cibersegurança (ENISA). (2022). *Cyber Europe 2022 : After action report*.
https://www.enisa.europa.eu/sites/default/files/publications/Enisa_AAR_2022.pdf

Resumo: O Cyber Europe 2022: After Action Report, publicado pela Agência da União Europeia para a Cibersegurança (ENISA), apresenta os resultados de um exercício europeu de grande dimensão destinado a avaliar a capacidade de resposta a uma crise cibernética complexa. O exercício simulou ataques ao setor da saúde e envolveu entidades públicas e privadas de vários Estados-Membros, permitindo testar os mecanismos de cooperação, coordenação e gestão de incidentes a nível nacional e europeu. O relatório conclui que o exercício contribuiu de forma significativa para o reforço da preparação e da resiliência coletiva e identificou fragilidades, sobretudo nos domínios da comunicação, da partilha de informação e do planeamento prévio, salientando a importância da realização regular deste tipo de exercícios.

Agência da União Europeia para a Cibersegurança (ENISA). (2024). *Cyber Europe 2024 : After action report*. https://www.enisa.europa.eu/sites/default/files/2024-12/Cyber_Europe_AAR_2024_1.pdf

Resumo: Relatório pós-exercício do Cyber Europe 2024, com lições e lacunas observadas. Útil para melhorar playbooks: comunicação, escalonamento e coordenação inter-organizações. Traz recomendações práticas para preparar operações sob stress realista. O exercício teve como pano de fundo cenários complexos de ciberataques, com especial enfoque em infraestruturas críticas, nomeadamente o setor da energia, simulando incidentes com impacto transfronteiriço e efeitos em cascata. O relatório destaca aspetos como a coordenação entre entidades nacionais e europeias, a eficácia dos mecanismos de partilha de informação, a tomada de decisão estratégica em contexto de crise e a articulação entre resposta técnica, operacional e política.

Australian Signals Directorate. (s.d.). *Cyber Security Partnership Program*. [Recuperado 2 DEZ 2025] https://www.cyber.gov.au/partnershipprogram

Resumo: O Cyber Security Partnership Program é um programa do Australian Cyber Security Centre (ACSC), integrado no Australian Signals Directorate (ASD), que cria um enquadramento de colaboração entre o Governo australiano e organizações dos setores público e privado (bem como a academia e a investigação) para reforçar a cibersegurança no país. A iniciativa promove a cooperação e o contacto regular entre parceiros, facilitando o acesso a informação relevante sobre ameaças, orientações práticas e oportunidades de participação em atividades de capacitação, como sessões de trabalho e exercícios, com o objetivo de melhorar a prevenção e a resposta a incidentes.

Centro Nacional de Cibersegurança. (2015-). *C-DAYS: 1.ª edição a 11.ª edição* [Coleção de páginas/relatórios de conferência]. [Consultado 2 Dez. 2025] https://www.cncs.gov.pt/pt/1-edicao/

Resumo: Coleção de relatórios/páginas das edições C-DAYS (1.ª a 11.ª) reúne a documentação oficial associada ao evento anual de cibersegurança do CNCS. Em conjunto, estas edições registam os temas, debates, intervenientes e conclusões que foram marcando a evolução das prioridades nacionais em cibersegurança (ex.: sensibilização, gestão de risco, cooperação institucional, resposta a incidentes, resiliência e enquadramento regulatório), funcionando como um repositório histórico e temático da conferência ao longo dos anos.

Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Cyber Storm 2020 after-action report*. [Recuperado 2 DEZ 2025], de https://fsscc.org/wp-content/uploads/2021/02/Cyber_Storm-2020_After-Action-Report_01052021_Final.pdf

Resumo: O *Cyber Storm 2020 After-Action Report* descreve o exercício nacional de cibersegurança realizado de 10 a 14 de agosto de 2020 pela Cybersecurity and Infrastructure Security Agency (CISA), que reuniu mais de 2 000 participantes de setores públicos e privados para simular a resposta a um ataque cibernético coordenado que afetaria infra-estruturas críticas nos Estados Unidos. O relatório apresenta a conceção, o planeamento, a execução e os resultados do exercício, destacando que o principal objetivo foi fortalecer a prontidão e as capacidades de resposta, testar políticas e procedimentos e reforçar a cooperação e partilha de informação entre organizações. Através de vários cenários de ataque simulados, incluindo exploração de vulnerabilidades em serviços essenciais da Internet, os participantes puderam treinar a coordenação de resposta, avaliar planos nacionais de cibersegurança e identificar áreas de melhoria. Entre as principais conclusões está o aumento da consciência sobre vulnerabilidades em infraestruturas críticas, a necessidade de melhorar a partilha de informação e de reforçar a coordenação entre entidades e sectores, bem como os benefícios de integrar exercícios deste tipo nas estratégias de resiliência cibernética.

International Telecommunication Union. (s.d.). *CyberDrills*. [Recuperado 2 DEZ 2025] https://www.itu.int/en/ITU-D/Cybersecurity/pages/cyberdrills.aspx

Resumo: *CyberDrills* da ITU é um programa que inclui exercícios realizados a nível global, regional e nacional. Estes exercícios têm por objetivo aumentar a capacidade dos países para responder a incidentes cibernéticos através de colaboração regional, workshops, simulações de ataques e troca de informação entre equipas de resposta. Em 2025, foram planeados vários *CyberDrills* regionais (por exemplo nas Américas, África e Ásia-Pacífico), com sessões estruturadas em torno de formação, conferências e exercícios práticos que reforçam competências técnicas e operacionais dos participantes.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (s.d.). *Exercises*. [Consultado 2 Dez. 2025] https://ccdcoe.org/exercises/

Resumo: A página Exercises do CCDCOE lista os principais exercícios de ciberdefesa nos quais o Centro participa ou que organiza em colaboração com a NATO e outros parceiros. Entre estes estão os exercícios "Locked Shields" e "Crossed Swords", concebidos para treinar equipas na defesa e ataque cibernético em cenários realistas, bem como outros exercícios apoiados pelo CCDCOE, incluindo o "Cyber Coalition", que testa a capacidade de defesa de redes da NATO e dos Estados Aliados, e exercícios como "Trident Juncture", "Trident Jaguar" e "CWIX", nos quais o CCDCOE contribui com especialistas em cibersegurança no planeamento, treino e avaliação.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (s.d.). *Locked Shields*. [Consultado 2 Dez. 2025] https://ccdcoe.org/locked-shields/

Resumo: *Locked Shields* é a página institucional do NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) dedicada ao exercício internacional de ciberdefesa do mesmo nome. O exercício constitui uma das maiores iniciativas de treino em ciberdefesa a nível mundial, tendo como objetivo avaliar e reforçar a capacidade de resposta técnica, operacional e estratégica dos participantes perante incidentes cibernéticos complexos e de grande escala. O exercício decorre num ambiente altamente realista, simulando ataques a "infraestruturas críticas", combinando desafios técnicos com aspetos legais, estratégicos e de comunicação. A informação disponibilizada descreve o enquadramento, os objetivos e o papel do CCDCOE na coordenação do exercício, funcionando como fonte oficial de referência para compreender a natureza, a metodologia e a relevância do *Locked Shields* no contexto da cooperação internacional em ciberdefesa.

6.3. Formação, Treino e Sensibilização

Agência da União Europeia para a Cibersegurança (ENISA). (s.d.). *Events*. [Recuperado 3Dez2025] https://www.enisa.europa.eu/events

Resumo: A página "Events" da ENISA apresenta o calendário de eventos públicos e atividades organizadas ou co-organizadas pela Agência da União Europeia para a Cibersegurança (ENISA). Esta secção reúne conferências, workshops, webinars, encontros e outras iniciativas sobre temas como competências e formação, certificação e normalização de cibersegurança, partilha de informação entre sectores críticos, gestão de ameaças, identidade digital, privacidade e higiene cibernética. Alguns exemplos incluem a "European Cybersecurity Skills Conference", encontros sobre normalização de segurança, conferências e eventos dedicados ao reforço da consciencialização em cibersegurança. Estes eventos destinam-se a públicos diversos, incluindo autoridades nacionais e europeias, profissionais do sector privado e outros stakeholders envolvidos na melhoria da resiliência cibernética na União Europeia.

Centro Nacional de Cibersegurança (CNCS). (2023). *C-Academy: Programa de formação avançada em cibersegurança* (Portaria n.º 163/2023, de 5 de abril). https://www.cncs.gov.pt/pt/c-academy/

Resumo: O programa C-Academy é uma iniciativa nacional lançada em 2023 pelo Centro Nacional de Cibersegurança (CNCS) para promover formação avançada em cibersegurança, especialmente dirigida a quadros da Administração Pública, operadores de infra-estruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, em linha com o Regime Jurídico da Segurança do Ciberespaço e as exigências do RJSC/NIS. A C-Academy conta com uma oferta extensa de cursos técnicos e ações de treino especializadas, distribuídos em vários níveis de exigência e ministrados em formatos presencial, online ou híbrido, em parceria com instituições de ensino superior. Até ao primeiro trimestre de 2026, prevê-se formar perto de 9 800 participantes em temas relevantes como gestão de risco, resposta a incidentes, segurança de sistemas (incluindo ICS/SCADA) e outras áreas críticas da cibersegurança. Algumas formações são desenvolvidas em colaboração com entidades internacionais, como a ENISA, reforçando competências técnicas e práticas no contexto nacional e europeu.

CANARIE. (s.d.). *Cybersecurity Initiatives Program (CIP)*. [Recuperado 2 DEZ 2025] https://www.canarie.ca/cybersecurity/cip/

Resumo: O Cybersecurity Initiatives Program (CIP) é um programa da CANARIE que apoia o reforço da cibersegurança no setor canadiano da investigação e do ensino superior. Através deste programa, são disponibilizados recursos e serviços de segurança, por regra sem custos para as entidades elegíveis, com o objetivo de melhorar a prevenção, deteção e resposta a ameaças. O CIP promove iniciativas como avaliação de maturidade e de riscos, monitorização e medidas técnicas de proteção, trabalhando em articulação com parceiros regionais das redes de investigação e educação, para aumentar a resiliência das organizações e reduzir a exposição a incidentes.

NATO Cooperative Cyber Defence Centre of Excellence. (s.d.). *Training*. [Recuperado 10 DEZ 2025] https://ccdcoe.org/training/

Resumo: A página Training do CCDCOE apresenta o portefólio de cursos e formações em ciberdefesa oferecidos pelo NATO Cooperative Cyber Defence Centre of Excellence, um centro de especialização acreditado pela NATO dedicado à investigação, treino e desenvolvimento de capacidades em cibersegurança e ciberdefesa. Entre as formações divulgadas estão cursos de nível estratégico (como seminários executivos), operacional (por exemplo, planeamento operacional em ciberespaço e proteção de infraestruturas críticas), jurídico (como direito das operações cibernéticas) e técnico (incluindo malware, defesa de sistemas, forense digital e segurança de sistemas industriais). A página indica também os cursos programados anualmente, abrangendo sessões presenciais e módulos online (e-learning), com o objetivo de reforçar competências e responder às exigências de um cenário de ameaças digitais em constante evolução.

7. Literatura científica

7.1. Infraestruturas Críticas no Contexto da Segurança e da Resiliência

Bearse, R. (2023, January 6). Understanding critical infrastructure (from *Enabling NATO's collective defense: Critical infrastructure security and resiliency*). U.S. Army War College, Strategic Studies Institute. https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Article/3946047/understanding-critical-infrastructure-from-enabling-natos-collective-defense-ci/

Resumo: O artigo enquadra as infraestruturas críticas como a base do funcionamento do Estado e um elemento essencial da defesa coletiva, destacando as dependências entre os setores civil e militar. Analisa como interrupções em serviços essenciais afetam a mobilidade, a prontidão e a condução de operações, com implicações diretas para a segurança nacional e aliada. O texto sublinha a necessidade de coordenação estreita entre governos, operadores e parceiros internacionais, sendo particularmente relevante para a definição de prioridades em setores como energia, transportes e serviços digitais.

Fita, N. D., Tatar, A., & Ilieva Obretenova, M. (2025). *Security risks assessment of critical energy infrastructures*. Lambert Academic Publishing. ResearchGate+1

Resumo: O livro aborda a segurança energética a partir da perspetiva do risco, analisando como a vulnerabilidade de infraestruturas energéticas críticas (como subestações e linhas de muito alta tensão) pode gerar ameaças com impacto significativo no funcionamento do Estado e no bem-estar da sociedade. Enquadra estes riscos num contexto geopolítico instável e de crise energética, defendendo a necessidade de uma estratégia para reforçar a resiliência destas infraestruturas assente em previsibilidade, flexibilidade, continuidade e capacidade de adaptação. A obra pretende apoiar decisores e responsáveis do setor energético na identificação e gestão de riscos, contribuindo para uma abordagem mais estruturada à proteção de infraestruturas essenciais.

G7 Cyber Expert Group. (2016-). *G7 Cyber Expert Group*. GOV.UK. [última atualização 6/10/2025] https://www.gov.uk/government/collections/g7-cyber-expert-group

Resumo do conteúdo do site: O site G7 Cyber Expert Group reúne uma coleção de documentos produzidos pelo grupo desde 2016, centrados em questões de cibersegurança no setor financeiro. Nele encontram-se publicações como declarações e orientações que abordam temas como inteligência artificial e cibersegurança, boas práticas para reconexão após incidentes e elementos fundamentais para a resiliência contra ransomware e gestão de risco cibernético de terceiros. As publicações são regularmente atualizadas e incluem uma série de "Fundamental Elements", princípios não vinculativos destinados a orientar autoridades e organizações na preparação e resposta a ameaças cibernéticas

Leroy, I., Zolotaryova, I., & Semenov, S. (2025). Impact of Critical Infrastructure Cyber Security on the Sustainable Development of Smart Cities: Insights from Internal Specialists and External Information Security Auditors. *Sustainability, 17*(3), 1188. https://doi.org/10.3390/su17031188

Resumo: Este estudo analisa como a cibersegurança das infraestruturas críticas influencia o desenvolvimento sustentável de cidades inteligentes, considerando perspetivas internas e externas sobre recuperação e resiliência após incidentes cibernéticos. A pesquisa mostra a importância de integrar medidas de proteção e recuperação de forma estratégica para garantir a estabilidade económica e funcional dos serviços urbanos essenciais

Naserinia, V. (2021). *Cyber resilience for critical infrastructure: A systematic review* (Master's thesis). Högskolan i Skövde, University of Skövde. https://www.diva-portal.org/smash/get/diva2%3A1576950/FULLTEXT03.pdf

Resumo: Esta revisão sistemática de literatura usa o método PRISMA para explorar as áreas de investigação sobre resiliência cibernética de infraestruturas críticas, identificando tendências de desenvolvimento e orientações para investigação futura. Combinando análise de co-ocorrência através da ferramenta VOSviewer, o estudo mapeia os principais domínios e lacunas na literatura existente, oferecendo uma visão abrangente sobre como a resiliência cibernética tem sido compreendida, desenvolvida e aplicada em diferentes contextos de infraestruturas críticas.

Ndiaye, S., Diop, I., & Talla, S. (2025). Critical infrastructures: Presentation, cyberattacks and protection mechanisms: A survey. *E3S Web of Conferences, 680*, 00018. DOI:10.1051/e3sconf/202568000018

Resumo: O artigo faz uma revisão do estado da arte sobre infraestruturas críticas, descrevendo os principais tipos de ciberataques que as têm afetado, como ataques de negação de serviço e malware, e salientando que a crescente interligação digital aumenta a exposição a ameaças. Com base nessa realidade, o texto compila e organiza métodos de ataque e mecanismos de proteção usados para mitigar estes riscos, defendendo a urgência de reforçar medidas de defesa para reduzir a frequência e o impacto de incidentes em serviços essenciais.

7.2. Conformidade com NIS2/CER

Becker, M. (2025). *Transposing EU-legislation on critical infrastructure protection: Legal implementation performance in the Baltic Sea region*. International Journal of Critical Infrastructure Protection, 50, 100781. https://doi.org/10.1016/j.ijcip.2025.100781

Resumo: Infraestruturas energéticas críticas tornaram-se alvos centrais na guerra contra a Ucrânia e em ataques híbridos na UE. O artigo analisa a transposição da Diretiva ECI (2008) como precedente da atual Diretiva CER (2022). Demonstra atrasos, desvios e falta de harmonização entre Estados-Membros. Identifica fatores estruturais que afetam a implementação nacional. Relevante para avaliação prática da eficácia da CER.

Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. *Computer Law & Security Review, 53*, 105987. https://doi.org/10.1016/j.clsr.2024.105987

Resumo: O artigo explica que as novas regras da UE para o relatório de sustentabilidade (CSRD/ESRS) obrigam as empresas a incluir a gestão de riscos relacionados com os dados, o que integra a cibersegurança no relatório e melhora a informação para os interessados.

Casaril, F., & Galletta, L. (2025). *Developing security metrics for space systems: A study considering the NIST Cybersecurity Framework 2.0 and the NIS2*. International Journal of Critical Infrastructure Protection, 51, 100805. https://doi.org/10.1016/j.ijcip.2025.100805

Resumo: O artigo propõe métricas de cibersegurança alinhadas com o NIST CSF 2.0 para apoiar a conformidade com a Diretiva NIS2 e o regulamento CER. Foca-se no setor espacial enquanto infraestrutura crítica, identificando lacunas nas funções *Respond* e *Recover*. Demonstra como métricas quantitativas podem apoiar auditorias e decisões de gestão.

Gonçalves, M. (2024). *Sete desafios para a resiliência das entidades críticas: o contributo do Serviço de Informações de Segurança*. *Nação e Defesa*, 169, 27–41. https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD169/NeDef169_Manuel%20Gon%C3%A7alves.pdf

Resumo: O artigo identifica sete desafios centrais para a implementação da Diretiva (UE) 2022/2557 sobre a resiliência das entidades críticas, com foco no papel do Serviço de Informações de Segurança. Analisa questões como a identificação e designação de entidades críticas, a articulação entre segurança, resiliência e cibersegurança, a avaliação nacional de riscos e a definição de estratégias nacionais de reforço da resiliência. O texto destaca a necessidade de uma abordagem holística, integrando dimensões físicas, organizacionais e informacionais, e sublinha a importância da coordenação institucional para assegurar a continuidade de serviços essenciais.

Lomba, P., & Cabugueira, I. (2025, 9 de abril). Critical infrastructure resilience: Implementation of the directive in Portugal. PLMJ. (Informatives Notes) https://www.plmj.com/en/knowledge/informative-notes/Critical-infrastructure-resilience-implementation-of-the-directive-in-Portugal/33889/

Resumo: Nota informativa que descreve a implementação da Diretiva CER no contexto português. Explica impactos práticos (coordenação, responsabilidades e medidas esperadas). Ajuda a traduzir o texto europeu para implicações regulatórias e operacionais.

Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review, 41*, 105502. https://doi.org/10.1016/j.clsr.2020.105502

Resumo: O artigo analisa o enquadramento regulatório aplicável à proteção das infraestruturas críticas contra ciberameaças, com especial enfoque no setor da saúde. Identifica limitações e lacunas na legislação existente, discutindo os desafios específicos associados à continuidade dos serviços de saúde e à proteção de dados sensíveis. O estudo liga as exigências legais às realidades operacionais do setor, sendo útil para justificar prioridades de segurança, medidas de controlo e abordagens de conformidade orientadas para o risco.

Shaffique, M. R. (2024). Cyber resilience act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? *Computer Law & Security Review, 54*, 106009. https://doi.org/10.1016/j.clsr.2024.106009

Resumo: Analisa criticamente o CRA (Cyber Resilience Act)e impacto prático na segurança de IoT (Internet of Things / Internet das Coisas). Discute benefícios, limites e desafios de implementação e fiscalização. É relevante por afetar fornecedores/produtos que entram no ecossistema NIS2/CER.

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review, 52*, 105890. https://doi.org/10.1016/j.clsr.2023.105890

Resumo: Compara NIS2 vs NIS1: âmbito, obrigações, reporte e supervisão. Destaca reforços de enforcement e deveres na cadeia de fornecimento. Ajuda a interpretar impacto por tipo de entidade e setor. Útil para fundamentar capítulos de *compliance* e diferenças regulatórias.

Vieira, S., & Coelho, R. (2025, 26 de março). As novas regras de identificação, proteção e resiliência de entidades críticas. *Direito Público*. https://www.macedovitorino.com/xms/files/2025/20250326-Novas_Regras_Entidades_Criticas.pdf

Resumo: O artigo analisa o Decreto-Lei n.º 22/2025, que transpõe para o ordenamento jurídico nacional a Diretiva (UE) 2022/2557, estabelecendo o novo regime de identificação, proteção e resiliência das entidades críticas em Portugal. Descreve os critérios de designação, as obrigações impostas às entidades (avaliação de riscos, planos de resiliência, notificação de incidentes e realização de exercícios) e o respetivo regime sancionatório. O texto enquadra ainda os prazos para a definição da estratégia nacional de resiliência e da avaliação nacional de risco, salientando o impacto prático do novo quadro legal para operadores de serviços essenciais.

Zemanek, L. (2024). Cyber space in focus: Civilian and military aspects. *China-CEE Institute Weekly Briefing.* 72(1) (Abril 2024). https://china-cee.eu/2024/05/14/czech-republic-political-briefing-cyber-space-in-focus-civilian-and-military-aspects/

Resumo: Em dezembro de 2022 foi publicada a segunda Diretiva relativa à segurança das redes e dos sistemas de informação (Diretiva NIS2). Perante novas ameaças resultantes da digitalização e do aumento generalizado de ciberataques, decidiu-se reformular este enquadramento para reforçar os requisitos de segurança, incluir a segurança da cadeia de fornecimento, simplificar as obrigações de reporte e introduzir medidas mais exigentes de supervisão e de aplicação. Neste trabalho, analisam-se os princípios centrais da NIS2, compara-se o novo regime com o da NIS original e enquadra-se a iniciativa no conjunto das políticas de cibersegurança da União Europeia. Demonstra a interligação entre cibersegurança civil, militar e proteção de infraestruturas críticas.

7.3. Continuidade de negócios (BCP/DRP)[1]

Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization, 12*, 100268. https://doi.org/10.1016/j.rico.2023.100268

Resumo: Discute desafios de segurança e resiliência em ecossistemas cloud. Relevante para continuidade devido a dependências, disponibilidade e recuperação em serviços distribuídos. Ajuda a justificar controlos e requisitos a fornecedores cloud.

Ampratwum, G., Osei-Kyei, R., & Tam, V. W. Y. (2025). *Developing a performance assessment tool for building critical infrastructure resilience through public, private partnership*. International Journal of Critical Infrastructure Protection, 50, 100784. https://doi.org/10.1016/j.ijcip.2025.100784

Resumo: O estudo apresenta um modelo quantitativo para avaliar a resiliência de infraestruturas críticas, incluindo planos de continuidade e recuperação. Introduz indicadores ligados à deteção de eventos disruptivos e recuperação funcional. Enfatiza a importância da cooperação público-privada na continuidade operacional. Aplicável a energia, transportes e telecomunicações.

[1] BCP/DRP (Business Continuity Plan / Plano de Continuidade de Negócio) / (Disaster Recovery Plan / Plano de Recuperação de Desastres)

Araujo, M. S. D., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. *Applied Sciences, 14*(5), 2116. https://doi.org/10.3390/app14052116

Resumo: A resiliência cibernética é altamente relevante para organizações de vários setores e apresenta diferentes nuances consoante as suas dimensões, exigindo também que se reconheçam e distingam as etapas que caracterizam o seu estado. Este artigo procura clarificar os vários conceitos de resiliência cibernética nos seus diferentes contextos, com base numa revisão bibliográfica de artigos, livros e outras publicações. O estudo identifica e mapeia as principais etapas da resiliência, analisa a forma como essas etapas evoluíram ao longo do tempo e, por fim, propõe uma versão atualizada dessas etapas, consolidando as propostas encontradas na literatura. A revisão reforça a importância de compreender estas etapas e de integrar mais a resiliência cibernética na gestão das organizações.

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: Management perspectives. *Australasian Journal of Information Systems, 27.* https://doi.org/10.3127/ajis.v27i0.4183

Resumo: O estudo analisa, através de casos em duas universidades australianas, como gestores de topo compreendem a resiliência cibernética, usando a *Cyber Resilience Matrix* como enquadramento. Verificou-se que gestores de TI e gestores de negócio adotam abordagens diferentes: os primeiros preferem uma perspetiva "de engenharia" e estruturas menos burocráticas, enquanto os segundos favorecem uma abordagem ecológica e hierárquica. Ambos tendem a valorizar mais a fase de preparação antes da crise do que a recuperação após incidentes, procurando deslocar o foco de "cibersegurança" para "ciber-resiliência.

Bellini, E., & Marrone, S. (2020). Towards a novel conceptualization of cyber resilience. In *2020 IEEE World Congress on Services (SERVICES)* (pp. 189,196). IEEE. https://doi.org/10.1109/SERVICES48979.2020.00048

Resumo: O artigo revê as diferentes perspetivas e conceptualizações da resiliência cibernética e propõe uma nova definição holística, capaz de integrar, numa visão única e coerente, as várias dimensões existentes. O conceito integrado resultante é formalizado através da definição de uma nova ontologia abrangente, baseada em domínios, para a resiliência cibernética, destinada a servir como base de conhecimento para um processo eficaz de apoio à decisão multicritério orientado por dados.

Onwubiko, C. (2020). Focusing on the recovery aspects of cyber resilience. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1,13). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139685

Resumo: Os avanços tecnológicos e as novas táticas e técnicas de ciberataque têm utilidade social, mas também têm aumentado os incidentes e as fugas de dados. Como não é possível evitar totalmente ciberincidentes, a ciber-resiliência torna-se essencial numa estratégia de cibersegurança. O artigo destaca que há poucas contribuições sobre recuperação cibernética, um elemento central da resiliência, e propõe um quadro operacional abrangente de recuperação, adaptável e robusto, que pode ser usado diretamente ou ajustado para criar um manual interno. O trabalho descreve detalhadamente os componentes do quadro e apresenta uma versão simplificada para organizações de diferentes dimensões.

Setola, R. (2025). Protection of critical infrastructures in times of peace and war. *International Journal of Critical Infrastructure Protection*. https://www.sciencedirect.com/science/article/pii/S1874548225000605

Resumo: O texto destaca que as ameaças às infraestruturas críticas integram hoje estratégias de conflito mais amplas, designadas por conceitos como guerra híbrida ou irregular, combinando meios físicos e cibernéticos. Face a adversários cada vez mais sofisticados e com apoio estatal, a assimetria entre atacantes e operadores está a diminuir, exigindo uma evolução da proteção baseada apenas na resiliência para abordagens de defesa mais ativas. Este contexto implica maior envolvimento do Estado, incluindo forças de defesa, e o desenvolvimento de estratégias preventivas e, potencialmente, ofensivas, como ficou evidente no conflito Rússia–Ucrânia, que reforçou o papel estratégico das infraestruturas críticas.

Tong, W., Li, H. X., Nasirzadeh, F., Yao, F., & Ji, Y. (2025). Resilience of interdependent infrastructure networks: Review and future directions. *International Journal of Critical Infrastructure Protection, 51*, 100793. https://doi.org/10.1016/j.ijcip.2025.100793

Resumo: Revisão sobre resiliência de redes interdependentes com base em 101 estudos, útil para fundamentar BCP/DRP em contexto multissetorial. Identifica abordagens para avaliação e melhoria da resiliência, incluindo falhas em cascata. Propõe modelos orientados por dados e análise espácio-temporal do desempenho. Defende estratégias holísticas e gestão de trade-offs na continuidade de serviço.

7.4. Resposta a incidentes e playbooks operacionais

Akamai. (2024). XZ utils backdoor: Everything you need to know, and what you can do. *Akamai Blog*. https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know

Resumo: O artigo analisa o caso da backdoor introduzida na biblioteca XZ utils, amplamente utilizada em sistemas Linux, explicando como uma dependência de software crítica foi comprometida de forma deliberada ao longo do tempo. Descreve o impacto potencial deste tipo de ataque na cadeia de fornecimento de software, incluindo riscos sistémicos para organizações que dependem de componentes de código aberto. O texto destaca a importância da governação de dependências, da verificação da integridade dos processos de desenvolvimento e da monitorização contínua, oferecendo orientações práticas de mitigação relevantes para a gestão do risco e da segurança da cadeia de fornecimento.

Alenezi, A., Kumar, A., & Mishra, S. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors, 23*(8), 4060. https://doi.org/10.3390/s23084060

Resumo: O artigo analisa o impacto crescente dos ciberataques sobre infraestruturas críticas, num contexto de forte integração das tecnologias de informação nos processos operacionais. Com base numa análise de incidentes ocorridos nas últimas duas décadas, o estudo identifica os principais tipos de ataques, vulnerabilidades exploradas, consequências operacionais e perfis de vítimas e atacantes. O trabalho sistematiza ainda normas e ferramentas de cibersegurança utilizadas para mitigar estes riscos e apresenta uma estimativa preocupante de aumento significativo de ataques nos próximos anos, prevendo mais de mil incidentes graves a nível mundial num horizonte de cinco anos, com elevados impactos económicos.

Easterly, J., & Fanning, T. (2023, May 7). The attack on Colonial Pipeline: What we've learned & what we've done over the past two years. *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Resumo: Síntese das lições aprendidas do caso "*Colonial Pipeline*" (ransomware) e das respostas institucionais posteriores. Mostra como um incidente cibernético pode forçar paragem operacional e gerar impacto social e económico rápido. Reforça a necessidade de BCP/DRP, decisões de crise e capacidade de restauro.

Ferry, G., & Valadon, G. (2025, September 5). The GhostAction campaign: 3,325 secrets stolen through compromised GitHub workflows. *GitGuardian Blog*. https://blog.gitguardian.com/ghostaction-campaign-3-325-secrets-stolen/

Resumo: O artigo descreve a campanha GhostAction, na qual milhares de segredos, como chaves e credenciais, foram roubados através da exploração de fluxos de trabalho automatizados comprometidos em plataformas de desenvolvimento. O caso demonstra como ambientes de integração e entrega contínuas podem tornar-se vetores de ataque quando não são devidamente protegidos. O texto destaca a necessidade de reforçar os controlos de segurança no desenvolvimento de software, incluindo a limitação de privilégios, a rotação de segredos, a deteção de exposições e a validação de terceiros, sendo também útil como exemplo para ações de sensibilização e exercícios de segurança.

Gülmez, Y., Konur, O., Erbas, M., & Bauk, S. (2025). Identifying cyber attack vulnerabilities in the main lubricating oil system of marine propulsion units. *International Journal of Critical Infrastructure Protection*, 51, 100810. https://doi.org/10.1016/j.ijcip.2025.100810

Resumo: O estudo analisa vulnerabilidades cibernéticas no sistema de óleo lubrificante do motor principal de navios, recorrendo a um modelo de simulação detalhado. Foca-se em ataques a sensores e equipamentos de controlo de temperatura, simulando vários cenários em MATLAB/Simulink para avaliar o impacto no funcionamento do sistema. Identifica componentes críticos mais expostos e quantifica o risco através de uma abordagem que combina simulações de Monte Carlo, metodologias de margens de segurança e um simulador completo de sala de máquinas. Os resultados mostram que diferentes ataques podem aumentar significativamente a temperatura do óleo, podendo causar falhas graves e até catastróficas no motor. Com base nisso, o trabalho propõe estratégias para reforçar a resiliência cibernética no setor marítimo, destacando a necessidade de melhores mecanismos de deteção e medidas de defesa abrangentes.

Islam, U., Ullah, H., Khan, N., Saleem, K., & Ahmad, I. (2025). AI-enhanced intrusion detection in smart renewable energy grids. *International Journal of Critical Infrastructure Protection*, 50, 100769. https://doi.org/10.1016/j.ijcip.2025.100769

Resumo: A adoção rápida de tecnologias da Indústria 4.0 nas redes elétricas de energia renovável aumentou a eficiência, mas também agravou os riscos de cibersegurança, tornando insuficientes os sistemas tradicionais de deteção de intrusões. O estudo propõe um sistema de deteção de intrusões baseado em IA para redes energéticas inteligentes. Combina deteção por assinatura e anomalias, permitindo resposta automática a incidentes. Reduz tempos de reação e de falsos positivos.

Khadidos, A. O., et al. (2025). CyberSentry: Enhancing SCADA security through advanced deep learning and optimization strategies. *International Journal of Critical Infrastructure Protection*, 50, 100782. https://doi.org/10.1016/j.ijcip.2025.100782

Resumo: O artigo apresenta o CyberSentry, um enquadramento de segurança para sistemas de controlo industrial que combina três componentes: um método de seleção de características para melhorar a precisão, um mecanismo de deteção que junta diferentes abordagens (anomalias, assinaturas e aprendizagem automática) e um módulo de otimização para ajustar automaticamente os parâmetros. Ao integrar estas técnicas numa arquitetura única, o sistema procura aumentar a robustez e a cobertura na deteção de ameaças. Em testes com vários conjuntos de dados, o CyberSentry mostrou elevada eficácia, com uma precisão global de 99,5%. Relevante para energia, água e indústria pesada

Mandiant. (2023, April 20). 3CX software supply chain compromise initiated by a prior software supply chain compromise; suspected North Korean actor responsible. *Google Cloud Blog* (Threat Intelligence). https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise

Resumo: Este texto descreve um caso real de comprometimento de software que afetou a aplicação de comunicações 3CX, distribuindo código malicioso através de versões adulteradas disponibilizadas aos utilizadores. A análise indica que a intrusão terá começado por um comprometimento anterior noutro fornecedor de software, mostrando como um ataque à cadeia de fornecimento pode servir de "ponte" para um segundo ataque. O artigo detalha a forma como o malware foi introduzido e executado, e salienta implicações práticas para a gestão de fornecedores e terceiros, como verificação de origem, monitorização contínua e procedimentos de contenção e comunicação em caso de incidente.

McCallion, J. (2025, August 7). Air France and KLM confirm customer data stolen in third-party breach. *IT Pro*. https://www.itpro.com/security/data-breaches/air-france-and-klm-confirm-customer-data-stolen-in-third-party-breach

Resumo: O artigo relata uma violação de dados associada a uma plataforma de terceiros usada por centros de contacto, que levou ao acesso indevido a dados de alguns clientes das companhias. O caso é um exemplo claro de risco originado no fornecedor, com impacto reputacional e obrigações de notificação. Serve para sustentar requisitos contratuais, avaliação e monitorização de fornecedores e preparação de resposta a incidentes envolvendo terceiros.

Saraf, I., & Balassiano, O. (2025, September 3). Model namespace reuse: An AI supply-chain attack exploiting model name trust. *Unit 42* (Palo Alto Networks). https://unit42.paloaltonetworks.com/model-namespace-reuse/

Resumo: O artigo descreve um vetor de ataque à cadeia de fornecimento aplicado a modelos de inteligência artificial, explorando a confiança excessiva em nomes/identificadores de modelos. Mostra como um atacante pode reaproveitar um "nome" anteriormente usado (por exemplo, quando um autor ou organização é eliminado ou quando há transferências de propriedade) e publicar um modelo malicioso com o mesmo identificador, levando sistemas e pipelines a descarregá-lo automaticamente. A análise inclui exemplos em catálogos e plataformas de modelos e sublinha a necessidade de controlos de proveniência e validação, como verificação de origem, políticas de consumo seguro de artefactos e governação de repositórios e dependências externas.

Taylor, J. (2025, July 2). Qantas confirms cyber-attack exposed records of up to 6 million customers. *The Guardian*. https://www.theguardian.com/business/2025/jul/02/qantas-confirms-cyber-attack-exposes-records-of-up-to-6-million-customers

Resumo: A notícia descreve um incidente na Qantas com potencial exposição de dados pessoais de milhões de clientes, associado a uma plataforma de terceiros usada no apoio ao cliente. O caso é relevante para discutir gestão de crise, comunicação pública e dependências do ecossistema de fornecedores. Também é útil para construir cenários de exercícios e testes de stress focados em resposta a incidentes e coordenação com autoridades.

7.5. Avaliação de riscos e auditorias

Alguliyev, R., Aliguliyev, R., & Sukhostat, L. (2025). An approach for assessing the functional vulnerabilities criticality of CPS components. *Cyber Security Applications, 3*, 100058. https://doi.org/10.1016/j.csa.2024.100058

Resumo: O artigo propõe um método quantitativo para classificar a criticidade e as vulnerabilidades dos sistemas. A abordagem permite ordenar e destacar os componentes mais vulneráveis, testada com um modelo e três cenários de ataque. Em comparação com métodos como TOPSIS, VIKOR e ELECTRE, mostrou-se eficaz e apoia decisões mais informadas sobre medidas de proteção.

Aribilola, I., Alsamhi, S. H., Breslin, J. G., & Asghar, M. N. (2025). SuPOR: A lightweight stream cipher for confidentiality and attack-resilient visual data security in IoT. *International Journal of Critical Infrastructure Protection*, 50, 100786. https://doi.org/10.1016/j.ijcip.2025.100786

Resumo: O artigo apresenta o SuPOR, um algoritmo criptográfico leve concebido para proteger dados visuais em dispositivos da Internet das Coisas utilizados em contextos críticos. A proposta assegura confidencialidade e resistência a ataques, mantendo um baixo custo computacional adequado a equipamentos com recursos limitados. O estudo demonstra a aplicabilidade da solução em áreas como saúde, vigilância, cidades inteligentes e serviços públicos, alinhando-se com requisitos de segurança, privacidade e resiliência operacional.

Calviño, B. O., Rodriguez, E., Costa, J. J., & Oriol, M. (2025). Enhancing cybersecurity in railways: Machine learning approaches for attack detection. *International Journal of Critical Infrastructure Protection*, 50, 100788. https://doi.org/10.1016/j.ijcip.2025.100788

Resumo: O artigo analisa a aplicação de técnicas de aprendizagem automática para a deteção de ciberataques em sistemas ferroviários, um setor crítico fortemente dependente de tecnologias digitais. Demonstra como estes métodos permitem identificar tanto ataques conhecidos como ameaças novas, melhorando a capacidade de deteção em ambientes operacionais complexos. O estudo evidencia o contributo destas abordagens para reforçar a resiliência operacional e a continuidade dos serviços de transporte público, sublinhando a importância da inteligência artificial na segurança de infraestruturas críticas.

Coppolino, L., Nardone, R., Petruolo, A., Romano, L., & Souvent, A. (2023). Exploiting digital twin technology for cybersecurity monitoring in smart grids. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES)* (pp. 1,10). ACM. https://doi.org/10.1145/3600160.3605043

Resumo: O artigo propõe a utilização de "gémeos digitais" para apoiar a monitorização de cibersegurança em redes elétricas inteligentes, permitindo observar o comportamento do sistema e identificar anomalias em tempo quase real. A abordagem reforça a deteção precoce de incidentes e melhora a compreensão das interações entre tecnologias operacionais e de informação. O estudo demonstra o potencial dos "gémeos digitais" para aumentar a visibilidade e apoiar respostas mais informadas em infraestruturas críticas do setor da energia.

Hobbs, C., Naser, Z., & Tzinieris, S. (2025, May). *Securing the nuclear supply chain: Addressing the issue of counterfeiting*. *International Journal of Critical Infrastructure Protection, 50*, 100767. https://doi.org/10.1016/j.ijcip.2025.100767

Resumo: O artigo analisa o problema da contrafação na cadeia de fornecimento do setor nuclear e os riscos que pode introduzir na segurança e na operação de infraestruturas críticas. Discute fragilidades de controlo, rastreabilidade e reporte, e como estas lacunas podem comprometer confiabilidade e conformidade. É particularmente relevante para políticas de gestão de fornecedores críticos e para requisitos de resiliência e supervisão em setores de elevado impacto

Itäpelto, T., Elhajj, M., & van Sinderen, M. (2025). *Digital twin application in lifecycle security of critical infrastructures: A systematic literature review*. International Journal of Critical Infrastructure Protection, 50, 100783. https://doi.org/10.1016/j.ijcip.2025.100783

Resumo: O artigo apresenta uma revisão sistemática da literatura sobre a aplicação de "gémeos digitais" na segurança ao longo do ciclo de vida das infraestruturas críticas. Analisa de que forma estes modelos digitais permitem monitorizar riscos de forma contínua, apoiar testes de segurança, auditorias e simulações de cenários de ataque ou falha. O estudo destaca a utilidade dos gémeos digitais em ambientes complexos e com longos períodos de operação, evidenciando o seu contributo para decisões de segurança mais informadas e baseadas no risco.

Kampova, K., Lovecek, T., & Rehak, D. (2020). Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *International Journal of Critical Infrastructure Protection, 30*, 100376. https://doi.org/10.1016/j.ijcip.2020.100376

Resumo: O artigo apresenta uma abordagem quantitativa para avaliar a eficácia dos sistemas de proteção física de elementos de infraestruturas críticas, com aplicação prática no contexto da República Eslovaca. O método permite realizar avaliações estruturadas, repetíveis e comparáveis, apoiando a identificação de fragilidades e a priorização de medidas de proteção. O estudo é particularmente relevante para a resiliência não digital e para a integração entre proteção física e cibersegurança, contribuindo para decisões fundamentadas sobre investimento e reforço da segurança.

Laxman, N., et al. (2023). Understanding resilience: Looking at frameworks & standards: A systematic study from cyber perspective. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 295,300). IEEE. https://doi.org/10.1109/CSR57506.2023.10224958

Resumo: A resiliência tornou-se um conceito central devido à crescente complexidade e interdependência dos sistemas, em especial das infraestruturas críticas, cuja dependência de tecnologias de informação torna mesmo interrupções curtas economicamente graves. O estudo analisa o conceito de resiliência a partir da perspetiva cibernética, reconhecendo a sua aplicação em várias áreas, e apresenta uma revisão sistemática focada em enquadramentos e normas, com o objetivo de compreender como construir sistemas capazes de responder e recuperar de perturbações inesperadas.

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting, 13*(1), 25,47. https://doi.org/10.1504/IJMFA.2021.116207

Resumo: O artigo analisa o contributo da auditoria interna para a cibersegurança nas organizações, clarificando o seu papel na governação, no controlo interno e na gestão do risco tecnológico. Discute como a auditoria interna pode apoiar a definição de responsabilidades e linhas de defesa, bem como a criação de procedimentos e controlos verificáveis para avaliar a eficácia das medidas de segurança. O texto enquadra ainda a auditoria como instrumento de apoio ao cumprimento de requisitos regulatórios e de reforço da conformidade, ligando cibersegurança a práticas de supervisão e melhoria contínua.

Rehak, D., et al. (2024). Critical entities resilience failure indication. *Safety Science, 170*, 106371. https://doi.org/10.1016/j.ssci.2023.106371

Resumo: O artigo analisa como identificar e medir sinais de falha de resiliência em entidades críticas, propondo indicadores que permitem detetar fragilidades antes de ocorrerem incidentes graves. O estudo contribui para tornar o conceito de resiliência mais operacional, através da definição de métricas, limiares e mecanismos de alerta que apoiam a monitorização contínua. É particularmente relevante para a avaliação da prontidão organizacional e para a adoção de medidas preventivas e de melhoria contínua em contextos regulatórios exigentes.

Rehak, D., Hromada, M., & Lovecek, T. (2020). Personnel threats in the electric power critical infrastructure sector and their effect on dependent sectors: Overview in the Czech Republic. *Safety Science, 127*, 104698. https://doi.org/10.1016/j.ssci.2020.104698

Resumo: O artigo analisa ameaças relacionadas com pessoas no setor da energia elétrica, como erro humano, negligência e ações internas maliciosas, e o efeito dessas ocorrências em setores dependentes. Com base no contexto da República Checa, evidencia como incidentes de origem humana podem propagar impactos a outras atividades essenciais, reforçando a importância de considerar dependências e risco sistémico. O estudo é útil para sustentar medidas organizacionais como controlo de acessos, segregação de funções, formação e mecanismos de prevenção e deteção de "insiders", com impacto direto na continuidade e na resiliência operacional.

Tekinerdogan, B., Aksit, M., Catal, C., Hurst, W., & AlSkaif, T. (Eds.). (2023). *Management and engineering of critical infrastructures*. Academic Press. https://www.sciencedirect.com/book/edited-volume/9780323993302/management-and-engineering-of-critical-infrastructures

Resumo: Este livro reúne contributos de vários autores sobre a gestão e a engenharia de infraestruturas críticas, abordando de forma integrada aspetos técnicos e organizacionais. Analisa temas como a avaliação de riscos, a governação, as interdependências entre sistemas, o desenho de arquiteturas e a operação de infraestruturas complexas, bem como mecanismos de resiliência. A obra constitui uma base metodológica relevante para a definição de modelos de risco, práticas de gestão e processos de auditoria, sendo útil tanto para equipas técnicas como para decisores.