LABORATÓRIO NACIONAL
DE ENGENHARIA CIVIL

A CIBERSEGURANÇA EM PORTUGAL

Panorâmica organizativa e legislativa em 2022

RELATÓRIO 263/**2023 – CD/NTIEC**

LABORATÓRIO NACIONAL
DE ENGENHARIA CIVIL

A CIBERSEGURANÇA EM PORTUGAL

Panorâmica organizativa e legislativa em 2022

Lisboa • julho 2023

OAC&T CONSELHO DIRETIVO

RELATÓRIO 263/**2023 – CD/NTIEC**

Título

A CIBERSEGURANÇA EM PORTUGAL
Panorâmica organizativa e legislativa em 2022

Autoria

CONSELHO DIRETIVO

João Palha Fernandes
Investigador Auxiliar, Núcleo de Tecnologias da Informação em Engenharia Civil

Copyright © LABORATÓRIO NACIONAL DE ENGENHARIA CIVIL, I. P.
AV DO BRASIL 101 • 1700-066 LISBOA
e-mail: lnec@lnec.pt
www.lnec.pt

Relatório 263/2023

Proc. 0109/3401/1093401

A CIBERSEGURANÇA EM PORTUGAL

Panorâmica organizativa e legislativa em 2022

Resumo

As sociedades contemporâneas estão crescentemente dependentes das tecnologias de informação e de comunicação. Embora estas tecnologias tragam benefícios inegáveis às sociedades, aumentam as ameaças e os riscos que resultam da sua dependência. Por esse motivo têm sido tomadas medidas em Portugal para dotar o país de uma melhor resposta operacional a ciberataques.

Sendo esta realidade pouco conhecida dos agentes da sociedade e da administração pública, este relatório apresenta uma panorâmica da situação atual da área de cibersegurança no plano organizativo e legislativo.

Palavras-chave: Ameaça / Risco / Ciberespaço / Cibersegurança

CYBERSECURITY IN PORTUGAL

Organisational and legislative overview in 2022

Abstract

Contemporary societies are increasingly dependent on information and communication technologies. Although these technologies bring undeniable benefits for societies, they increase the threats and risks that result from their dependence. In the last years a number of measures have been taken in Portugal to provide the country with a better operational response to cyberattacks.

Since this reality is still largely unknown, this report presents of the current situation in the area of cybersecurity at the organisational and legislative level.

Keywords: Threat / Risk / Cyberspace / Cybersecurity

Índice

Índice de figuras

Glossário

ciberespaço – ambiente informático cujo objetivo é o de criar, armazenar, modificar, trocar, partilhar, utilizar e eliminar informação, assim como de alterar o comportamento de recursos físicos.

ciberataque – ataque informático dirigido contra um sistema de informação com objetivo de prejudicar parcial ou totalmente a sua segurança.

hacker – pessoa que explora as falhas de segurança de um sistema com objetivos maliciosos.

infraestrutura crítica – componente ou sistema cujo funcionamento é essencial para uma sociedade cuja perturbação ou destruição teria um impacto significativo.

IoT – extensão da conectividade de rede e capacidade de computação para dispositivos que não são considerados computadores.

malware – programa introduzido num sistema de forma encoberta com a intenção de perturbar o seu funcionamento ou comprometer a segurança dos dados.

phishing – forma de comunicação baseada em técnicas de engenharia social com a intenção de ludibriar a vítima a revelar informação confidencial ou a instalar *malware.*

ransomware – tipo de *malware* concebido para impedir o acesso a dados tendo como objetivo exigir um resgate para que os mesmos sejam disponibilizados.

Lista de acrónimos

3G – 3ª Geração

4G – 4ª Geração

5G – 5ª Geração

CCD – Centro de Ciberdefesa

CERT – *Community Emergency Response Team*

CNCS – Centro Nacional de Cibersegurança

CSIRT – *Computer Security Incident Response Team*

CSSC – Conselho Superior de Segurança do Ciberespaço

EMFGA – Estado Maior General da Forças Armadas

GNS – Gabinete Nacional de Segurança

PCM – Presidência do Conselho de Ministros

IoT – *Internet of Things*

SIS – Serviços de Informação de Segurança

TAC – Tomografia Computorizada

UNC3T – Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

1 | Introdução

A adoção pelas pessoas e organizações de novas tecnologias de informação e de redes de comunicação criou um ambiente em se interage, troca e desenvolve atividades *online* designado por **ciberespaço**. Este ambiente inclui tudo o que existe no mundo digital como os *websites*, o correio eletrónico, as plataformas de redes sociais e as outras formas de comunicação digital. É baseado numa rede alargada de tecnologias de informação e comunicação que permite que as pessoas interajam entre si e que acedam a conteúdo digital de qualquer parte do mundo.

Esta mudança tecnológica induziu a que uma parcela crescente da economia passasse a ser baseada em infraestruturas e serviços existentes no ciberespaço, uma situação que oferece novas capacidades, mas que cria novos riscos. Tecnologias emergentes como a *Internet of Things* (IoT), *Cloud Computing* e o *5G* são tecnologias baseadas em elementos do ciberespaço que oferecem possibilidades para aumentar a flexibilidade e eficiência dos processos. No entanto, a utilização de processos baseados em infraestruturas do ciberespaço cria a possibilidade de ocorrência de incidentes com repercussões económicas que não podem ser ignoradas. Observe-se que estes incidentes têm o potencial de se estender para além do espaço digital caso tornem inoperacionais infraestruturas físicas manipuladas ciberneticamente, tendo um impacto económico elevado caso interfiram com os serviços essenciais ao funcionamento de uma sociedade.

Com a crescente dependência das tecnologias digitais, a ameaça de ataques cibernéticos tornou-se mais prevalente e sofisticada, pelo que é necessário que os diversos agentes da sociedade – quer sejam pessoas, quer sejam organizações públicas ou privadas – adotem medidas para proteger os seus ativos digitais, uma prática designada por **cibersegurança**.

Este relatório pretende sensibilizar os utilizadores e gestores de infraestruturas informáticas para a adoção da cibersegurança como parte integrante do seu quotidiano. Nas páginas seguintes ir-se-á descrever as motivações para a adoção de medidas de segurança no ciberespaço, qual é a missão das organizações em Portugal cujo foco é cibersegurança e a legislação mais relevante que foi produzida para melhorar a segurança do ciberespaço nacional.

2 | Motivações

Atualmente, o ciberespaço permite que comuniquemos com os nossos amigos e colegas, mantem-nos informados, apoia-nos nas atividades lúdicas ou profissionais que desempenhemos e controla o funcionamento de um sem número de dispositivos físicos.

O ciberespaço inclui as redes bancárias utilizadas pelos cartões de crédito ou para fazer transferências e pagamentos, os sistemas de informação em saúde que armazenam os registos clínicos, as redes de fornecimento de energia, as redes de abastecimento de água e as redes de transporte público. Esta conetividade tem alterado a forma como comunicamos, viajamos e fazemos compras. Permite realizar reuniões à distância com participantes de múltiplas organizações, permite consultar ou trocar informação de forma muito célere e permite que os investigadores de instituições geograficamente distantes colaborem mais facilmente num projeto comum..

A larga maioria da população portuguesa está ligada direta ou indiretamente ao ciberespaço. Em 2022, 11,8% das famílias portuguesas não tinham acesso à Internet em casa, o que constitui uma redução substancial relativamente a 2010, quando cerca de metade das famílias não tinha esta ligação. Na última década assistiu-se, também, a uma crescente utilização por parte das famílias para comunicar, obter informação, comprar, realizar transações financeiras, utilizar serviços de saúde, aprender e utilizar ludicamente (INE, 2022a). No caso das empresas portuguesas, em 2022, apenas 3,1% não tinham acesso à Internet, por comparação com 15% em 2010 (INE, 2022b).

Dada a difusão digital existente, um número crescente de serviços assume que os elementos tecnológicos em que se sustentam são fiáveis e robustos. Esta situação leva a que tais serviços estejam vulneráveis a atividades maliciosas no espaço digital.

As **vulnerabilidades** existentes no espaço digital são exploradas por criminosos, ativistas, terroristas e até estados. Estes cibercriminosos conhecidos como ***hackers*** ou **piratas informáticos** (Figura 2.1) tentam obter informações confidenciais, lançar programas maliciosos (***malware***), roubar identidades, invadir contas bancárias, utilizar fraudulentamente cartões de crédito, enganar pessoas e, de uma maneira geral causar danos. Os ataques utilizados pelos *hackers*, conhecidos como **ciberataques**, utilizam métodos como o rastreamento de vulnerabilidades, a exploração de vulnerabilidades conhecidas e o uso de técnicas de manipulação humana para obter informações como as credenciais de acesso (**engenharia social**).

Figura 2.1 – Hackers (CNCS, 2021)

Os impactos de um incidente variam de forma muito substancial com graus de severidade diferentes, desde a indisponibilidade um *website* institucional com impacto reputacional para a organização até à

redução da capacidade de defesa das forças armadas com perda de vidas humanas e avultados danos materiais para o país.

Os ciberataques ocorrem diariamente em Portugal, tendo sido registados 8971 incidentes em 2022, dos quais 33,2% afetaram organismos da Administração Pública (Sistema de Segurança Interna, 2023). Alguns dos ciberataques foram divulgados nos meios de comunicação social de grande audiência, uma vez que atingiram empresas de grande dimensão, como foram os casos dos ataques que afetaram a Impresa, a Vodafone Portugal e o Hospital Garcia da Orta.

Em janeiro de 2022, os *sites* da empresa de comunicação social Impresa, detentora do jornal Expresso e da operadora de televisão SIC, foram alvos de um ataque informático. O grupo de atacantes, que se identificaram como pertencentes ao Lapsus$ Group, realizaram uma intrusão à rede interna e tomaram o controlo dos serviços de *cloud*, da plataforma de *streaming* e dos *websites* da Impresa. A recuperação parcial iniciou-se com a disponibilidade dos *websites* do Expresso e da SIC Notícias passados três dias. No entanto, a recuperação da normalidade levou pelo menos três semanas, uma vez que a plataforma de *streaming* Opto só voltou a estar disponível passado este período (Agência Lusa, 2022).

Em fevereiro de 2022, ocorreu um ciberataque à operadora de telecomunicações Vodafone que inoperacionalizou as redes móveis 3G, 4G e 5G levando à paralisação dos serviços de voz, televisão e dados. Milhões de clientes ficaram impossibilitados de fazer chamadas telefónicas, enviar mensagens de texto, utilizar a Internet ou aceder à televisão por cabo. Milhares de operações bancárias intermediadas pela SIBS, a maior operadora de redes de caixas automáticas e terminais de pagamento, não puderam ser realizadas. Foram afetadas as comunicações de diversas corporações de bombeiros, operadores de ambulâncias e hospitais, o que dificultou o acesso aos cuidados de saúde a nível nacional. O processo de recuperação do ataque levou mais de três dias e envolveu várias equipas da Vodafone e diversos parceiros externos (Goodin, 2022).

Em abril de 2022, o Hospital Garcia da Orta foi alvo de um ataque cibernético que impediu o acesso aos exames imagiológicos. Os atacantes encriptaram as imagens de radiografia e tomografia computorizada (TAC) e exigiram um pagamento em troca da recuperação das imagens, um tipo de ataque conhecido como ***ransomware***. Como consequência os serviços de urgência foram afetados e foram canceladas consultas, cirurgias e exames imagiológicos (IT Security, 2022).

Os ciberataques podem, também, ser promovidos por outros estados e ter objetivos de espionagem, de disrupção das infraestruturas críticas ou para conduzir à perda de confiança nas instituições públicas.

Um exemplo desta situação aconteceu no conflito que opôs a Geórgia à Rússia, no verão de 2008, em que um ataque militar convencional foi precedido de forma sincronizada por um ciberataque. Em 7 de agosto, as forças da Geórgia lançaram um ataque contra as forças separatistas da Ossétia do Sul em resposta a bombardeamentos a aldeias georgianas ocorridos na semana anterior. Em resposta, a 8 de agosto, a Rússia, o único país que na altura reconhecia o governo da Ossétia do Sul, respondeu ao ataque invadindo a Geórgia com meios militares terrestres. No entanto, um dia antes do ataque russo, vários *sites* do governo e da comunicação social da Geórgia foram atacados de forma coordenada

criando uma perda de confiança entre a população georgiana, uma vez que isolou a Geórgia do resto do mundo. Foi o primeiro caso em que uma operação de combate terrestre foi executada em conjunto com um ataque no ciberespaço (Shakarian, 2011).

3 | Organização Nacional

Em Portugal existem quatro entidades públicas que promovem a cibersegurança a nível nacional: uma de coordenação e as restantes respetivamente restritas à segurança nacional, vigilância criminal e inteligência.

A entidade de coordenação de cibersegurança nacional é o Centro Nacional de Cibersegurança (CNCS). Foi criada em 2014 (Decreto-Lei n.º 69/2014 de 9 de maio) com o objetivo de contribuir para a utilização segura do ciberespaço através da promoção de melhores medidas de cibersegurança em Portugal, em cooperação com organizações congéneres a nível internacional em matéria de segurança e em articulação com as outras entidades de cibersegurança nacionais. Do ponto de vista de organização, o CNCS é uma divisão do Gabinete Nacional de Segurança (GNS), um serviço que depende diretamente da Presidência do Conselho de Ministros (PCM). O CNCS é a autoridade no domínio da cibersegurança das entidades públicas, operadores de infraestruturas críticas, operadores de serviços essenciais, prestadores de serviços digitais e da sociedade portuguesa em geral. Um dos serviços integrantes do CNCS é o CERT.PT (*Community Emergency Response Team of .PT*). É um serviço que coordena a resposta a incidentes de cibersegurança que afetem equipamentos pertencentes a uma rede de um operador de comunicações português, de uma pessoa singular ou coletiva residentes em território nacional.

A entidade nacional orientada para a segurança nacional é o Centro de Ciberdefesa (CCD). O CCD é uma entidade criada em 2014 (Decreto-Lei n.º 184/2014 de 29 de dezembro) inserida no Estado Maior General da Forças Armadas (EMGFA) constituída por militares dos três ramos das Forças Armadas (Marinha, Exército e Força Aérea). A sua missão é o de garantir a segurança da informação e dos sistemas de informação militares, quer numa ótica de defesa, quer eventualmente numa ótica de ataque.

A entidade cujo foco é a vigilância criminal no ciberespaço é a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T). A UNC3T é do ponto de vista organizacional uma unidade operacional especializada da Polícia Judiciária criada em 2016 (Decreto-Lei n.º 81/2016 de 29 de novembro). É uma unidade que se dedica à investigação e recolha de provas de crimes cometidos no ciberespaço que utilizem meios informáticos cujo alvo sejam ativos digitais.

A entidade que se preocupa com a inteligência é uma unidade interna dos Serviços de Informação de Segurança (SIS). É uma unidade que se foca na avaliação e alerta precoces para prevenir ameaças de cibercriminalidade que coloquem a segurança do estado em risco. Dado o perfil que possui não se conhece de forma detalhada a sua atividade, mas sabe-se que tem promovido a adoção de medidas de resiliência das infraestruturas informáticas portuguesas nos setores de transporte público, abastecimento de água, fornecimento de energia, centros comerciais e parques de diversões (Sistema de Segurança Interna, 2023; Security Magazine, 2022).

Complementando estas entidades públicas existe a Rede Nacional CSIRT (*Computer Security Incident Response Team*), uma rede de equipas responsáveis pela segurança informática constituída por mais de quatro dezenas de membros, sendo uma delas o CERT.PT (Security Magazine, 2021). O seu objetivo é o de fomentar a cooperação em caso de incidentes, partilhar boas práticas de segurança e coligir informações estatísticas sobre incidentes cibernéticos (Rede Nacional CSIRT, 2023).

Para além destas entidades, existem outras de natureza consultiva ou técnico-científica: o Conselho Superior de Segurança do Ciberespaço e o Observatório de Cibersegurança.

O Conselho Superior de Segurança do Ciberespaço (CSSC) é um órgão de consulta do Primeiro-Ministro para assuntos relativos à segurança do ciberespaço. É um grupo criado em 2018 (Lei n.º 46/2018 de 13 de agosto) que monitoriza a execução das medidas de cibersegurança planeadas e propõe alterações ou novas medidas em planeamentos futuros.

O Observatório de Cibersegurança é um órgão de natureza técnico-científica constituído por académicos convidados pelo CNCS com o objetivo de produzir indicadores e séries temporais no domínio da cibersegurança.

4 | Legislação

Em 2015, foi aprovada a primeira peça legislativa portuguesa na área de cibersegurança, a Estratégia Nacional de Segurança do Ciberespaço. O seu propósito foi o de reforçar a segurança do ciberespaço a nível nacional. Como ameaças do ciberespaço identificava o cibercrime associado à fraude bancária e à usurpação de identidade (*identity theft*), bem como o *hacktivismo* político e religioso associado à revelação de informação sensível, à sabotagem informática e à espionagem. Enfatizava que os criminosos, terroristas ou *hacktivistas* possuíam capacidades para conduzir ações com impacto na segurança de infraestruturas críticas do ciberespaço nacional criando ameaças à sobrevivência do próprio estado. O anexo de natureza mais operacional identificava seis linhas de atuação (designadas por Eixos) para aumentar a segurança no ciberespaço nacional: estabelecer uma estrutura de segurança do ciberespaço (Eixo 1), combater o cibercrime (Eixo 2), proteger o ciberespaço (Eixo 3), promover uma cultura de cibersegurança (Eixo 4), fomentar as atividades de investigação e desenvolvimento (Eixo 5) e cooperar a nível nacional e internacional (Eixo 6). Face à expectável evolução das ameaças e vulnerabilidades devidas ao desenvolvimento tecnológico, definiu que a estratégia seria revista num prazo máximo de três anos (Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho).

Em 2016, foi aprovada pelo Parlamento Europeu a Diretiva Segurança das Redes e Informação (Diretiva SRI) que impôs a obrigação da adoção de um conjunto de medidas de cibersegurança às entidades suscetíveis de sofrerem incidentes graves. A Diretiva SRI procura garantir que as organizações responsáveis pelas infraestruturas informáticas críticas para o funcionamento da sociedade tomam as medidas adequadas para prevenir os ciberriscos que se colocam às redes e aos sistemas de informação que utilizam nas suas operações, sendo obrigadas a participar os incidentes com impacto relevante às autoridades competentes. A Diretiva SRI cria o enquadramento legal para os Estados-Membros legislarem no domínio da cibersegurança (Diretiva (UE) 2016/1148 de 6 de julho).

Apenas em 2018 foi transposta a Diretiva SRI para o ordenamento jurídico nacional (Lei n.º 46/2018 de 13 de agosto). A legislação portuguesa definiu como sendo especialmente suscetíveis a sofrerem incidentes de segurança com repercussões graves as seguintes entidades:

- prestadores de serviços nos setores de abastecimento de água, fornecimento de energia, transportes, instituições bancárias e infraestruturas digitais (e.g. registo de nomes de domínio, pontos de troca de tráfego);
- prestadores de serviços digitais de pesquisa, de cloud computing e de marketplaces;
- operadores de um componente crítico para a manutenção de funções para a saúde ou segurança;
- e, órgãos públicos como serviços do Estado, regiões autónomas, autarquias, reguladores, institutos públicos, empresas públicas e associações públicas.

Os requisitos de segurança das redes e sistemas de informação que estas entidades são obrigadas a cumprir foram apenas regulamentadas em 2021 (Decreto-Lei n.º 65/2021 de 30 de julho). As regras

para a notificação de incidentes que estas entidades estão obrigadas a comunicar ao CNCS, bem como outras exigências relativas aos pontos de contacto permanente e responsável de segurança, foram regulamentadas em 2022 (Regulamento n.º 183/2022 de 21 de fevereiro).

Em 2019, um ano posteriormente ao originalmente definido, foi revista a Estratégia Nacional de Segurança do Ciberespaço. Identifica três objetivos estratégicos (fortalecer a resiliência do ciberespaço, promover a capacidade nacional de inovação e garantir a alocação de recursos adequados para a segurança do ciberespaço) e mantêm as seis linhas de atuação da estratégia de 2015. Passa a ser objeto de avaliação anual pelo CSSC, onde se incluirá uma verificação dos objetivos estratégicos e do plano de ação. Define que a estratégia seja integralmente revista num prazo máximo de cinco anos (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho).

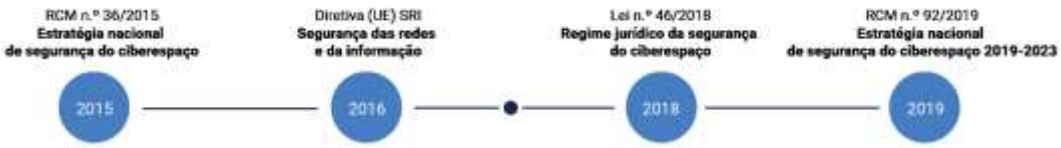

Figura 4.1 – Cronologia da Legislação de Cibersegurança (CNCS, 2021)

5 | Conclusões

Atualmente as sociedades contemporâneas confrontam-se com novos riscos e ameaças decorrentes da utilização das novas tecnologias de informação e comunicação que construiram um ambiente cada vez mais híbrido, onde o físico e o digital possuem fronteiras difusas.

As novas ameaças são não são presenciais mas têm a capacidade de ameaçar a confidencialidade, integridade e disponibilidade dos sistemas de informação e da informação que as pessoas ou organizações conservam no ciberespaço.

Neste relatório fez-se uma análise geral à estrutura de segurança do ciberespaço e à legislação produzida na área de segurança nos últimos anos com o objetivo de informar, sensibilizar e conscencializar as pessoas, mas em particular as entidades públicas para estas ameaças e para a necessidade de se adotar medidas que reduzam os riscos do ciberespaço.

Lisboa, LNEC, maio de 2023

VISTO	AUTORIA
O Conselho Diretivo	
	
Laura Caldeira	João Palha Fernandes
Presidente do LNEC	Investigador Auxiliar

Referências bibliográficas

AGÊNCIA LUSA, 2022 – **Ciberataques: cronologia de outros ataques em Portugal além da Vodafone**, CNN Portugal, 2022-02-08, Disponível em: https://cnnportugal.iol.pt/mario-vaz/ataque-informatico/vodafone-e-a-mais-recente-vitima-em-seis-anos-de-ciberataques/20500208/62028bd00cf21847f0a9ddfa.

CNCS, 2021 – **Quadro Nacional de Referência para a Cibersegurança**

Decreto-Lei 69/2014 de 9 de maio, 2014 – **Criação do Centro Nacional de Cibersegurança como unidade do GNS**, Diário da República, 1ª Série, 89, 2712 a 2719. Lisboa: Presidência do Conselho de Ministros.

Decreto-Lei 184/2014 de 29 de dezembro, 2014 – **Lei Orgânica do Estado-Maior General das Forças Armadas**, Diário da República, 1ª Série, 250, 6382 a 6397, Lisboa: Ministério da Defesa Nacional.

Decreto-Lei 81/2016 de 28 de novembro, 2016 – **Criação da Unidade Nacional do Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) como unidade da Polícia Judiciária**, Diário da República, 1ª Série, 228, 4215 a 4217, Lisboa: Ministério da Justiça.

Decreto-Lei 65/2021 de 30 de julho, 2021 – **Regulamenta o Regime Jurídico da Segurança do Ciberespaço**, Diário da República, 1ª Série, 147, 8 a 21. Lisboa: Presidência do Conselho de Ministros.

Diretiva (UE) 2016/1148 de 6 de julho, 2016 – **Segurança das Redes e Informação**, Jornal Oficial da União Europeia, L 194/1 a L 194/30, Bruxelas, Bélgica: Parlamento Europeu e do Conselho.

GOODIN, Dan, 2022 – **Vodafone Portugal struggles to restore service following cyberattack**, Ars Technica, 2022-02-09, Disponível em: https://arstechnica.com/information-technology/2022/02/vodafone-portugal-struggles-to-restore-service-following-cyberattack/.

INE, 2022a – **Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Famílias em 2022**, INE.

INE, 2022b – **Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas em 2022**, INE.

IT SECURITY, 2022 – **Hospital Garcia de Orta alvo de ciberataque**, IT Security, 2022-04-26, Disponível em: https://www.itsecurity.pt/news/news/hospital-garcia-de-orta-alvo-de-ciberataque.

Lei 46/2018 de 13 de agosto, 2018 – **Regime Jurídico da Segurança do Ciberespaço,** Diário da República, 1ª Série, 155, 4031 a 4037, Lisboa: Ministério da Justiça.

REDE NACIONAL CSIRT, 2023 – Objetivos da Rede Nacional CSIRT, Disponível em: https://www.redecsirt.pt/#objetivos.

Regulamento 183/202, 2022 – **Comunicações entre as entidades e o CNCS**, Diário da República, 2ª série, 36, 34 a 39. Lisboa: Gabinete Nacional de Segurança.

Resolução do Conselho de Ministros 36/2015 de 12 de junho, 2015 – **Estratégia Nacional de Segurança do Ciberespaço**, Diário da República, 1ª Série, 113, 3738 a 3742. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros 92/2019 de 5 de junho, 2019 – **Estratégia Nacional de Segurança do Ciberespaço**, Diário da República, 1ª Série, 108, 2888 a 2895. Lisboa: Presidência do Conselho de Ministros.

SECURITY MAGAZINE, 2021 – **Portugal tem 46 Computer Security Incident Response Teams (CSIRT)**, Security Magazine, 2021-05-20, Disponível em: https://www.securitymagazine.pt/2021/05/20/portugal-tem-46-computer-security-incident-response-teamscsirt/.

SECURITY MAGAZINE, 2022 – **Programa Krítica do SIS já realizou 487 acções e reuniões de trabalho**, Security Magazine, 2022-03-30, Disponível em: https://www.securitymagazine.pt/2022/03/30/programa-kritica-do-sis-ja-realizou-487-accoes-e-reunioes-de-trabalho/.

SISTEMA DE SEGURANÇA INTERNA. 2023 – Relatório Anual de Segurança Interna 2022, Disponível em: https://www.portugal.gov.pt/pt/gc23/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2022-.

www.lnec.pt

AV DO BRASIL 101 • 1700-066 LISBOA • PORTUGAL
tel. (+351) 21 844 30 00
lnec@lnec.pt **www.lnec.pt**