Trindade, Rui Emanuel Cedovim Fernandes dos Anjos

A importância de boas práticas de cibersegurança no contexto empresarial : políticas de inovação da União Europeia, aprendizagem e concretização

Metadados

Data de Publicação 2023

Resumo In our rapidly changing world, we are more interconnected than ever before thanks to remarkable advances in technology. According to estimates by the International Data Corporation, released by the European Commission, the number of Internet of Things (IoT) devices is expected to reach 41 billion by 2025. However, this interconnectivity, although advantageous for improving our productivity, communication and quality of life in general, also exposes us to cyber risks and the threat, a...

Num mundo em rápida evolução graças aos notáveis avanços da tecnologia, encontramo-nos mais interligados do que nunca. Segundo estimativas da International Data Corporation, divulgadas pela Comissão Europeia, é esperado que em 2025 o número de dispositivos Internet of Things (IoT) seja aproximadamente de 41 mil milhões. Porém, esta interconectividade, apesar de vantajosa por melhorar a nossa produtividade, comunicação e qualidade de vida em geral, também nos expõe a riscos cibernéticos...

Palavras Chave Direito, Cibersegurança - Medidas preventivas, Cibersegurança - Boas práticas - Empresas, Cibersegurança - Políticas europeias

Tipo masterThesis

Revisão de Pares Não

Coleções [ULP-FD] Dissertações

UNIVERSIDADE LUSÍADA DO PORTO

Boas práticas de cibersegurança no contexto empresarial: políticas de inovação da União Europeia, aprendizagem e concretização

Rui Emanuel Cedovim Fernandes dos Anjos Trindade

Dissertação para obtenção do Grau de Mestre

Porto, agosto de 2023

UNIVERSIDADE LUSÍADA DO PORTO

Boas práticas de cibersegurança no contexto empresarial: políticas de inovação da União Europeia, aprendizagem e concretização

Rui Emanuel Cedovim Fernandes dos Anjos Trindade

Dissertação para obtenção do Grau de Mestre

Sob orientação de

Professor Doutor Alberto Francisco Ribeiro de Almeida

Porto, agosto de 2023

Agradecimentos

À Universidade Lusíada, o meu profundo agradecimento por proporcionar o ambiente académico propício ao meu crescimento intelectual e pela disponibilização dos recursos necessários para levar a cabo esta investigação.

Ao meu orientador da tese, Professor Doutor Alberto Ribeiro de Almeida, quero expressar a minha sincera gratidão pela sua orientação experiente, paciência e incentivo ao longo de todo o processo. As suas valiosas sugestões e orientações moldaram significativamente o meu trabalho e enriqueceram o meu conhecimento.

À minha família, o meu pilar inabalável, agradeço pelo apoio constante e encorajamento que me deram ao longo desta jornada. Cada palavra de incentivo e gesto de carinho foi fundamental para o meu sucesso.

Deixo também os meus agradecimentos meus amigos e colegas de trabalho pelo apoio que recebi.

Agradeço em especial à Valentina pelo seu apoio constante e motivação que me proporcionou, dando-me forças nos momentos mais desafiantes.

A todos vós, o meu mais profundo obrigado por terem feito parte desta jornada e por terem contribuído para o meu crescimento académico e pessoal.

Índice

Índice de Figuras

Resumo

Num mundo em rápida evolução graças aos notáveis avanços da tecnologia, encontramo-nos mais interligados do que nunca.

Segundo estimativas da *International Data Corporation*, divulgadas pela Comissão Europeia, é esperado que em 2025 o número de dispositivos *Internet of Things (*IoT) seja aproximadamente de 41 mil milhões. Porém, esta interconectividade, apesar de vantajosa por melhorar a nossa produtividade, comunicação e qualidade de vida em geral, também nos expõe a riscos cibernéticos e a ameaças, sempre presentes no espaço digital.

Deste modo, surge a necessidade premente de uma maior consciencialização para as boas práticas de cibersegurança de forma a não cair em armadilhas ardilosamente criadas por cibercriminosos para explorar vulnerabilidades e obter acesso não autorizado a informações confidenciais, tais como credenciais de acesso, informações pessoais e empresariais, dados financeiros, propriedade intelectual entre outros.

Tendo em consideração este risco e a dimensão que pode assumir, é essencial que os indivíduos, as organizações e os governos dêem prioridade à cibersegurança para se protegerem contra estas ameaças cada vez mais frequentes e sofisticadas.

Nesta senda, o objectivo desta dissertação, é trazer à luz alguns dos principais riscos cibernéticos a que indivíduos, empresas, infraestruturas críticas, e, até a administração pública se encontram sujeitos. Nomeadamente, qual o impacto, a nível de danos económicos, legais, operacionais ou mesmo reputacionais de um ciberataque; quais são algumas das medidas de mitigação que as empresas podem adotar para minimizar a ocorrência ou o impacto de um ciberataque. Por fim, analisar a conjetura atual do panorama empresarial privado português e europeu, bem como, os principais desafios relacionados com a transformação digital, nomeadamente, no plano da cibersegurança.

Palavras-chave:

Cibersegurança, Cultura de Cibersegurança, Sensibilização para a cibersegurança, Segurança da Informação, Resposta a incidentes, Prevenção, Ciberameaças.

Abstract

In our rapidly changing world, we are more interconnected than ever before thanks to remarkable advances in technology.

According to estimates by the International Data Corporation, released by the European Commission, the number of Internet of Things (IoT) devices is expected to reach 41 billion by 2025. However, this interconnectivity, although advantageous for improving our productivity, communication and quality of life in general, also exposes us to cyber risks and the threat, always present in the digital space.

Hence, the pressing need for greater awareness of good cybersecurity practices so as not to fall into traps cunningly created by cybercriminals to exploit vulnerabilities and gain unauthorized access to confidential information such as: access credentials, personal and corporate information, financial data, intellectual property and others.

In this regard, the aim of this dissertation is to bring to light some of the main cyber risks to which individuals, companies, critical infrastructures and even the public administration are exposed. What are the damage impacts of a cyber-attack regarding economic, legal, operational or even reputational domains. What are some mitigation measures that companies can adopt to minimize the occurrence or impact of a cyber-attack. And, finally, to analyze the current situation of the Portuguese and European private corporate landscape, assessing the main challenges related to digital transformation, particularly, in terms of cybersecurity.

Keywords:

Cybersecurity, Cybersecurity Culture, Cybersecurity Awareness, Information Security, Incident Response, Prevention, Cyber threats.

Abreviaturas, siglas e acrónimos

AED	Agência Europeia de Defesa
ANCC	Autoridade Nacional de Certificação da Cibersegurança
Art.	Artigo
BEC	Business Email Compromise
CISO	Chief Information Security Officer
CNCS	Centro Nacional de Cibersegurança
CNCSeg	Antiga definição para o centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
CSIRT	Computer Security Incident Response Team
DDoS	Negação de Serviço Distribuída
RCE	Relativa à resiliência das entidades críticas
DNS	Domain Name System
DL	Decreto-Lei
EC QNRCS	Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança
EC3	Centro Europeu da Cibercriminalidade da Europol
ECCC	Centro Europeu de Competências
ENISA	Agência da União Europeia para a Cibersegurança
ENSC	Estratégia Nacional de Segurança do Ciberespaço
UE	União Europeia
CyCLONe	Rede de Organizações Cibernéticas de Ligação de Crise da EU
EUCS	Estratégia da UE para a Cibersegurança um ciberespaço aberto, seguro e protegido.
IoT	Internet of Things
ITU	International Communication Union
N.º	Número
PME	Pequena e Média Empresa

QNCC	Quadro Nacional de Cibersegurança
QNRCS	Quadro Nacional de Referência para a Cibersegurança
RGPD	Regulamento Geral de Proteção de Dados
RT	Responsável pelo Tratamento de Dados
SEAE	Serviço Europeu para a Ação Externa
SOC	Security Operations Centres
SQL	Structured Query Language
TIC	Tecnologias da informação e comunicação
TJUE	Tribunal de Justiça da União Europeia
WEF	World Economic Forum

Introdução

Na era digital e das informações na qual vivemos, as preocupações em relação às ameaças cibernéticas estão cada vez mais presentes. A evolução tecnológica e a interconectividade generalizada de dispositivos, máquinas e sistemas têm proporcionado benefícios significativos, mas também aumentaram os riscos associados à segurança do ciberespaço.

O ciberespaço, definido pelo glossário do Centro Nacional de Cibersegurança como um "*ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação*"[1], desafia diariamente iniciativas e acordos internacionais para a sua regulamentação e para o combate a ameaças cibernéticas. Além disso, o ciberespaço alberga uma ampla gama de atores, como hackers e crackers, grupos criminosos organizados, agências de inteligência e ativistas, o que torna ainda mais desafiador o estabelecimento de uma governança eficaz e o equilíbrio entre a segurança e a liberdade no ciberespaço.

O primeiro tratado internacional sobre cibercriminalidade, definido na Convenção do Conselho da Europa sobre o Cibercrime de 2001 - a Convenção de Budapeste - define as infrações relacionadas com a cibercriminalidade e prevê uma série de poderes e procedimentos para investigar este fenómeno, com vista a estabelecer normas que asseguram a cooperação internacional no combate a crimes cibernéticos. Contudo, ainda não foi conseguido superar alguns dos desafios, em termos de jurisdição, identificação dos responsáveis e velocidade das comunicações digitais, o que pode dificultar a aplicação das leis e a responsabilização dos infratores.

Desde então, diversos esforços a nível nacional e internacionais estão a ser levados a cabo para fortalecer a cibersegurança, combater o cibercrime e estabelecer princípios e normas para a governança do ciberespaço. A esta luz, a cooperação entre governos, organizações internacionais, setor privado e sociedade civil, é fundamental para enfrentar os desafios que se impõem para promover um ambiente digital mais seguro e confiável. Assim, considera-se fundamental contribuir para a consciencialização dos cidadãos, empresas e mesmo dos sistemas governamentais, para o tema da cibersegurança, objetivando a promoção da sensibilização de práticas de proteção pessoal e segurança

[1] CNCS (2022). "Glossário". https://www.cncs.gov.pt/pt/glossario/

corporativa, com vista à mitigação de riscos de incidentes de cibersegurança e ao fortalecimento generalizado da segurança do ciberespaço.

Para a elaboração da presente dissertação, foi considerada a informação mais recente sobre o panorama da cibersegurança, especialmente na Europa e em Portugal, nomeadamente, instituições públicas portuguesas, como o Centro Nacional de Cibersegurança ou a Comissão Nacional de Proteção de Dados, instituições públicas Europeias, como a Comissão Europeia ou a Agência da União Europeia para a Cibersegurança. Foram ainda considerados documentos provenientes de consultoras, organizações privadas e empresas tecnológicas de renome internacional, como a *Marsh*, *Microsoft* ou o *World Economic Forum*, e demais fontes literárias disponíveis tanto nos acervos impressos quanto nos digitais em bases de dados como *Elsevier*, *SciELO* e *Google Scholar*.

Porquanto, o capítulo I, será dedicado ao enquadramento legal e a um exercício de retrospetiva sobre os avanços a nível de legislação e regulamentação do ciberespaço.

O capítulo II, é dedicado aos problemas, desafios e ameaças relacionados com a cibersegurança, tais como, os tipos de ciberataques e as vulnerabilidades mais comuns.

No capítulo III, são exploradas as principais motivações dos cibercriminosos que levam a ataques cibernéticos, identificando-se também os diversos fatores que impulsionam as suas ações.

O capítulo IV apresenta algumas das boas práticas de cibersegurança que as empresas devem levar a cabo, são considerados alguns exemplos de grandes empresas portuguesas, partilhando uma reflexão sobre a conjuntura atual das empresas portuguesas e europeias e da abordagem à cibersegurança.

No capítulo V, é abordada a relação entre a cibersegurança e a proteção de dados, na medida em que uma das principais consequências decorrentes de um ciberataque bem-sucedido são as violações de dados. Apesar de serem dois temas indissociáveis, nem sempre são considerados quando se ouve falar que determinada empresa sofreu um ciberataque, não obstante, o impacto considerável que uma contraordenação em matéria de proteção de dados pessoais poderá causar numa organização.

O último ponto, é reservado para a conclusão da dissertação, onde se encontram as considerações finais sobre o presente estudo, com sugestões de aspetos a melhorar no futuro, nomeadamente, a forma como a cibersegurança deve ser percecionada por todos, cidadãos, empresas e estado, e qual o papel da cibersegurança nos anos que advêm.

CAPÍTULO 1 - Origem e Evolução

1. Cibersegurança na União Europeia

O ano de 2013 foi marcante para a cibersegurança no quadro da União Europeia (UE)[2], com a publicação da *Cybersecurity Strategy of the European Union, An Open, Safe and Secure Cyberspace*[3], ou, em português, Estratégia da UE para a Cibersegurança: um ciberespaço aberto, seguro e protegido (EUEC). A EUEC teve como principais princípios subjacentes à sua criação o reforço da segurança e da resiliência das redes e sistemas digitais da Europa, bem como a proteção dos direitos e liberdades dos cidadãos no ciberespaço.

A EUEC foi desenvolvida em resposta à crescente ameaça de ataques cibernéticos e à crescente dependência da das economias e das sociedades europeias, em relação às tecnologias digitais.[4] Com isso, a UE reconheceu que um ciberespaço seguro e resiliente é essencial para o crescimento e competitividade da economia da UE, bem como, para a proteção dos dados pessoais, privacidade e direitos fundamentais dos cidadãos.

A EUEC foi implementada com o objetivo de alcançar as seguintes metas[5]:

- Reforçar a capacidade da UE para prevenir, detetar e responder a ameaças e incidentes de cibersegurança;
- Reforçar a segurança e a resiliência das redes e sistemas digitais, incluindo infraestruturas críticas e serviços essenciais;
- Promover um mercado único digital seguro e de confiança, incluindo através do desenvolvimento de normas e certificação de cibersegurança;
- Apoiar o desenvolvimento de uma forte indústria de cibersegurança, incluindo através da criação de um ambiente empresarial de apoio e do desenvolvimento de novas tecnologias e soluções; e,

[2] Cavelty, M., 2018b. "*Europe´s cyber-power. European Politics and Society*", 19(3), pp. 304-320. https://doi.org/10.1080/23745118.2018.1430718

[3] Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, Join/2013/01 Final, Document 52013JC0001, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

[4] Christou, G., 2018. "*The collective securitisation of cyberspace in the European Union*". West European Politics, 42(2), Routledge, pp. 278-301.

[5] Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, Join/2013/01 Final, Document 52013JC0001, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

- Aumentar a consciência e compreensão da segurança cibernética entre os cidadãos, empresas e autoridades públicas.

Apesar da sua importância, a criação da EUEC não considerou alguns pontos importantes que tiveram, e ainda têm, um efeito negativo que impede a plena concretização da estratégia Europeia de Cibersegurança. Esses pontos prendem-se com a falta de uma visão coletiva na medida em que, a falta de um plano concreto para todos os países da UE faz com que cada país desenvolva as suas estratégias e a sua conceptualização de cibersegurança. [6]

Também não foram considerados alguns aspetos relacionados a questões financeiras e de recursos dos diversos países membros da EU.[7] Enquanto países mais ricos da zona Euro têm um poder de investimento superior, outros países ficam para trás no desenvolvimento.[8] Perante esta realidade, para que a Estratégia tivesse sucesso seria necessário que todos os países possuíssem a mesma preparação, maturidade e recursos – isto é claramente necessário, dadas as enormes somas que concorrentes como a China, Índia e EUA investem nas suas indústrias de TI e na investigação[9]. Não acontecendo, o plano revelou-se fragmentado por toda a Europa, debilitando seriamente a sua força, eficácia e eficiência.

1.1 Diretiva (UE) 2016/1148 de 6 de Julho de 2016 - Diretiva NISD

Em resposta aos obstáculos relatados à concretização da Estratégia da UE para a Cibersegurança, o Parlamento Europeu e o Conselho da Europa aprovaram, em 2016, a Diretiva (UE) 2016/1148 de 6 de Julho de 2016[10]. A *Network and Information Security Directive* (NISD), em português, Segurança das Redes e da Informação (SRI), foi a primeira legislação a nível da União Europeia sobre cibersegurança, evidenciando a evolução para uma postura mais madura, assertiva e regulativa por parte da UE nesta matéria. [11]

[6] Bendiek, A. et al. (Novembro, 2017) «*The EU's Revised Cybersecurity Strategy Half-Hearted Progress on Far-Reaching Challenges*» https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf
[7] Christou, G., 2018, op. cit pp. 278-301
[8] Bendiek, A. et al. (Novembro, 2017), op. cit
[9] Ibidem.

[11] A base jurídica da Diretiva é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia, cujo objetivo é o estabelecimento e o funcionamento do mercado interno através do reforço das medidas de aproximação das normas nacionais.

Esta Diretiva estabeleceu um conjunto de medidas obrigatórias destinadas a prevenir e a diminuir o impacto de incidentes de cibersegurança, tendo como o principal objetivo aumentar a segurança e a resiliência das redes e sistemas digitais ao introduzir requisitos mínimos de segurança para empresas públicas e privadas operadoras de infraestruturas críticas. Ainda, impôs a obrigatoriedade de reporte de incidentes de cibersegurança.

Esta peça de legislação da UE entrou em vigor em Maio de 2018[12] e foi a ponta da lança da estratégia da cibersegurança para a EU. A NISD estabelece os requisitos mínimos de segurança para redes e sistemas digitais em toda a UE e aplica-se a uma série de operadores dos sectores público e privado, incluindo fornecedores de infraestruturas críticas, fornecedores de serviços digitais, e organismos públicos[13].

Com a entrada em vigor desta diretiva, foi dado um passo muito significativo no sentido de aumentar a ciber-resiliência na União Europeia. Assim, esta revelou-se um instrumento essencial, que despertou a atenção e a conscientização das pessoas e dos governos para uma abordagem institucional e regulamentar para a cibersegurança, "abrindo as portas a uma mudança significativa de mentalidades"[14].

Outro passo muito importante dado por esta diretiva foi a atribuição de competências de fiscalização, controlo e monitorização da aplicação das posições da Diretiva à Agência da União Europeia para a Cibersegurança (ENISA). A ENISA é o centro de especialização da UE em matéria de cibersegurança, com o papel especial de facilitar a cooperação e partilha de informação entre os Estados-Membros da UE e o sector privado, detendo ainda "competências especializadas de aconselhamento e da

[12] Tendo em conta os prazos iminentes para a sua transposição para a legislação nacional (até 9 de Maio de 2018) e para a identificação dos operadores de serviços essenciais (até 9 de Novembro de 2018), a Comissão adotou, em 13 de Setembro de 2017, uma comunicação destinada a apoiar os Estados-Membros nos seus esforços para aplicar a diretiva de forma rápida e coerente em toda a UE. Introduziu um conjunto de ferramentas de interpretação da Diretiva NISD que fornece informações aos Estados-Membros sobre as melhores práticas relacionadas com a aplicação da Diretiva, bem como esclarecimentos sobre algumas das suas disposições. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: *Making the most of NIS – towards the effective implementation of Directive (UE) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*" COM/2017/0476 final, disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476

[13] Artigo 1º da diretiva NISD

[14] Expressão constante no considerando 2 da NISD 2, sucessora da NISD, 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, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1690926026132, Documento 32022L2555

facilitação do intercâmbio de boas práticas. Em particular, na aplicação da presente diretiva (NISD)[15]".

Graças a esta iniciativa legislativa, foi possível começar a desenvolver "uma abordagem global a nível da União, que abranja os requisitos mínimos comuns de desenvolvimento de capacidades e de planificação, o intercâmbio de informações, a cooperação e os requisitos comuns de segurança para os operadores de serviços essenciais e para os prestadores de serviços digitais[16]", não obstante, a possibilidade dos operadores de serviços essenciais e os prestadores de serviços digitais terem a possibilidade de adotar medidas de segurança mais rigorosas que aquelas previstas na NISD.

Cumpre ainda referir, que foi através desta diretiva que foram criados o Grupo de Cooperação NISD, artigo 11º da NISD, e a rede de equipas de resposta a incidentes de segurança informática (CSIRT), artigo 9º da NISD, para assegurar o intercâmbio de informações sobre cibersegurança e a cooperação em incidentes de cibersegurança específicos.

Aposta esta análise, é possível verificar que a EUEC e a NISD estão intimamente relacionadas e são iniciativas complementares. A EUEC fornece a visão global e os objetivos para melhorar a cibersegurança na UE, enquanto que a Diretiva fornece o quadro legal e medidas específicas para alcançar alguns desses objetivos.

Segundo o Tribunal de Justiça da UE no seu acórdão no processo C-58/08 Vodafone e outros[17], o recurso ao artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), [18] justifica-se quando existem diferenças entre as regras nacionais que têm um efeito direto no funcionamento do mercado interno.

Igualmente, o Tribunal considerou que as medidas de aproximação abrangidas pelo artigo 114.º do TFUE se destinam a deixar uma margem de apreciação, em função do contexto geral e das circunstâncias específicas da matéria a harmonizar, quanto ao método de aproximação mais adequado para alcançar o resultado pretendido.

Neste caso em específico, a NISD eliminaria os obstáculos e melhoraria o estabelecimento e o funcionamento do mercado interno para as entidades abrangidas em

[15] Considerando 36 da Diretiva NISD1.
[16] Quesito 6 do preambulo da NISD
[17] Tribunal de Justiça da União Europeia (TJUE). ECLI:EU:C:2010:321 disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=79665&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=541615
[18] Versão consolidada do Tratado sobre o Funcionamento da União Europeia (2016) C 202/47, disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF

matéria de segurança das redes e dos sistemas de informação, estabelecendo regras claras de aplicação geral sobre o âmbito de aplicação da NIDS, harmonizando as regras aplicáveis no domínio da gestão dos riscos de cibersegurança e da comunicação de incidentes.[19]

Este enquadramento jurídico afigura-se essencial, uma vez que as atuais disparidades neste domínio a nível legislativo, de supervisão, nacional e da UE constituem obstáculos ao mercado interno, e dado que as entidades que exercem actividades transfronteiriças se vêem confrontadas com requisitos regulamentares e/ou a sua aplicação diferentes e eventualmente sobreposta, em detrimento do exercício das suas liberdades de estabelecimento e de prestação de serviços. A existência de regras diferentes tem também um impacto negativo nas condições de concorrência no mercado interno quando se trata de entidades do mesmo tipo em diferentes Estados-Membros.

1.2 A Agência da União Europeia para a Cibersegurança

Com vista a promover a ciber-resiliência, combater a cibercriminalidade e fomentar a ciberdiplomacia e a ciberdefesa, a Agência da União Europeia para a Cibersegurança (ENISA), localizada na Grécia,[20] coopera com os países e organismos da UE e contribui para a antecipação, intervenção e resposta a futuros desafios relacionados com a cibersegurança.

A ENISA foi fundada pelo Regulamento (CE) n.º 460/2004 ("Regulamento ENISA")[21], enquanto o seu atual quadro regulamentar consiste no Regulamento (UE) n.º 2019/881[22]. Desde 2004, a ENISA tem contribuído ativamente para garantir um elevado nível de segurança das redes e da informação dentro da UE. A missão da ENISA é a "de contribuir para a consecução dos objetivos de garantir um nível elevado e eficaz de segurança das redes e da informação na União e de desenvolver uma cultura de segurança

[19] EU MONITOR - *Explanatory Memorandum to COM (2020)823 - Measures for a high common level of cybersecurity across the Union*, disponível em https://www.eumonitor.eu/9353000/1/j4nvhdfdk3hydzq_j9vvik7m1c3gyxp/vlenlgffo5zv

[20] ENISA (2022, Maio). ENISA Mandate and Regulatory Framework. https://www.enisa.europa.eu/about-enisa/regulatory-framework

[21] Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência da União Europeia para a Cibersegurança (Texto relevante para efeitos do EEE), , disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32004R0460, Documento 32004R0460

[22] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança), disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32019R0881, Documento 32019R0881

das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas".[23]

Em 2019 foi implementado um novo regulamento sobre a ENISA, que revoga o Regulamento (UE) n.º 526/2013, com vista a reforçar as suas capacidades e competências de modo a alcançar a resiliência da cibersegurança e melhor apoiar os Estados-Membros, empresas, instituições, órgãos e organismos da EU.

Algumas das contribuições da ENISA para a segurança das redes e da informação inclui, entre outras, a emissão de recomendações, o apoio à elaboração de políticas, bem como o trabalho prático, através do qual a ENISA colabora diretamente com as equipas operacionais em toda a UE.

Parte da estratégia da ENISA passa por seguir as seguintes prioridades: (a) antecipar e apoiar a Europa a enfrentar os desafios emergentes da segurança das redes e da informação, (b) promover a segurança das redes e da informação como uma prioridade política da UE, (c) apoiar a Europa na manutenção das capacidades NISD de ponta, (d) fomentar a Comunidade NISD europeia emergente, e (e) reforçar o impacto da ENISA.[24] Ao mesmo tempo, a ENISA assiste ativamente as autoridades competentes, nomeando o seu representante no Grupo de Cooperação e fornecendo o secretariado na rede CSIRT.

1.3 A Diretiva (UE) 2016/1148 de 6 de Julho de 2016 e a Agência da União Europeia para a Cibersegurança

No que diz respeito à Diretiva NISD em particular, o papel da ENISA na implementação das suas disposições está praticamente integrado no seu texto. O considerando 36 refere que a ENISA deve prestar assistência aos Estados-Membros e à Comissão, fornecendo conhecimentos especializados, enquanto tanto os Estados-Membros como a Comissão devem poder consultar a ENISA. Além disso, o considerando 38 refere a responsabilidade da ENISA de prestar assistência ao Grupo de Cooperação e de participar na elaboração de orientações. Por último, de acordo com o considerando 69, a Comissão deve consultar a ENISA ao adotar atos de execução.

Na prática, e no que diz respeito aos prestadores de serviços digitais, a ENISA publicou um relatório, *Technical Guidelines for the implementation of minimum security*

[23] Considerando 14 da Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança).
[24] European Court of Auditors. (2019), "*Challenges to effective EU cybersecurity policy*", disponível em https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

measures for Digital Service Providers (2017)[25], para auxiliar os Estados-Membros nos seus esforços para fornecer uma abordagem comum relativamente às medidas mínimas de segurança para os prestadores de serviços digitais. O escopo do relatório é definir objetivos de segurança de base comuns para os prestadores de serviços digitais, descrever diferentes níveis de sofisticação na implementação dos objetivos de segurança, bem como mapear os objetivos de segurança em relação a normas industriais, quadros nacionais e sistemas de certificação bem conhecidos.

Além disso, a ENISA publicou outro conjunto de diretrizes para descrever melhor o processo de notificação de incidentes demandado aos fornecedores de serviços digitais, *Incident notification for DSPs in the contexto of the NIS Directive*[26], em conformidade com o artigo 16º da Diretiva NISD. O seu objetivo, tal como declarado no ponto 1.1 do guia supramencionado é o de "desenvolver um conjunto de diretrizes para todas as partes interessadas (autoridades a nível da UE, públicas ou privadas), destinadas a apoiar a implementação da Diretiva NIS requisitos relativos à notificação obrigatória de incidentes".

As diretrizes emanadas pela ENISA contribuem significativamente para a elaboração e clarificação das noções incluídas no texto da Diretiva, tais como o conceito de "incidentes" que são abrangidos pela obrigação de notificação, o termo "impacto substancial", bem como os "parâmetros" que devem ser tidos em conta na determinação do impacto de um incidente de cibersegurança, uma vez que estes estão incluídos no n.º 4 do artigo 16º da Diretiva NISD (número de utilizadores, duração do incidente, distribuição geográfica, extensão da perturbação e extensão do impacto nas atividades económicas e sociais).

2. A evolução da cibersegurança

Desde a primeira estratégia a nível europeu em matéria de cibersegurança, chamada a "*Estratégia da UE para a Cibersegurança: um ciberespaço aberto, seguro e protegido* (EUCS)" em 2013, o panorama global e europeu mudou consideravelmente, de

[25] ENISA. (Fevereiro, 2017), "*Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*", disponível em https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

[26] ENISA. (Fevereiro, 2017) "*Incident notification for DSPs in the contexto of the NIS Directive*", disponível em https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/

maneira que se tornou imperativo adaptar às novas tendências, ameaças e avanços tecnológicos, este impulso resultou numa nova e mais sofisticada estratégia de cibersegurança da UE 2020-2025.[27]

A nova estratégia de cibersegurança propôs, entre outras coisas, a revisão da Directiva NISD, a adoção de uma nova diretiva relativa à resiliência das entidades críticas (RCE)[28] no campo da segurança física contra ameaças dinâmicas desde terrorismo a catástrofes naturais[29], uma rede de Centros de Operações de Segurança (SOC)[30] e novas medidas para reforçar o conjunto de instrumentos de ciberdiplomacia da UE. Estas medidas estão em consonância com as prioridades da Comissão de preparar a Europa para a era digital e de construir uma economia preparada para o futuro que corresponda às necessidades dos cidadãos, um dos principais desafios identificados foi o de garantir a segurança da tecnologia 5G.

Relativamente à Diretiva NISD de 2016, com a evolução galopante da tecnologia e do cenário de ameaças, determinou-se necessário que o âmbito de aplicação deveria ser atualizado e alargado para fazer face aos riscos atuais e desafios futuros. Além disso, a transposição e execução da Diretiva revelaram falhas inerentes a determinadas disposições, dada a delimitação pouco clara do âmbito de aplicação da Diretiva.

Por sua vez, a pandemia veio sublinhar a importância de preparar a UE para a década digital, bem como a necessidade de melhorar continuamente a ciber-resiliência, em especial para os operadores de serviços essenciais como os cuidados de saúde e a energia.

Já a nível de financiamento e investimento das iniciativas da UE em matéria de cibersegurança pode dizer-se que ocorreu um aumento muito significativo para o período de 2021-2027 através de uma combinação de instrumentos como o Programa Europa

[27] Comissão Europeia. "*New EU Cybersecurity Strategy and new rules to make physical and digital crital entities more resilient.".* (Dezembro 2020). Documento IP/20/2391, disponível em https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

[28] 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, disponível para consulta em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2557&qid=1687729156275, Document 32022L2557

[29] Ibidem.

[30] Comissão Europeia (Novembro, 2022). "*Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres".*, disponível em https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-launches-first-phase-deployment-european-infrastructure-cross-border-security

Digital[31], o Horizonte Europa[32], o Fundo Europeu de Defesa e o Mecanismo de Recuperação e Resiliência da UE[33]. O objetivo da UE é atingir até 4,5 mil milhões de euros de investimento combinado. Nomeadamente para as PME, no âmbito do recém-criado Centro de Competências em Cibersegurança e da Rede de Centros de Coordenação.[34][35]

2.1 Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de Dezembro de 2022 – Diretiva NIS2

A NIS 2, Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de Dezembro de 2022, (doravante designada NIS2)[36] que entrou em vigor em 2023, dá seguimento e altera a diretiva sobre segurança das redes e da informação da NISD, adotada em 2016.

Esta renovada diretiva foi introduzida com o objetivo de modernizar o quadro legal Europeu existente para acompanhar o aumento da digitalização e a evolução do fenómeno de ameaças de cibersegurança e eliminar as divergências profundas nesta matéria entre as estratégias e recursos dos Estados-Membros.[37]

Algumas das principais mudanças passaram pelo alargamento do âmbito das regras de cibersegurança abrangendo agora novos sectores e entidades, e estabelecendo regras e mecanismos concretos desenhados para melhorar a capacidade de resistência e os meios de resposta a incidentes de cibersegurança de entidades públicas e privadas, assim como autoridades competentes.

---

[31] Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de Abril de 2021 que cria o Programa Europa Digital, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32021R0694, Documento 32021R0694.

[32] Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho de 28 de Abril de 2021 que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação, que define as suas regras de participação e difusão, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021R0695, Documento 32021R0695.

[33] Regulamento (UE) 2021/241 do Parlamento Europeu e do Conselho de 12 de Fevereiro de 2021 que cria o Mecanismo de Recuperação e Resiliência, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32021R024, Documento 32021R0241.

[34] EU-LEX. "Centro e rede europeus de competências em cibersegurança" (Julho 2021), disponível em https://eur-lex.europa.eu/PT/legal-content/summary/european-cybersecurity-network-and-competence-centre.html

[35] 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 e a Rede de Centros Nacionais de Coordenação, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32021R0887, Documento 32021R0887.

[36] NISD 2

[37] Considerando 4 Diretiva NISD 2

A Diretiva NISD 2 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, prevê medidas legais para aumentar o nível global de cibersegurança na UE, assegurando:

- A preparação dos Estados Membros, exigindo-lhes que estejam devidamente equipados. Por exemplo, com uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT) e uma autoridade nacional competente em matéria de redes e sistemas de informação[38];
- Cooperação entre todos os Estados Membros, criando um Grupo de Cooperação[39] para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados Membros.
- O desenvolvimento de uma cultura de segurança nas infraestruturas críticas para a economia e sociedade e que dependem fortemente das TIC, como o são os sectores da energia, transportes, setor bancário, infraestruturas do mercado financeiro, saúde, água potável, águas residuais, infraestruturas digitais, gestão de serviços TIC (entre empresas), administração pública, espaço.[40]

Um ponto importante que foi acrescentado com esta Diretiva foi em relação às Infraestruturas digitais, designadamente aos fornecedores de pontos de troca de tráfego; prestadores de serviços de DNS[41], excluindo operadores de servidores de nomes raiz; registos de nomes de TLD[42]; Prestadores de serviço de mercados online; Prestadores de serviços de computação em nuvem; prestadores de serviços de centro de dados; fornecedores de redes de distribuição de conteúdos; prestadores de serviços de confiança; fornecedores de redes públicas de comunicações eletrónicas; e, prestadores de serviços

[38] Em Portugal a autoridade nacional competente em matéria de redes e sistemas de informação é o Centro Nacional de Cibersegurança.

[39] Este Grupo foi criado com o objetivo de apoiar e assegurar a cooperação e o intercâmbio de informações entre os Estados-Membros, de acordo com o consignado no artigo 14º da NISD e funciona de acordo com DECISÃO DE EXECUÇÃO (UE) 2017/179 DA COMISSÃO de 1 de Fevereiro de 2017 que estabelece as disposições processuais necessárias para o funcionamento do grupo de cooperação ao abrigo do artigo 11.o, n.o 5, da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32017D0179, Documento 32017D0179.

[40] ANEXO I da Diretiva NISD 2, "Setores de importância Crítica".

[41] OVHcloud. "*O Domain Name System (DNS), ou sistema de nome de domínio, é o serviço que assegura a ligação entre o domínio e o endereço IP de um servidor. Permite ao utilizador não ter de conhecer o endereço de IP exato de um site para poder aceder ao mesmo.",* mais informações disponíveis em https://www.ovhcloud.com/pt/domains/dns-server/

[42] Google. *"As bases de dados de registo funcionam como grossistas para o registo de domínios. Os domínios utilizam extensões de nomes de domínios, também conhecidas como domínios de nível superior ou TLDs. Por exemplo, a empresa Verisign gere o registo dos domínios .com e .net.*" "Bases de Dados de Registo"

de comunicações eletrónicas acessíveis ao público, que agora também são considerados setores de importância crítica o que por sua vez determina que adotem medidas de gestão dos riscos de cibersegurança, conforme consignado no artigo 21º da Diretiva NIS2.

3. Em Portugal

Um dos primeiros grandes passos de Portugal em matéria de Cibersegurança foi em 2009 com a aprovação da Lei nº 109/2009, de 15 de Setembro, Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, destinada a aumentar a segurança dos cidadãos no ciberespaço[43] e a conferir instrumentos de intervenção às entidades que combatem o cibercrime. Este diploma estabelece as disposições penais materiais, substantivas, e processuais, adjetivas.

As normas substantivas, tipificam as condutas suscetíveis de enquadrar a prática de crimes vulgarmente chamados "informáticos", artigo 3º a 8º do diploma. As normas adjetivas, estabelecem as medidas processuais específicas para a recolha de prova em suporte eletrónico, artigo 12º a 19º do mesmo diploma.[44][45]

Em suma, esta lei inovadora, para além de introduzir um conjunto de disposições relativas à cooperação internacional penal e um catálogo de crimes informáticos, a Lei do Cibercrime veio introduzir "*um verdadeiro sistema processual de prova digital*"[46], porquanto das medidas processuais que aí se encerram de aplicação geral, quer nos

---

[43] Para a definição de ciberespaço deverá ser tida em consideração a definição avançada pelo CNCS na Estratégia Nacional de Segurança do Ciberespaço 2019-2023, "*Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação",* disponível em *https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf*.

[44] Artigo 11.º Âmbito de aplicação das disposições processuais
1 - Com excepção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:
a) Previstos na presente lei;
b) Cometidos por meio de um sistema informático; ou
c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.
2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.

[45] Na esteira do pensamento de Pedro Venâncio, "*a consagração de disposições processuais relativas à preservação, revelação, apresentação, pesquisa e apreensão de dados informáticos (previstas nos artigos 12.º a 17.º da LC* (Lei do Cibercrime) *impunha-se não só como um imperativo de direito internacional, face à ratificação da Convenção sobre Cibercrime, mas, acima de tudo, como uma inevitabilidade civilizacional.",* in VENÂNCIO, Pedro Dias, "As Disposições Processuais Relativas a Dados Informáticos na Lei do Cibercrime", JusJornal, N.º 1183, 24 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer.

[46] CORREIA, João Conde (2014, Julho-Set), "Prova Digital: as leis que temos e a lei que devíamos ter", Revista do Ministério Público, n.º 139, https://rmp.smmp.pt/indice-do-no-139/, pp.29 a 59".

processos relativos a crimes expressamente previstos nesse diploma quer nos processos relativos a crimes cometidos por meio de um sistema informático, como ainda em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (artigo 11.º, n.º 2 da Lei do Cibercrime). [47]

Em 2012, o Governo de Portugal, através da Resolução do Conselho de Ministros n.º 12/2012, 7 de Fevereiro, considerou essencial a consolidação da Estratégia Nacional de Segurança da Informação (ENSI), determinando a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNCSeg). Foi através da Resolução do Conselho de Ministros n.º 42/2012, de 13 de Abril, na dependência do Primeiro-Ministro, que se constituiu a Comissão Instaladora do CNCSeg, com a missão de definir as medidas e os instrumentos necessários à criação, instalação e operacionalização do CNCSeg. A responsabilidade pela constituição da comissão instaladora do novo centro foi coordenada pelo Gabinete Nacional de Segurança, com a colaboração de todas as entidades relevantes em razão da matéria. Contudo, apenas em 2014, foram definidas as características, competências e regime de funcionamento do Centro Nacional de Cibersegurança, por via do Decreto-Lei n.º 69/2014, de 9 de Maio, no qual ficou definido que seria a principal missão do CNCSeg seria "*contribuir para que Portugal use o ciberespaço de uma forma segura e as suas competências não prejudicam as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço, nomeadamente no que respeita a infraestruturas críticas e integridade das redes e serviços, sendo exercidas em coordenação com estas entidades.*".[48] , tendo ficado definido que funcionaria no âmbito do Gabinete Nacional de Segurança (GNS).

Posteriormente, em 2013, o Governo de Portugal lança uma revisão do Conceito Estratégico de Defesa Nacional, através da Resolução do Conselho de Ministros n.º 19/2013, de 5 de Abril, esta resolução resulta da necessidade de acompanhar o desenvolvimento da sociedade moderna da informação e do papel do Estado, enquanto entidade soberana e reguladora, de forma a garantir um ciberespaço confiável e seguro,

[47] Ministério Público (2019, Abril) "Meios de Obtenção de Prova e Medidas Cautelares e de Polícia", Coleção formação, Centro de Estudos Judiciários.
[48] Decreto-Lei n.º 69/2014, de 9 de Maio, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança, https://diariodarepublica.pt/dr/detalhe/decreto-lei/69-2014-25343754

combatendo e reprimindo as ameaças de Ciberterrorismo e da Cibercriminalidade[49], definindo como linhas de ação prioritárias:

- Garantia a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN);
- Definir uma Estratégia Nacional de Cibersegurança;
- Montar a estrutura responsável pela Cibersegurança, através da criação dos órgãos técnicos necessários;
- Sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e levantar a capacidade de Ciberdefesa nacional".

Em 28 Outubro de 2013, é publicado o Despacho n.º 13692/2013, denominado como "Orientação política para a Ciberdefesa", esta orientação visou introduzir as linhas orientadoras dos esforços a desenvolver ao nível da Defesa Nacional para o levantamento da capacidade nacional de Ciberdefesa. Esta Orientação apresenta como objetivos "*garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques*", "*assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional*" e, por último, "*contribuir de forma cooperativa para a cibersegurança nacional*" [50], tendo ficado determinado que o Centro de Ciberdefesa, fique na dependência do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA).

Em 2015, foi dado mais um passo importante em matéria de segurança do ciberespaço, com a aprovação da primeira Estratégia Nacional de Segurança do Ciberespaço (doravante designada ENSC). Introduzida pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de Junho[51], foi um marco importante do país, demostrando uma postura atenta e atual aos problemas modernos decorrentes da evolução tecnológica. Ficou definido que se atualizaria dali a três anos.

---

[49] "*A cibercriminalidade, porquanto os Ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna*" (Resolução do Conselho de Ministros n.º 19/2013, de 5 de Abril, p.22.
"No domínio da cibercriminalidade, impõe-se uma avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados". (Conceito Estratégico de Defesa Nacional, Resolução do Conselho de Ministros n.º 19/2013, de 5 de Abril, p.22)

[50] Despacho do Ministro da Defesa n.º 13692/2013, de 28 de Outubro*." Orientação para a política de Ciberdefesa Nacional"* https://files.dre.pt/2s/2013/10/208000000/3197631979.pdf

[51] Ibidem.

Esta estratégia surgiu com o objetivo de "*aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas*"[52]. Para tanto, foram elencados 4 objetivos basilares desta estratégia, "*(a) Promover uma utilização consciente, livre, segura e eficiente do ciberespaço; Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; c) Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; d) Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação*" que se desdobram em seis eixos de intervenção, destinados a reforçar o potencial estratégico nacional no ciberespaço, nomeadamente através: (i) assegurar a segurança do Ciberespaço; (ii) Combater o Cibercrime; (iii) Proteção do ciberespaço e das infraestruturas nacionais[53]; (iv) promoção da educação, sensibilização e prevenção; (v) potenciar a investigação e desenvolvimento; e, (vi) fomento da cooperação nacional, europeia e internacional neste domínio.

Como principais inovações desta estratégia, destacam-se os mecanismos de reporte de incidentes ao Centro Nacional de Cibersegurança por parte de órgãos públicos e de operadores de infraestruturas críticas.

Mais tarde, em 2017, com vista a alcançar uma melhor organização foi constituído o Conselho Superior de Segurança do Ciberespaço, através da Resolução do Conselho de Ministros n.º 115/2017, de 24 de Agosto, ao qual foi atribuída a missão de rever e propor a Nova Estratégia Nacional de Segurança do Ciberespaço (ENSC), e também de funcionar como órgão de coordenação político-estratégica para a segurança do ciberespaço, isto é, tendo um papel de interlocutor em matérias de cibersegurança com o membro designado do Governo.

Outro ano volvido, ocorreu a transposição da Diretiva (UE) 2016/1148 - do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, (Diretiva NIS) relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União - a entrada em vigor da Lei n.º 46/2018, de 13 de Agosto, veio estabelecer o regime jurídico da segurança do ciberespaço.

---

[52] Resolução do Conselho de Ministros n.º 36/2015, de 12 de Junho, disponível em https://dre.pt/dre/detalhe/resolucao-conselho-ministros/36-2015-67468089

[53] O caminho para o reforço da proteção das infraestruturas já havia começado a ser traçado por via do o Decreto-Lei n.º 62/2011, de 9 de Maio, peça de legislação que transpôs para o ordenamento jurídico português a Diretiva de Proteção de Infraestruturas Críticas (PIC), no qual foram estabelecidos os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social nos setores da energia e dos transportes

Efetivamente, foi com a Lei n.º 46/2018, de 13 de Agosto, que ficaram consolidadas as bases jurídicas e institucionais em matéria de cibersegurança relativamente às entidades da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais, bem como dos prestadores de serviços digitais e, ainda, a quaisquer entidades que utilizem redes e sistemas de informação, nomeadamente no âmbito da notificação voluntária de incidentes.

Ademais, a Lei n.º 46/2018, de 13 de Agosto, desempenhou um papel relevante, pois introduziu os conceitos e noções sobre o ciberespaço, por exemplo, veio esclarecer o que se entende por "incidente", o que são "estruturas críticas", quem são "prestadores de serviços digitais", entre outros, assim como as responsabilidades e obrigações a que cada um está adstrito.

Neste diploma foi também consagrada a competência do Governo para elaborar e aprovar a Estratégia Nacional de Segurança do Ciberespaço, estratégia essa que *"define o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional."* [54]

Foi também agrupado, pela primeira vez, toda a estrutura de segurança do Ciberespaço em Portugal, que compreende o Conselho Superior de Segurança do Ciberespaço, Centro Nacional de Cibersegurança CNCS enquanto Autoridade Nacional de Cibersegurança que funciona no âmbito do Gabinete Nacional de Segurança – GNSE a Equipa de Resposta a Incidentes de Segurança Informática CERT.PT[55]

Em 2019 é implementada a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, revogando a sua primeira versão. Esta estratégia surgiu da necessidade de atualização da ENSC 2015, que embora pioneira, em contexto nacional, apresentava-se limitada quando confrontada com nas necessidades emergentes do desenvolvimento tecnológico dos últimos anos.

Desenvolvida pelo Conselho Superior de Segurança do Ciberespaço, esta nova estratégia apresenta-se como um "*instrumento estruturante para a capacitação nacional neste âmbito, definindo o enquadramento, os objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço, de acordo com o interesse nacional*."[56]

---

[54] Artigo 4º n.º 1 da Lei 46/2018, de 13 de Agosto.

55 O CERT.PT é a equipa de resposta a incidentes de Segurança Informática Nacional. Funciona no Centro de Nacional de Cibersegurança, consultar artigos 8º e 9º da Lei n.º 46/2018, de 13 de Agosto.

[56] Resolução do Conselho de Ministros n.º 92/2019, de 5 de Junho, aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962

Nesta linha de ação, a ENSC 2019-2023 foi desenvolvida com base em 3 eixos estratégicos bem definidos:

- Garantir Recursos
- Promover a Inovação
- Maximizar a Resiliência

Os impactos e necessidades associados a cada um destes objetivos estratégicos permitem definir uma direção global e específica, que se desdobra em seis eixos de intervenção, que enformam linhas de ação concretas destinadas a desenvolver o potencial estratégico nacional do ciberespaço.

Figura 1 - Eixos de intervenção da ENSC 2019-2023

Fonte: *CNCS (Junho, 2019). "Estratégia Nacional de Segurança do Ciberespaço 2019-2023", https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf*

Para executar esta Estratégia, foi desenvolvido um Plano de Ação[57], cuja execução está atribuída ao Centro Nacional de Cibersegurança enquanto Autoridade Nacional de Cibersegurança, que tem como função o acompanhamento e avaliação da execução da ENSC 2019-2023, e que, ademais, deverá ser articulado com a Estratégia Nacional de

[57] As atividades do plano de ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 poderão ser consultadas no site do Centro Nacional de Cibersegurança, https://www.cncs.gov.pt/docs/ensc2019-2023-pa-2019-2020-2021-execucao2020-mai21.pdf

Combate ao Terrorismo, designadamente contemplando medidas de proteção contra as respetivas ameaças à segurança do ciberespaço, com a Estratégia TIC 2020 - Estratégia para a Transformação Digital na Administração Pública, bem como com a Estratégia de Inovação Tecnológica e Empresarial para Portugal 2018-2030.

Quando contraposta com a primeira versão, existem pontos positivos que se destacam, desde logo, a definição concreta de um Plano de Ação. Ao tomar esta iniciativa remove-se a ambiguidade anteriormente existente, originada pela generalidade e grande abrangência das medidas e atividades definidas pela ENSC 1, substituindo-se por instruções e medidas claras a adotar.

A ENSC 2019-2023, apesar do passo importante que constituiu, na análise envolvente elaborada, são apontados alguns desafios e vulnerabilidades conjeturais relacionadas essencialmente com a "*insuficiente maturidade digital"* para atender às necessidades de segurança, tanto no setor público como no privado, e uma "*fraca cultura de cibersegurança e de consciência das responsabilidades individuais*". A par desta realidade, é também dado conta da "*dificuldade de capacitação, manutenção e captação de recursos humanos e financeiros que permitam o acompanhamento da rápida evolução tecnológica e o concomitante impacto na vida em sociedade representa uma vulnerabilidade nacional adicional, que exige um forte investimento para ser colmatada, modelos de colaboração inovadores em rede e um incremento da investigação, desenvolvimento e inovação.".*

A partir deste diagnóstico, constante na própria ENSC 2019-2023, encontram-se contextualizados e identificados os principais desafios atuais e reais inerentes à implementação desta Estratégia, que apesar de dinâmica e inovadora, terá de superar estas condicionantes através de uma coordenação e cooperação estratégica entre entidades nacionais e europeias.

4. Centro Nacional de Cibersegurança

A história do Centro Nacional de Cibersegurança começa em 2012 através da Resolução do Conselho de Ministros n.º 42/2012, de 13 de Abril[58], que visou constituir a Comissão Instaladora do Centro Nacional de Cibersegurança com o objetivo de proceder à criação, instalação e operacionalização de um Centro Nacional de Cibersegurança. Mais tarde a 6 de Outubro de 2014, é desenvolvido o mesmo, dentro do Gabinete Nacional de Cibersegurança, através do Decreto-Lei n.º 69/2014, de 9 de Maio[59], com a missão de

[58] Resolução do Conselho de Ministros 42/2012, de 13 de Abril, disponível em https://dre.pt/dre/detalhe/resolucao-conselho-ministros/42-2012-552560

[59] O Decreto-Lei 69/2014, de 09 de Maio, Procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de Janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança, disponível em

"(…) *contribuir para que o país o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais*."[60]

Foi em 2017, através da instituição do Decreto-Lei n.º 136/2017, de 6 de Novembro que o CNSC adquire a sua designação atual.

Posteriormente, com a publicação da Lei n.º 46/2018, de 13 de Agosto (Regime Jurídico da Segurança do Ciberespaço), que transpõe a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, é atribuída a CNCS a competência de Autoridade nacional de Cibersegurança e ao CERT.PT a de ponto de contato único internacional para reação a ciberincidentes, conforme os artigos 7º e 9º da referida Lei.

Atualmente o Centro Nacional de Cibersegurança atua como coordenador operacional e autoridade nacional especialista em matérias de cibersegurança junto das entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, o CNCS transporta também a sua ação para a sociedade em geral[61].

O Centro Nacional de Cibersegurança é ainda a Autoridade Nacional de Certificação da Cibersegurança (ANCC), conforme estabelece o art.º 20 do Decreto-Lei n.º 65/2021, de 30 de Julho (Regulamenta o Regime Jurídico Da Segurança Do Ciberespaço) em aplicação do art.º 58 do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de Abril de 2019.[62]

---

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=2100&pagina=1&ficha=1. Ademais, cumpre reforçar que, o CNCS funciona no âmbito do GNS, e segue as atribuições consignadas na Lei orgânica do GNS/CNCS, segundo Decreto-Lei n.º 3/2012, de 16 de Janeiro (Lei Orgânica do GNS), na sua redação atual, disponível https://www.cncs.gov.pt/docs/dl-136-2017-alt-lo-gns.pdf

[60] Artigo 2º, n.º 2 do Decreto-Lei n.º 69/2014, de 09 de Maio.

[61] Centro Nacional de CiberSegurança. Missão do CNCS. Disponível em https://www.cncs.gov.pt/pt/sobre-nos/#trabalhar

[62] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019R0881

5. Decreto-Lei n.º 65/2021, de 30 de Julho

Mais recentemente, foi introduzido o Decreto-Lei n.º 65/2021, de 30 de Julho, que veio regulamentar o Regime Jurídico de Segurança do Ciberespaço, definindo, entre outros, os requisitos de segurança das redes e sistemas de informação, as regras para a notificação de incidentes e as obrigações em matéria de certificação da Cibersegurança, em execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019.[63]

De entre as obrigações impostas pelo referido Decreto-Lei deve-se destacar[64]:

- A necessidade das entidades abrangidas indicarem um ponto de contacto permanente, de modo a assegurar os fluxos de informação de nível operacional e técnico com o CNCS;
- A necessidade das entidades abrangidas desenvolverem um plano de segurança;
- A ser elaborado um relatório anual até ao último dia útil do mês de Janeiro.
- Deve ser elaborado um inventário de todos os ativos essenciais e posteriormente enviado, juntamente com o relatório anual, para o Centro Nacional de Cibersegurança;
- Reforçar obrigações de análise de risco de implementação e medidas para cumprimento dos requisitos de segurança;
- Definidas as regras para a notificação de incidentes;
- Consagra o Centro Nacional de Cibersegurança como a Autoridade Nacional de Certificação da Cibersegurança;

Quanto ao ponto de contacto permanente cumpre referir que tem função assegurar os fluxos de informação de nível operacional e técnico com o Centro nacional de Cibersegurança.

[63] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança), https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019R0881, Documento 32019R0881

[64] O Regulamento n.º 183/2022, que aborda a Instrução Técnica relacionada com a comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes, encontra-se publicado no Diário da República, 2.ª série, número 36, de 21 de Fevereiro de 2022, disponível em https://diariodarepublica.pt/dr/detalhe/regulamento/183-2022-179325870.

O ponto de contacto pode ser composto por uma ou mais pessoas, devendo dispor de meios de comunicação principais e alternativos e, acima de tudo, apresentar disponibilidade 24 horas por dia, 7 dias por semana.

Ademais, as entidades devem designar um responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, de acordo com os artigos 4.º e 5.º do referido Decreto-Lei.

5.1 Plano de segurança

Trata-se de um novo elemento introduzido pelo artigo 7º do aludido Decreto-Lei, que impõe às entidades abrangidas a necessidade de elaborar e manter atualizado um plano de segurança com medidas organizativas e de segurança no âmbito da cibersegurança.

Será de realçar que o plano não se trata de um documento estático, vai evoluindo à medida que as tecnologias e os recursos vão avançando, de maneira que deve ser regularmente monitorizado e revisto pelos responsáveis para estar a par de todos os cenários e potenciais ameaças de segurança.

Quanto ao conteúdo do plano, deve conter[65]:

- A política de segurança, incluindo a descrição das medidas organizativas e a formação de recursos humanos;
- A descrição de todas as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes;
- A identificação do responsável de segurança;
- A identificação do ponto de contacto permanente.

5.2 Relatório anual e inventário de ativos

Quanto à elaboração do relatório anual e ao Inventário de Ativos, o Decreto-Lei enumera alguns requisitos específicos que devem ser cumpridos: ambos os documentos devem ser enviados, anualmente, para o Centro Nacional de Cibersegurança até ao último dia útil do mês de Janeiro do ano civil seguinte aos quais os mesmos se reportam, nos termos do artigo 8º n.º2 e 6º n.º 3, al. b) do Decreto-Lei.

[65] Cfr. Artigo 7º n.º 1 do Decreto-Lei n.º 65/2021.

Relativamente ao relatório anual, impõe-se ainda outros requisitos formais para a sua elaboração, tais como[66]:

a) Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação;
b) Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes;
c) Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre:
    i. Número de utilizadores afetados pela perturbação do serviço;
    ii. Duração dos incidentes;
    iii. Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
d) Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação;
e) Problemas identificados e medidas implementadas na sequência dos incidentes;
f) Qualquer outra informação relevante.

5.3 Análise de risco e implementação e medidas para cumprimento dos requisitos de segurança

No artigo 10º deste Decreto Lei, é referido um ponto muito importante que cumpre salientar, e tem que ver com a análise dos riscos e a implementação dos requisitos de segurança.

Reforçar a análise de risco e a implementação de sistemas de segurança é de cabal importância no mundo atual, onde a informação digital é um bem inestimável para indivíduos, organizações e nações.

Uma vez que os ataques cibernéticos, violação de dados e outras formas de cibercriminalidade estão a aumentar, revela-se crítico adotar medidas proactivas que auxiliem na proteção da informação e dos sistemas sensíveis.

A análise de risco envolve a identificação de potenciais riscos e vulnerabilidades num sistema e a avaliação da probabilidade e do impacto potencial desses riscos. Esta informação pode então ser utilizada para implementar medidas de segurança apropriadas

[66] Artigo 8.º n.º 1 do Decreto-Lei 65/2021

para mitigar ou eliminar esses riscos. O reforço da análise de risco auxilia as organizações a identificar potenciais ameaças e vulnerabilidades antes de serem exploradas, permitindo-lhes tomar medidas preventivas para salvaguardar os seus sistemas.

Para o efeito, o Decreto-Lei, elenca uma série de indicadores que devem ser monitorizados[67], tais como:

- Uma análise de risco para cada ativo com base na identificação das ameaças, internas ou externas, intencionais ou não intencionais abrangendo: i) Falha de sistema; ii) Fenómeno natural; iii) Erro humano; iv) Ataque malicioso; v) Falha no fornecimento de bens ou serviços por terceiro, conforme o artigo 10º n.º3, al. a) do aludido Decreto de Lei;

- A realização de uma análise de riscos que tenha em consideração: a) O histórico de situações extraordinárias ocorridas; b) O histórico de incidentes e, em especial, de incidentes com impacto relevante; c) O número de utilizadores afetados pelos incidentes; d) A duração dos incidentes; e) A distribuição geográfica, no que se refere à zona afetada pelos incidentes; f) As dependências intersectoriais para efeitos da prestação dos serviços, incluindo os constantes do anexo ao Regime Jurídico da Segurança do Ciberespaço e o setor das comunicações eletrónicas, nos termos do artigo 10º n.º4, al. a) do aludido Decreto-Lei.

- Devendo, também, ser considerada a avaliação integrada dos riscos para a segurança das redes e dos sistemas de informação a nível nacional, europeu e internacional, publicada anualmente ou notificada às entidades pelo CNCS, constante nos relatórios publicados no Observatório de Cibersegurança.

A implementação de um sistema de segurança permite gerir a incerteza da organização em relação à segurança da informação. Este sistema, envolve a criação de controlos técnicos, administrativos e físicos para proteger sistemas e dados contra acesso, utilização, divulgação, perturbação, modificação, ou destruição não autorizados. Estes sistemas de segurança são essenciais para prevenir ataques informáticos e violações de dados, e para assegurar a confidencialidade, integridade e disponibilidade de informações sensíveis.

Por fim, uma vez que a gestão de risco se trata de um processo contínuo que requer monitorização e revisão regulares para assegurar que os riscos estão efetivamente identificados, avaliados e geridos, deverá ser revisto pelo menos uma vez por ano ou

[67] Não obstante, o CNCS poder emitir instruções técnicas com vista a uma harmonização da matriz de risco a adotar pelas entidades. – artigo 10º n.º 10 do Decreto-Lei.

aquando da notificação pelo CNCS de um risco com elevada probabilidade de ocorrência (artigo 10º n.º 1, al. a).

Como tal, deverá estar disponível para consulta o conjunto documental referente à preparação, execução e a apresentação dos resultados da análise dos riscos (artigo 10º n.º 2).

5.4 Notificação de incidentes

Este é um dos principais pontos deste Decreto-Lei, uma vez que a notificação de incidentes de cibersegurança não se trata apenas de uma obrigação legal, mas também de um momento importante para assegurar que todas as medidas são tomadas com vista a conter os danos e a salvaguardar os dados pessoais perdidos, a privacidade das pessoas afetadas e a integridade das informações ilegalmente acedidas.

Na sequência de um incidente de cibersegurança, uma das principais preocupações que uma organização terá de enfrentar é se deve informar as entidades competentes sobre o incidente, uma vez que esta decisão poderá ter implicações jurídicas e empresariais significativas para a organização.

Existem casos em que a notificação é obrigatória, ocorrendo algum incidente com impacto relevante ou substancial, as entidades em causa deverão notificar o Centro Nacional de Cibersegurança.[68]

Fora dos casos obrigatórios, a resposta dependerá intrinsecamente dos factos e circunstâncias vigentes, abrangendo tanto o incidente em questão como o enquadramento empresarial circundante. Nesse sentido, será imperativo recorrer à orientação de consultores especializados, peritos externos e os principais intervenientes da empresa, a fim de delinear uma abordagem integral e fundamentada.

Não obstante, não deveram ser descuradas as vantagens em efetuar tal comunicação. Uma empresa que tenha implementado um processo de resposta atempada e de recuperação eficaz, ao efetuar a notificação de uma violação da cibersegurança permite que as entidades competentes respondam rapidamente e tomem as medidas adequadas para mitigar os danos causados pela violação. Isto pode incluir a realização de

[68] Para atender ao critério de impacto relevante ou substancial deve ser tido em consideração os parâmetros indicados no artigo 15 º da Lei 46/2018: "4 - A fim de determinar a relevância do impacto de um incidente são tidos em conta, designadamente, os seguintes parâmetros: a) O número de utilizadores afetados; b) A duração do incidente; c) A distribuição geográfica, no que se refere à zona afetada pelo incidente."

uma investigação, a identificação da causa raiz da violação, e a implementação de medidas para prevenir a ocorrência de incidentes semelhantes no futuro.

Mais, não é invulgar que as polícias de investigação tenham vindo a seguir uma ameaça cibernética durante algum tempo e tenham adquirido informação significativa sobre as actividades e táticas de grupos específicos de cibercriminosos.[69]

Ao coordenar a ação com as autoridades de investigação, uma organização pode receber informações valiosas, não públicas, sobre ameaças que a possam ajudar a identificar as vulnerabilidades exploradas numa violação, a intenção potencial por detrás do incidente e a fonte do ataque. Tais informações podem ajudar determinantemente na resposta ao incidente da organização e nos esforços de remediação a longo prazo.[70][71]

Por fim, a necessidade de manter a confiança e a credibilidade, também são um elemento preponderante a considerar nestas situações. A notificação imediata de uma violação da cibersegurança pode ajudar a manter a confiança e credibilidade junto dos clientes, partes interessadas, e do público. Demonstrando um compromisso de transparência e responsabilidade, e pode ajudar a minimizar os danos de reputação que podem resultar da violação.[72]

Quanto ao processo de notificação ao CNCS, as entidades devem efetuar 3 tipos de notificação:

a) Uma notificação inicial, deve ser enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após

[69] Numa entrevista, o diretor da Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica, Carlos Cabreiro, informou aos jornalistas que (…) A nível nacional, o número de inquéritos relacionados com cibercrime estará entre 20 mil e 22 mil. Agência Lusa (2022, Maio) "*PJ defende que precisa de metadados para investigar cibercrime*" Diário de Notícias. https://www.dnoticias.pt/2022/5/4/309372-pj-defende-que-precisa-de-metadados-para-investigar-cibercrime/#

[70] Graças a estas bases de informação recolhidas pelas policias de investigação, foi possível ao Departamento da Justiça dos EUA (DOJ) auxiliar várias empresas a recuperar os fundos perdidos em ataques de *ransomware*:
Quase um mês após o ataque de resgate do Colonial Pipeline de 2021, o DOJ e o FBI recuperaram 2,3 milhões de dólares do pedido de resgate. Office of Public Affairs. U.S. Department of Justice. (2021, Junho) "*Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside*" https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside;

[71] outro exemplo, Em Novembro de 2021, o DOJ e o FBI apreenderam 6,3 milhões de dólares de um famoso grupo russo de resgate - para além de extraditarem um arquitecto dos ataques.; mais recentemente E, em 2023, o DOJ e o FBI infiltraram-se e desmantelaram o grupo "*Hive ransomware*" e utilizaram esse acesso para fornecer chaves de descodificação a mais de 300 organizações vítimas deste ataque, evitando mais de $130 milhões de dólares em pagamentos de resgate Office of Public Affairs. U.S. Department of Justice. (2023, Janeiro)." *U.S. Department of Justice Disrupts Hive Ransomware Variant*" https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

[72] Por exemplo da Vodafone, a 7 de Fevereiro de 2022, foi alvo de ciberataque e imediatamente divulgou o sucedido. https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html

essa verificação, devendo a entidade, sem prejuízo do cumprimento deste prazo, dar prioridade à mitigação e à resolução do incidente, nos termos do artigo 13.º;

b) Uma notificação de fim, notificação de fim de impacto relevante ou substancial do incidente deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial. de impacto relevante ou substancial, nos termos do artigo 14.º;
c) Uma notificação final, a notificação final deve ser enviada no prazo de 30 dias úteis, a contar do momento em que o incidente deixou de se verificar. nos termos do artigo 15.º;

Além dos tipos de notificação a realizar, também se encontra previsto um procedimento para efetuar o envio das notificações de incidentes e de informação adicional. Este deverá ser efetuado conforme o consignado no artigo 6º do Regulamento n.º 183/2022, de 21 de Fevereiro, de acordo com o qual o envio das notificações de incidentes e de informação adicional, é realizado através do sítio na Internet do CNCS (https://www.cncs.gov.pt) na funcionalidade «Notificação de Incidentes», mediante o preenchimento do modelo de reporte estabelecido para o efeito, ou via API (*application programming interface*) disponibilizada pelo CNCS. Conferindo, ainda, a possibilidade, a título excecional, de efetuar a notificação ao CNSC por via de e-mail ou número de telefone, nas situações em que por resultado do acidente ou outro motivo de natureza técnica devidamente justificado, não seja possível submeter pelo meio supramencionado.[73]

O Regulamento n.º 183/2022[74], de 21 de Fevereiro, surge como um documento de apoio contendo as instruções técnicas relativas à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes, tendo por objectivo complementar o Decreto-Lei n.º 65/2021, de 30 de Julho, nos termos das competências que lhe são cometidas e de acordo com os poderes e funções do Centro Nacional de Cibersegurança, como Autoridade Nacional de Cibersegurança de acordo com o n.º 5 do artigo 7.º da Lei n.º 46/2018, de 13 de Agosto.

[73] Artigo 6º n.º 1 e 2 do Regulamento n.º 183/2022 de 21 de Fevereiro.
[74] Regulamento n.º 183/2022-Regulamento que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança, https://dre.pt/dre/detalhe/regulamento/183-2022-179325870

5.5 Processo de Certificação

O Decreto-Lei n.º 65/2021, estabelece também um conjunto de medidas inovadoras em matéria de certificação dos sistemas de cibersegurança, em execução do Regulamento UE 2019/881, do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, permitindo a implementação de um Quadro Nacional de Certificação da Cibersegurança (QNCC) pelo CNCS que, por via desse regulamento, passa a assumir o papel de Autoridade Nacional de Certificação da Cibersegurança (ANCC).

Nessa qualidade, o CNCS integra o Grupo Europeu para a certificação da Cibersegurança (GECC), previsto no art. 62º do Regulamento UE 2019/881.[75]

Como Autoridade Nacional de Cibersegurança o CNCS passará a assumir a responsabilidade pelas atividades de supervisão da certificação, incluindo:

a) Solicitar aos organismos de avaliação da conformidade, aos titulares de certificados de cibersegurança e aos emitentes de declarações de conformidade, as informações de que necessite para o exercício das respetivas atribuições;
b) Tomar as medidas adequadas a garantir que os organismos de avaliação da conformidade, os titulares de certificados nacionais ou europeus de cibersegurança, e os emitentes de declarações de conformidade cumprem o disposto na lei em matéria de certificação da cibersegurança;
c) Executar as demais competências estabelecidas para as autoridades de certificação da cibersegurança, designadamente as decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de Abril de 2019.

Uma vez designado como ANCC – nos termos do artigo 20º do Decreto-Lei n.º 65/2021 – o CNCS terá ainda a oportunidade de desenvolver e implementar esquemas específicos de certificação da cibersegurança relativos a produtos, serviços e processos de tecnologia de informação e comunicação, que não sejam ainda abrangidos por um esquema europeu, sempre que a especificidade do objeto da certificação o justifiquem,

[75] Artigo 62.º n.º. 1 do Grupo Europeu para a certificação da cibersegurança do Regulamento EU 2019/881 « É criado o grupo europeu para a certificação da cibersegurança (a seguir designado «GECC»)

sendo, nesta qualidade, a entidade responsável pela supervisão do cumprimento das regras estabelecidas nos esquemas nacionais.

Em todo o caso, cumpre referir que a certificação da cibersegurança é voluntária e facultativa, salvo se as autoridades europeias ou nacionais estabelecerem a sua obrigatoriedade para fins de determinado conceito específico.

5.6 Regime Sancionatório

É ainda estabelecido o regime sancionatório pela violação das disposições do Decreto-Lei em matéria de certificação.

Constitui contraordenação punível com coima de € 1.000,00 a € 3.740,98, no caso de pessoa singular, ou de € 5.000,00 a € 44.891,81, no caso de pessoa coletiva, a prática das seguintes infrações[76]:

a) A utilização de marca de certificação da cibersegurança inválida, caducada ou revogada;
b) A utilização de expressão ou grafismo que expressa ou tacitamente sugira a certificação da cibersegurança de produto, serviço ou processo que não seja certificado;
c) A omissão dolosa de informação ou a prestação de falsa informação que seja relevante para o processo de certificação da cibersegurança que se encontre em curso, nos termos definidos em cada esquema de certificação.

Às demais infrações das disposições do Decreto-Lei é aplicável o regime sancionatório previsto no Regime Jurídico da Segurança do Ciberespaço aprovado pela Lei n.º 46/2018, de 13 de Agosto.[77]

6. Quadro Nacional de Certificação de Cibersegurança

Na acessão do CNCS, o Quadro Nacional de Certificação de Cibersegurança (doravante designado por QNCC) é "designação que condensa o conceito de ecossistema nacional de certificação da cibersegurança.[78]"

[76] Artigo 21º n.º 2 do DL n.º 65/2021, de 30 de Julho.
[77] Artigo 21º n.º.1 do DL n.º 65/2021, de 30 de Julho
[78] CNCS. (2022). "Quadro Nacional de Certificação da Cibersegurança" https://www.cncs.gov.pt/pt/quadro-nacional-de-certificacao-da-ciberseguranca/

O QNCC estabelece, em Portugal, as disposições necessárias à elaboração, implementação e execução dos esquemas de certificação de cibersegurança relativos a produtos, serviços e processos de tecnologias de informação e comunicação que não sejam ainda abrangidos por um esquema europeu.

Por outras palavras, é o meio conceptual que possibilita a criação e a operação de esquemas de certificação nacionais de cibersegurança com vista a responder às necessidades nacionais nesta matéria. Estabelece o esquema de certificação, o dono dos esquemas, a entidade supervisora dos esquemas, o organismo nacional de acreditação e os organismos de certificação.[79]

O QNCC é gerido pelo CNCS uma vez que se trata da Autoridade Nacional de Certificação da Cibersegurança, contando com a cooperação de outras entidades como o Organismo Nacional de Acreditação, o Instituto Português de Acreditação, o Organismo Nacional de normalização e o Instituto Português da Qualidade, I.P, para o auxiliar na análise e verificação dos esquemas de certificação específicos quanto à sua adequação aos objetivos propostos. [80]

A certificação de cibersegurança trata-se de um processo de avaliação e verificação de que um determinado sistema, produto ou serviço que cumpre as normas e requisitos de segurança estabelecidos. Este processo é normalmente executado por terceiros e fornece uma validação da postura de cibersegurança de uma organização e ajuda a demonstrar a conformidade com os regulamentos e normas da indústria.

Por sua vez, a certificação pode auxiliar as organizações a mitigar os riscos associados às ameaças cibernéticas, melhorar o desempenho, aumentar a sua credibilidade perante os seus clientes e parceiros comerciais, proporcionando uma vantagem competitiva no mercado.

O processo de certificação envolve tipicamente a definição de requisitos de segurança, a avaliação do sistema, a remediação de fraquezas ou vulnerabilidades identificadas, a monitorização e manutenção contínuas para assegurar a conformidade contínua.

[79] Em Portugal, a entidade supervisora e o dono dos esquemas é o Centro Nacional de Cibersegurança ao abrigo das competências adquiridas pelo Decreto-Lei 65/2021, de 30 de Julho: Art.º 20.º "Autoridade Nacional de Certificação da Cibersegurança"

[80] CNCS (2022). *Quadro Nacional de Certificação da Cibersegurança* https://www.cncs.gov.pt/pt/quadro-nacional-de-certificacao-da-ciberseguranca/

6.1 Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança

Em Portugal, o Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança (EC QNRCS) foi o primeiro esquema nacional de certificação da cibersegurança a ser desenvolvido no âmbito do Quadro Nacional de Certificação Cibersegurança, e permite atestar a conformidade da implementação das medidas de cibersegurança definidas no Quadro Nacional de Referência para a Cibersegurança por parte de uma organização.

O Quadro Nacional de Referência para a Cibersegurança (QNRCS) define determinadas medidas por cada objetivo de segurança a alcançar, indicando para cada subcategoria um conjunto de recomendações para a respetiva implementação técnica e implementação processual. Porém, tendo em conta a complexidade e exigências do processo, o CNCS desenvolveu um documento com o objectivo de providenciar às organizações" um *guia de cibersegurança que sistematiza um conjunto de medidas para as problemáticas mais relevantes da atualidade nesta matéria*".[81]

Este Guia, facilita o entendimento do procedimento de auditoria e a forma de obter a certificação, uma vez que apresenta as medidas de uma forma acessível e sistematizada, permitindo às empresas que possam cumprir com os requisitos mínimos de segurança da informação recomendados.

Relativamente à Certificação EC QNRCS, esta tem por base alguns dos critérios utilizados nos esquemas europeus trazidos pelo Enquadramento Europeu de Certificação de Cibersegurança, e permite a obtenção de uma certificação que pode ser definida em 3 níveis de garantia: básico, substancial e elevado. Nessa certificação encontram-se definidas as medidas de segurança que as empresas têm de cumprir, designadamente, medidas relacionadas com a identificação, proteção, deteção, resposta e recuperação contra ameaças que coloquem em causa a segurança do ciberespaço da empresa.[82] Depois de validada, é emitido um certificado que tem a duração de 3 anos.

O ciclo de vida e processo de certificação do EC QNRCS é ilustrado na Figura 2, retirada do site do Centro Nacional de Cibersegurança.

[81] CNCS. "Quadro Nacional de Referência para a Cibersegurança". https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf
[82] Ibidem.

Figura 2 - Ciclo de vida e processo de certificação do EC QNRCS

Fonte*: CNCS (2023). "Certificação QNRCS", https://www.cncs.gov.pt/pt/certificacao-nacional/*

6.2 O Selo de Maturidade Digital

Com o objectivo de incentivar o aumento da maturidade digital das pequenas e médias empresas, uma das medidas do Plano de Ação para a Transição Digital aprovado através da RCM n.º 30/2020 de 21 de Abril, foi a criação do Selo de Maturidade Digital.[83]

No âmbito deste Plano foram criados 4 Selos de Maturidade Digital, cada um correspondente a uma área de atuação. Existem selos para a Cibersegurança, Privacidade e Proteção de Dados Pessoais, Sustentabilidade e Acessibilidade.

O método de obtenção destes Selos é semelhante ao da certificação EC QNRCS, na medida em que define uma série de requisitos técnicos que a organização tem de cumprir a nível de Cibersegurança, depois é executada uma auditoria e no final é conferido, ou não, o selo.

Este selo, pretende mitigar os riscos de cibersegurança a que as organizações estão expostas e contribuir para a prevenção e proteção da informação, assim como, aumentar o nível de confiança de clientes, fornecedores ou parceiros de negócio, na resiliência da infraestrutura digital da empresa.

Os critérios para a obtenção do Selo de Cibersegurança encontram-se consignados na Norma DNP TS 4475-1:2015.

A certificação pode ser obtida em três níveis de maturidade específicos (Bronze, Prata e Ouro), determinados com base no grau de avaliação a ser realizada.

[83] Imprensa Nacional Casa da Moeda. "Certificação de Maturidade Digital" https://selosmaturidadedigital.incm.pt/

A emissão dos selos é coordenada pela Imprensa Nacional-Casa da Moeda, sendo esta iniciativa resultado do envolvimento de diversos organismos, incluindo a Direção-Geral das Atividades Económicas, o Centro Nacional de Cibersegurança, a Comissão Nacional da Proteção de Dados e a Agência para a Modernização Administrativa.

A principal diferença entre este selo e o EC QNRCS é que este selo não se trata de uma certificação englobada no Quadro Nacional de Certificação da Cibersegurança.

6.3 Certificações na União Europeia

Na União Europeia existem vários esquemas europeus de certificação de Cibersegurança. Estes esquemas resultaram da necessidade de harmonização de certificações uma vez que uma entidade que quisesse obter uma certificação de cibersegurança e atua-se em vários países, teria que seguir tantos processos de certificação quantos os países onde deseje obter o certificado.

Assim, com vista a diminuir os custos e a burocracia envolvida, foi desenvolvido o Enquadramento Europeu de Certificação de Cibersegurança que garante que certificados de Esquemas Europeus emitidos por Autoridades Nacionais de Certificação de Cibersegurança (ANCC) sejam válidos em todos os países da UE.

A Agência da União Europeia para a Cibersegurança (ENISA) desenvolve todos os projectos de sistemas de certificação, a pedido da Comissão Europeia ou dos Estados-Membros. Para tal, a ENISA pode ser apoiada por grupos de peritos ("Ad-Hoc Working Group"), contando sempre com a colaboração da Comissão Europeia, dos países da UE, e partes interessadas relevantes.

Atualmente existem 3 esquemas Europeus:

- EUCC[84] – esquema europeu de certificação da cibersegurança baseado nos Critérios Comuns das TIC, na Common Methodology for Information Technology Security Evaluation e nos padrões correspondentes, ISO/IEC 15408 e ISO/ IEC 18045, respetivamente. – Concluído;
- EUCS – esquema europeu de certificação da cibersegurança para serviços de computação na nuvem – em elaboração;
- EU5G – esquema europeu de certificação da cibersegurança para as redes 5G – em elaboração.

[84] ENISA (2021, Maio). *Cybersecurity Certification.* https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

Cada esquema tem 3 níveis de garantia, básico, substancial e elevado, de maneira a que cada entidade possa escolher o nível de segurança adequado que pretende certificar.

CAPÍTULO 2 – Problemas, desafios e ameaças: os "ciberdesafios"

Segundo estimativas do *World Economic Forum,* no *Global Risks Report 2023*, o impacto económico global do cibercrime em 2021, foi de 6 biliões (milhão de milhões) de Dólares, tendo atingido tanto órgãos institucionais como empresas, de pequena e grande dimensão, estimando-se que alcance 10 biliões de dólares em 2025.[85]

Para colocar em perspetiva, se o valor do cibercrime fosse medido como se de um país se tratasse, então o cibercrime seria a terceira maior economia do mundo, depois dos EUA e da China.

Porém, apesar dos esforços e investimentos das empresas para diminuir os impactos destes ataques[86], é inegável a disparidade alarmante entre o custo de lançar um ataque e o custo da prevenção, investigação e reparação. Por exemplo, um ciberataque Negação de Serviço Distribuída (DDoS) pode ter um custo tão baixo quanto 15€ por mês para realizar[87], contudo as perdas sofridas pela empresa visada serão de grande vulto, podendo causar prejuízos financeiros, perdas económicas, repercussões legais e mesmo danos reputacionais irreversíveis.

Como tal, tendo em conta a quantidade crescente de dispositivos ligados à internet, segundo a estimativa do Parlamento Europeu existirão cerca de 22,3 mil milhões de dispositivos conectados à internet até 2024, e o crescente aumento de ciberataques a empresas, com cerca de 28% das PME's Europeias a ter sofrido um ataque em 2021[88], a conjetura atual e futura impõe que as empresas encarem a cibersegurança como uma pedra

---

[85] World Economic Forum (2023, Janeiro). "*2023 Global Risk Report"* disponível em https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

[86] De modo a tentar diminuir os custos das consequências decorrentes de um ciberataque, as empresas têm vindo a adotar diferentes estratégias, uma delas passa pela subscrição de seguros de cibersegurança. Segundo um relatório da Allied Market Research, a dimensão do mercado global de seguros de cibersegurança foi avaliada em 4,52 mil milhões de dólares em 2019 e prevê-se que atinja 28,60 mil milhões de dólares em 2027, crescendo a uma taxa anual de 25,2% de 2020 a 2027. Este crescimento é impulsionado pelo aumento das ameaças cibernéticas, pela crescente regulamentação cibernética, e pela crescente adopção de serviços baseados na nuvem e da Internet das Coisas (IoT). Fonte: Aarti G. (2020, Março). "*Cyber Insurance Market by Company Size (Large Companies and Small & Medium-sized Companies) and Industry Vertical (BFSI, IT & Telecom, Retail & E-commerce, Healthcare, Manufacturing, Government & Public Sector, and Others): Global Opportunity Analysis and Industry Forecast, 2019-2026*". AlliedMarketReserarch. https://www.alliedmarketresearch.com/cyber-insurance-market

[87] Europol. (2018, Abril). " World's biggest marketplace selling internet paralysing DDoS attacks taken down" https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

[88] Eurobarómetro (2022) "*Flash Eurobarómetro 496 PMEs e crime cibernético*". Disponível em: https://europa.eu/eurobarometer/surveys/detail/2280

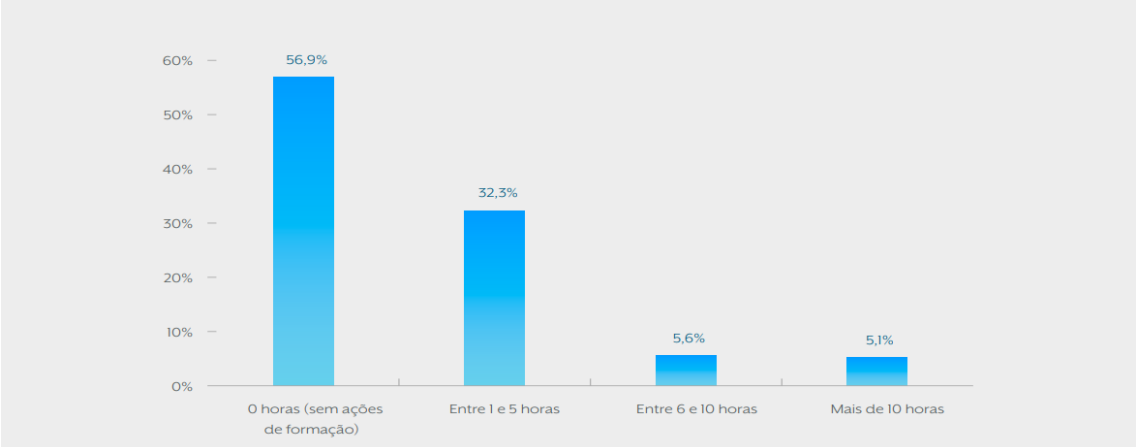
basilar, fundamental na prevenção contra as ameaças a que se encontram expostos e também como de meio consecução dos seus objetivos estratégicos.

Em Portugal, por exemplo, segundo os dados de incidentes de cibersegurança registados pelo CERT.PT, de 2019 para 2021, o número de incidentes aumentou de 754 para 1781, respetivamente, correspondendo a um aumento percentual de 136%[89]. Este cenário não é único de Portugal, mas também internacional, como tal, entidades como ENISA, Europol e WEF têm vindo a alertar para a premência de desenvolver atividades com o intuito da promoção de ações de consciencialização da cibersegurança e da luta contra o cibercrime.

Apesar de haver atualmente uma maior consciencialização por parte de indivíduos e organizações para a cibersegurança, com um empenho crescente na aquisição e disseminação das melhores práticas, a grande maioria ainda negligencia esta temática.

Num estudo levado a cabo pelo CNCS a 641 empresas nacionais, demonstra que 56,6% dos trabalhadores da empresa não têm qualquer ação de formação no âmbito da cibersegurança, 32,3% têm entre 1 e 5 horas, 5,6% têm entre 6 e 10 horas, e, somente, 5,1% das empresas oferece mais de 10horas por ano. (Figura 3).

Figura 3 - Número de horas em ações e formação e sensibilização em matérias de cibersegurança, para todas as empresas, Portugal, % de empresas



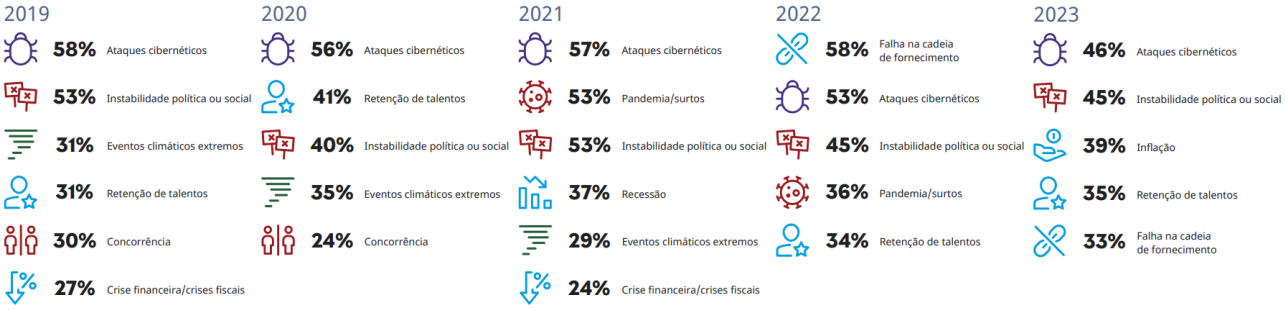
Fonte*: CNCS (Maio, 2022). "Relatório Economia 2022",* *https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf*

[89] CNCS (2022). "*Relatório Cibersegurança em Portugal –Riscos e Conflitos 2022"*, disponível em https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

Inquéritos como estes permitem-nos aferir um pouco daquela que é a realidade que se vive nas empresas, revelando, por um lado, a falta de maturidade do tema e, por outro, o grande desafio dos profissionais da área e governos dos países para apoiar e dinamizar o desenvolvimento da cibersegurança.

Estes dados revelam-se particularmente interessantes, quando contrastados com um inquérito recente realizado a 132 representantes de organizações portuguesas (do setor público e privado), dos mais variados setores de atividade, número de colaboradores, volume de vendas e participação em bolsa, levado a cabo pela corretora *Marsh*, que revela que para o ano de 2023 a nível nacional, estes representantes, colocam o risco de "ataques cibernéticos" como o risco mais esperado para o ano de 2023, situando-se em primeiro lugar, com 46%. (Fig. 4)[90].

Figura 4 - Principais riscos que a empresa vai enfrentar: evolução do top 5 de 2019-2023



Fonte: *MARSH (2023). "A Visão das Empresas Portuguesas sobre os Riscos 2023"* https://info.marsh.com/a_visao_das_empresas_portuguesas_sobre_os_riscos_2023

Apesar do risco já não ser novo e ser constantemente referenciado como um dos principais riscos em que a as empresas poderão enfrentar desde 2019, o nível de maturidade das empresas a nível de preparação para este tipo de ataques ainda se encontra a um nível reduzido no panorama global português.

[90] MARSH (2023, Abril). "*A Visão das Empresas Portuguesas sobre os Riscos 2023"* disponível para consulta em https://info.marsh.com/a_visao_das_empresas_portuguesas_sobre_os_riscos_2023

1. Cibercrime e Cibersegurança

1.1 Cibercrime

O cibercrime e a cibersegurança são dois conceitos relacionados, mas distintos no contexto da União Europeia.

Relativamente ao conceito de cibercrime, embora na literatura não exista uma definição comum para este conceito[91], segundo as duas definições mais citadas pela academia dos autores Thomas e Loader e Gordon e Ford, podemos definir este conceito como "*actividades mediadas por computador que são ilegais ou consideradas ilícitas por certas entidades e que podem ser realizadas através de redes electrónicas mundiais*"[92] ou como "*qualquer crime que seja facilitado ou cometido através de um computador, rede ou dispositivo de hardware*"[93]

Na União Europeia o conceito está em uniformizado, através da Convenção do Cibercrime[94], também conhecida como Convenção de Budapeste, identificando-se o cibercrime como uma actividade criminosa que seja cometida através da utilização de tecnologias digitais, tais como computadores, a Internet e dispositivos móveis. Esta atividade criminosa podem incluir o roubo de identidade, fraude financeira, hacking, cyberbullying, assédio online, ciberterrorismo, entre outras. Na convenção estão identificadas quatro categorias de atividades que configuram cibercrimes[95], tendo em 2003 sido acrescentada uma quinta categoria por via do Protocolo Adicional relativo à criminalização de atos de carácter racista e xenófobo cometidos através de sistemas informáticos.[96]

---

[91] Phillips, K.; Davidson, J.C.; Farr, R.R.; Burkhardt, C.; Caneppele, S.; Aiken, M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sci. 2022, 2, 379-398. https://doi.org/10.3390/forensicsci2020028

[92] Thomas, D.; Loader, B. Introduction-Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. *In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*; Thomas, D., Loader, B., Eds.; Routledge: London, UK, 2000.

[93] Gordon, S.; Ford, R. On *the Definition and Classification of Cybercrime*. J. Comput. Virol. 2006, 2, 13–20.

[94] Conselho Europeu. *Convenção do Cibercrime.* Tratado Europeu No. 185, disponível em https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 ;

[95] Ibidem, Categoria 1: Ofensas à confidencialidade, Integridade e disponibilidade de dados e sistemas informáticos (Artigo 1 a 6); Categoria 2: Ofensas relacionadas com computadores (Artigo 7 e 8); Categoria 3: Infrações Relacionadas com o conteúdo (Artigo 9); Categoria 4: Ofensas relacionadas com a violação de Direitos de autor e direitos conexos (Artigo 10).

[96] Concelho Europeu (2003). "*Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*", https://rm.coe.int/168008160f – Introduziu a Categoria 5: Actos de natureza racista e xenófoba cometidos através de sistemas informáticos (Artigo 3 a 7 do Protocolo Adicional.

Em linha com esta estratégia de combate ao cibercrime, cumpre ainda realçar o papel da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de Agosto de 2013 relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho [97] , que requer aos Estados-membros o reforço da legislação e das sanções aplicáveis ao Cibercrime. Conforme consignado no seu artigo 1º (Objeto) *"A presente diretiva estabelece regras mínimas relativas à definição das infrações penais e das sanções no domínio dos ataques contra os sistemas de informação. (...)"*

1.2 A Cibersegurança

A cibersegurança, por outro lado, refere-se à prática de proteger sistemas e redes informáticas contra acesso não autorizado, ataques ou danos.

Embora não exista uma definição normalizada e universal de cibersegurança[98], na União Europeia deverá ser considerada a definição constante no 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 tecnologias da informação e comunicação, que define a cibersegurança como o conjunto de *"atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas."*[99]

Tais atividades de proteção de ciberameaças, podem incluir medidas como: encriptação de informação, firewall's, software antivírus, sistemas de deteção de intrusão e, uma das componentes mais importantes, a própria formação e sensibilização dos utilizadores.

[97] Diretiva 2013/40/EU do Parlamento Europeu e do Concelho de 12 de Agosto de 2013 relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. Decisão 2005/222/JHA. Documento 32013L0040. Disponível em https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040

[98] Os termos "cibersegurança" e "segurança da informação" são muitas vezes utilizados indistintamente na literatura, embora existam diferenças entre os dois. Na sua obra, os autores Von Solms, R. e Van Niekerk, J. discutem que "A segurança da informação é a proteção da informação, que é um bem, contra possíveis danos resultantes de várias ameaças e vulnerabilidades. A cibersegurança, por outro lado, não é necessariamente apenas a proteção do ciberespaço em si, mas também a proteção daqueles que funcionam no ciberespaço e de quaisquer dos seus bens que possam ser atingidos através do ciberespaço." Von Solms, R. and Van Niekerk, J. (2013) From Information Security to Cyber Security. Computers & Security, p.101. https://doi.org/10.1016/j.cose.2013.04.004

[99] Artigo 2º n.º 1 do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança).

A este propósito a Comissão Europeia tem vindo a adotar uma postura muito ativa e dinâmica, desenvolvendo políticas e iniciativas para promover a cibersegurança, das quais se destaca a Estratégia de Cibersegurança da UE, que estabelece um quadro abrangente para melhorar a resiliência dos Estados Membros da UE e infraestruturas críticas contra as ameaças cibernéticas.

Para reprimir e reportar este tipo de crimes digitais, existem várias organizações como o Serviço Europeu para a ação Externa, a Europol e a Interpol, que se dedicam ao combate da cibercriminalidade e à promoção da cibersegurança.

2. Hacker e Craker

Quando se fala em cibercriminosos há que fazer uma importante distinção, que por vezes acaba por ser confundida, é a diferenciação entre um *Hacker* e um *Craker*.

O *Hacker* é uma pessoa que procura aceder a sistemas sem autorização, utilizando técnicas próprias, com o intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.[100]

Por sua vez, o *Cracker* é um *Hacker* que, ilegalmente, entra, altera, apaga ou introduz informação distinta, programas ou malware, em sistemas protegidos da Internet.[101]

Para além destes cibercriminosos se distinguirem pelo conceito, também se podem distinguir pela sua atuação, uma vez que o hacker é alguém que procura aceder a sistemas sem autorização, porém, adotando uma conduta menos lesiva; o *Cracker* adota uma conduta não ética, invadindo sistemas com interesses patrimoniais ou danosos. Ambas as condutas são puníveis por lei de acordo com o Regime Jurídico relativo a ataques contra sistemas de informação, Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime)[102]

[100] Pereira, Joel Timóteo Ramos, Compêndio Jurídico da Sociedade da Informação, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1035.
[101] Ibidem
[102] Lei n.º 109/2009 de 15 de Setembro Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, disponível em https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-128879174-128828710

3. Os Intervenientes da cibersegurança na União Europeia

No domínio da cibersegurança dentro da UE, existem diversos agentes e intervenientes que desempenham papéis fundamentais e contribuem ativamente para o desenvolvimento, a execução e aperfeiçoamento do tema.

Ao longo dos últimos anos o número de projectos de investigação financiados pela Comissão Europeia neste domínio aumentou significativamente, assim como, o nível de responsabilidade e autonomia das entidades que tutelam esta área, como por exemplo a ENISA, que ao longo dos anos tem vindo a promover e divulgar estudos pertinentes para o aperfeiçoamento de legislação e conceitos no mundo da Cibersegurança.

A Comissão Europeia, desempenha um papel fundamental nesta matéria, uma vez que se trata do órgão que estabelece e aplica políticas e regulamentos para proteger as infraestruturas digitais e garantir a segurança das actividades que acontecem no espaço, físico e digital, da União Europeia. Nessa missão, é apoiada diretamente pelas várias entidades europeias, nomeadamente a ENISA, o EC3 e a CERT-EU. O Parlamento Europeu intervém enquanto colegislador.

Para além do valioso contributo da ENISA enquanto órgão consultivo que apoia no desenvolvimento das políticas[103], no reforço de capacidades, na sensibilização e formação dos utilizadores, o Centro Europeu da Cibercriminalidade da Europol (EC3)[104], também tem produzido um trabalho muito pertinente no combate ao cibercrime, tendo como algumas das suas principais funções funcionar como ponto de convergência europeu das informações sobre a cibercriminalidade, reforçar a resposta das autoridades policiais Europeias no combate à mesma[105] e congregar conhecimentos especializados para apoiar o reforço das capacidades nos Estados-Membros.

---

[103] Considerando n.º 61 e artigo 21º e ss do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de Abril de 2019, relativo à ENISA, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881

[104] EUROPOL (Março, 2022). "*European Cybercrime Centre"* disponível em *https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3*

[105] Os laços de cooperação Internacional dentro a EU são reforçados pelas as Equipas de Investigação Conjuntas (EIC)/Joint Investigation Teams (JIT). As EIC/JIT são uma ferramenta jurídica de cooperação internacional judiciária e policial que se baseia num acordo escrito entre as autoridades competentes – tanto judiciárias (procuradores, juízes de instrução) como órgãos de polícia criminal – de dois ou mais Estados. As Equipas de Investigação Conjuntas são criadas por um período limitado e com um objetivo concreto, para realizar investigações criminais num ou mais dos Estados envolvidos, mais informação em Eurojust. *Joint Investigation Teams (2023)* https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams

No vértice da ciberdefesa, ciberdiplomacia e comunicação, o Serviço Europeu para a ação Externa (SEAE)[106] assume um lugar estratégico na medida em que alberga os centros de recolha e análise de informação das mais recentes e sofisticadas ameaças. Por sua vez, a Agência Europeia de Defesa (AED)[107] colabora em estrita cooperação com o SEAE enquanto entidade que tem por finalidade desenvolver as capacidades de ciberdefesa da UE.

Os Estados Membros são uma das peças essenciais nesta estratégia europeia, uma vez que são estes que fazem uma parte relevante de trabalho operacional como integração dos regulamentos e diretivas, a nomeação dos organismos nacionais e capacitação destes, de forma a dota-los de meios suficientes para que possam ter um papel ativo e participativo. Os Estados-Membros intervêm através do Conselho, que tem numerosos organismos de coordenação e partilha de informações (entre os quais o Grupo Horizontal das Questões do Ciberespaço).

Não deve ainda ser descurado o papel das organizações do setor privado, incluindo as empresas, os organismos de governação da Internet e também o meio académico, como parceiros que contribuem para o investimento, o desenvolvimento e execução das políticas, dado que, as empresas geram conhecimentos práticos a partir das suas experiências no desenvolvimento, implementação e gestão de soluções de cibersegurança, que podem servir como base de estudo para os investigadores e fornecer um feedback valioso sobre a eficácia das medidas de cibersegurança em cenários do mundo real.

4. As Ciberameaças

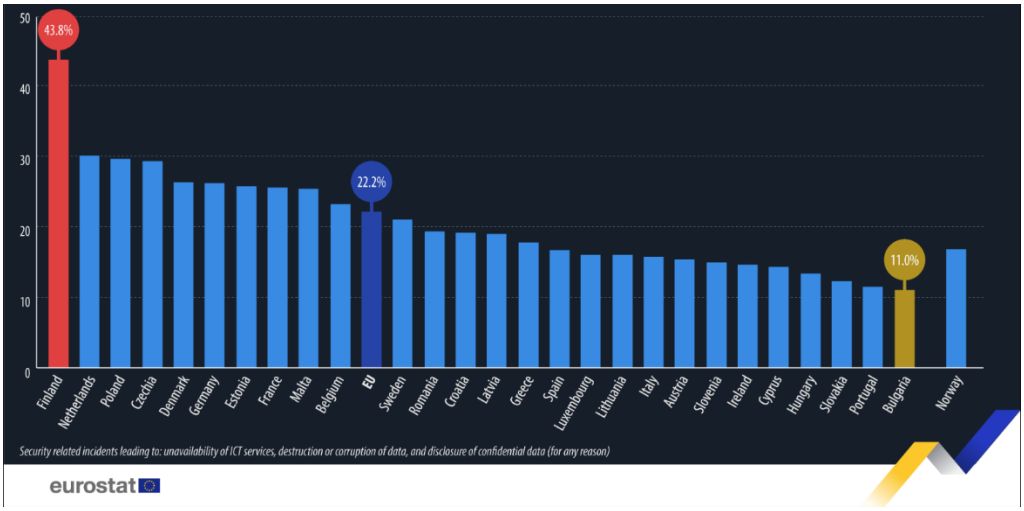
Em 2021, segundo dados da Eurostat, na UE, 22,2% das empresas (com 10 ou mais funcionários) no setor empresarial (excluindo do estudo o setor mineiro e de extração de pedra e setor financeiro) sofreram ciberataques, resultando em diferentes tipos de consequências, como indisponibilidade de serviços TIC, destruição ou corrupção de dados, divulgação de dados confidenciais, danos reputacionais, perdas financeiras, entre outros danos.

[106] Conselho da União Europeia. 2010/427/UE: Decisão do Conselho, de 26 de Julho de 2010 , que estabelece a organização e o funcionamento do Serviço Europeu para a Acção Externa, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010D0427 JOUE L 201 de 03.08.2010, pp. 30 a 40.

[107] Agência Europeia de Defesa (Maio, 2023), *Annual Report* disponível em https://eda.europa.eu/docs/default-source/Documentos/eda-annual-report-2022_en-web.pdf

Embora Portugal, registe apenas 11,5% de incidência de ciberataques (Figura 5), verifica-se que 1 em cada 10 empresas já foi vítima um ciberataque. Número este que se encontra a baixo da média Europeia, mas cuja tendência se prevê aumentar nos próximos anos.

Figura 5 - Empresas que sofreram incidentes relacionados com TIC em 2021



Fonte: *Eurostat (2022) isoc_cisce_ic*, *https://ec.europa.eu/eurostat/statistics-explained/images/a/a7/ICT_security_2022_-_graphs_and_tables.xlsx*

Numa conjetura em que as ameaças cibernéticas se estão a tornar cada vez mais comuns, mais eficazes e mais sofisticadas, nunca foi tão importante compreendermos quais são as ameaças que existem, quais os seus efeitos, as suas consequências e como preveni-las.

Com base nos dados da ENISA *Threat Ladscape 2022*, os tipos mais comuns de ameaças cibernéticas utilizadas incluem ataques de *ransomware*, *malware*, ataques de *phishing* e engenharia social, ataques de *Denial of Service* (comumente conhecidos como DDoS), roubo de dados, desinformação e ataques a cadeias de abastecimento (Supply Chain).

Ataques de malware: O malware é um tipo de software concebido para prejudicar um sistema ou rede de computadores. O malware pode incluir vírus, *worms*, *Trojans* (cavalo de Troia), e *ransomware*[108]. Estes tipos de ataques são frequentemente executados

[108] No relatório da ENISA (2022). "Theath Landscape for Ransomware Attacks" https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks, o *ransomware* é

através de e-mails maliciosos, descarregamentos de sítios da web, e táticas de engenharia social. Casos famosos de ataques de *malware*, da estirpe *ransomware*, incluem o ataque de resgate *WannaCry*[109] que afetou mais de 200.000 computadores em 150 países em 2017 e o ataque de malware *NotPetya*[110] que visou empresas ucranianas em 2017, causando mais de 10 mil milhões de dólares em danos.

Ataques de *Phishing*: Os ataques de *phishing* são concebidos para enganar os utilizadores no fornecimento de informações pessoais, tais como palavras-passe e números de cartões de crédito. Estes ataques utilizam frequentemente emails, chamadas telefónicas, ou mensagens de texto que parecem ser de uma fonte de confiança. Um dos casos frequentemente utilizado como exemplo para este tipo de ataques foi o ataque ao Yahoo em 2013[111], neste ataque foi utilizada a técnica de *Spearfishing*, esta técnica é mais avançada que o Phishing porque tem como objetivo atacar indivíduos específicos, por exemplo o CEO de uma empresa, equipa de IT, ou qualquer pessoa que trabalhe naquela organização. Neste caso, não se sabe ao certo qual foi o e-mail que foi recebido com o malware ou quem o abriu, o que é certo é que depois de ter sido acedido os hackers tiveram uma porta aberta para se infiltrarem nos servidores da empresa e assim poder exfiltrar os dados de cerca de três mil milhões de contas de utilizadores do Yahoo.

Ataques de DDoS: Os ataques de Negação de Serviço Distribuída (DDoS) são concebidos para sobrecarregar uma rede com tráfego, tornando-a indisponível aos

classificado "*como um tipo de ataque em que os agentes da ameaça assumem o controlo dos activos de um alvo e exigem um resgate em troca do retorno da disponibilidade do activo. disponibilidade do activo.".* O ransomware encripta os dados, impedindo que os utilizadores acedam aos ficheiros até que seja pago um resgate, geralmente por via de criptomoedas, na falta do qual é desencadeada uma ação. Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[109] Os cibercriminosos responsáveis pelo ataque tiraram partido de uma debilidade no sistema operativo do Microsoft Windows, alegadamente desenvolvido pela Agência de Segurança Nacional dos Estados Unidos, que permitia tomar o controlo à distância de qualquer computador. Fonte: Kaspersky *"What is WannaCry ransomware?",* Resource Center. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[110] O ransomware Petya criptografa a tabela de arquivos mestre (MFT) do computador que invadia, desta forma, o computador, impedindo-o de aceder ao disco rígido, nem ao próprio sistema operacional., Fonte: Ivan B. (2019, Novembro). *"O que é o ramsomware Petya?"* Academy Avast. https://www.avast.com/pt-br/c-petya

[111] Até hoje este ataque ocupa um lugar de destaque a nível da história mundial de ataques de cibersegurança por ter sido o ataque em que ocorreu o Maior número de exfiltração de dados de contas, incluindo nomes de utilizadores e passwords, ate hoje registado. Foram mais de mais de 3 mil milhões de dados de contas dos utilizadores, resultando num prejuízo estimado de cerca de 3 mil milhões de dólares. Fonte: Jonathan S., Jim F. (2017, Outubro). "Yahoo says all three billion accounts hacked in 2013 data theft". Reuters. https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1

utilizadores.[112] Estes ataques podem ser lançados utilizando *botnets*, que são redes de computadores infetados que são controladas pelo atacante. Um dos casos mais famosos de ataques DDoS foi o ataque ao Dyn em 2016[113], que perturbou o acesso à Internet a websites populares como Twitter, Amazon e Netflix.

Ataques de Engenharia Social: Os ataques de engenharia social são concebidos para explorar o comportamento humano para obter acesso a informação sensível. Embora esta prática possam servir-se da tecnologia, dependem sempre de um elemento humano para serem bem sucedidos.[114] Estes ataques podem incluir *phishing, spearphishing, whaling, smishing, vishing, business e-mail compromise* (BEC), fraude, falsificação de identidade e contrafacção.[115] Casos famosos de ataques de engenharia social incluem o ataque ao Target em 2013[116], onde hackers ganharam acesso à rede da empresa através de um fornecedor externo, roubando dados de mais de 40 milhões de contas de cartões de crédito e débito.

Suplly chain: Com um comércio à escala global baseado no online, os efeitos em cascata de um ataque cibernético à cadeia de abastecimento podem ser significativos. Como a própria palavra indica, trata-se de um ataque a uma cadeia logística que procura comprometer toda a cadeia a seu redor. Em termos formais, para que um ataque seja classificado como um ataque à cadeia de abastecimento, tem que ter como alvo o fornecedor e o cliente.[117]

---

[112] Cybersecurity & Infrastructure Security Agency (2021, Fevereiro). "*Understanding Denial-of-Service Attacks*", disponível em https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

[113] O ataque foi lançado pela inundação dos servidores da Dyn com um enorme volume de tráfego, sobrecarregando a sua capacidade de lidar com os pedidos. Isto resultou na indisponibilidade do serviço Sistema de Nomes de Domínio (DNS) da Dyn, que traduz os nomes de domínio de websites em endereços IP que podem ser utilizados para aceder aos websites. Fonte: Woolf, N. (2016, Outubro). "*DDoS attack that disrupted internet was largest of its kind in history, experts say*". The Guardian. Disponível em https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[114] ENISA. *ENISA Threat Landscape* (2022, Novembro), disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[115] Ibidem.

[116] De acordo com relatório da empresa que investigou o ataque, tudo começou com o roubo das credenciais de um fornecedor de serviços da target, o qual foi infectado por meio de uma campanha de 'phishing' por e-mail. Fonte: Committe on Commerce, Science, and Transportation. (2014, Março). "*A "Kill Chain" Analysis of the 2013Target Data Breach*" https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

[117] Tomemos de exemplo o ataque "The Colonial Pipeline Breach" ocorrido em Maio de 2021, que resultou em preços mais elevados da gasolina, compras em pânico e escassez local, após os sistemas informáticos que geriam os oleodutos da empresa terem sido bloqueados por hackers que só os libertariam se a empresa procede-se ao pagamento de 5 milhões de dólares. Kelly, S and Resnick-ault. (2021, Junho). "*One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators*". Reuters. *https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/*

Outros tipos de ciberataques incluem ataques de injeção SQL, ataques *"man-in-the-middle"*, e ataques de *cross-site scripting.* Os ataques de injeção SQL são concebidos para explorar vulnerabilidades em bases de dados para obter acesso a informação sensível. Os ataques de *man-in-the-middle* envolvem intercetar comunicações entre duas partes para obter acesso a informação sensível. Ataques de *cross-site scripting* envolvem a injeção de código malicioso num website para obter acesso a informação sensível.

Através destes exemplos é possível ter consciência da quantidade de ciberataques existentes e do impacto que podem exercer sob organizações, governos e particulares. Como tal, é importante estar ciente destas ameaças e tomar medidas de proteção para não estar vulnerável.

Quer seja no nosso local de trabalho, ao utilizar o computador ou qualquer aparelho digital ligado à internet, ou no nosso dia a dia, ao utilizarmos o nosso computador pessoal e telemóvel, é possível praticar algumas ações que permitem grandemente aumentar a nossa segurança quando utilizamos a internet, de forma a evitar que sejamos alvos de burlas e também diminuir o risco de nos expormos a qualquer ameaça informática, este tipo de ações chamam-se boas práticas de cibersegurança, ou de "ciber-higiene".

Alguns exemplos de boas práticas de cibersegurança devem incluir[118]:

- Relativamente a acessos e palavra passe, estas não devem em circunstância alguma ser partilhadas.
- Não utilizar a mesma palavra passe em diferentes sites ou aplicações;
- Não utilizar o email profissional para registo em sites e serviços pessoais;
- Não memorizar credenciais no acesso a sites ou aplicações;
- Bloquear o computador quando se ausentar do local;
- Não abrir ficheiros recebidos por email sem ter a certeza da origem / conteúdo, entre outras medidas.

Uma das recomendações mais veiculada, e que qualquer pessoa que já tenha criado um perfil na internet provavelmente conhece, é utilizar uma palavra passe complexa. Uma palavra passe complexa deverá ser composta por letras maiúsculas e minúsculas, números e outros símbolos especiais como por exemplo **" : / * @ # &**. Esta recomendação é muito popular dado o seu nível de eficácia, uma vez que a diferença entre

[118] CNCS (2022). "*Relatório Cibersegurança em Portugal –Riscos e Conflitos 2022"*, disponível em https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

escolher um palavra passe com 6 caracteres composta apenas por letras minúsculas ou uma palavra passe com 8 caracteres composta por letras maiúsculas e minúsculas, números e símbolos, pode representar a diferença de esta ser descoberta em alguns minutos ou mesmo segundos, para demorar alguns anos.[119]

5. Identificação dos responsáveis e os problemas de jurisdição

Atualmente a cibersegurança enfrenta uma série de desafios no que diz respeito à determinação da jurisdição responsável pelo julgamento dos cibercriminosos e à identificação desses criminosos. Esses desafios decorrem da natureza transnacional e complexa dos cibercrimes, que muitas das vezes ultrapassam fronteiras físicas e envolvem indivíduos ou grupos criminosos espalhados por diversas partes do mundo.

Como tal, é essencial que os principais intervenientes no combate ao cibercrime tenham a sua atuação bem definida, nomeadamente, quanto aos objetivos a atingir, aos intervenientes envolvidos, aos meios técnicos disponíveis e ao enquadramento jurídico aplicável.

De forma a desagregar os diferentes tipos de ação que podem ser tomadas pelas entidades privadas, militares e judiciais contra o fenómeno dos ciberataques, chamamos à colação a adaptação da sistematização realizada por Pedahzur relativamente ao contra-terrorismo[120], oportunamente adaptada aos ciberataques pelos Autores Lino Santos, Rogério Bravo e Paulo Viegas Nunes na obra "*Protecção do Ciberespaço: Visão Analítica*", na qual se identificam três domínios de atuação, o domínio da proteção simples, o domínio da prossecução criminal e o domínio da defesa do Estado.[121]

Do ponto de vista da defesa do Estado os ciberataques são percecionados como atos de guerra, como tal a resposta a estes centra-se na ação militar, sendo invocados os recursos "*(…) no plano nacional à Constituição da República, à Lei do estado de Sítio e do*

[119]Conforme se pode constatar pelo estudo realizado por Navor, P. (2021). *The Effects of Password Length and Complexity on Password Resiliency* in http://hdl.handle.net/10790/6830, da eficácia de uma password complexa e longa contra uma password simples.

[120] Encontrada na sua obra Pedahzur, A. (2009). The Israeli Secret Services & the struggle against Terrorism. Nova Iorque: Columbia University Press.

[121] C. Guedes Soares, A. P. Teixeira, C. Jacinto (Eds), "Riscos, Segurança e Sustentabilidade" Edições Salamandra, Lisboa, 2012, (ISBN 978-972-689-247-2), pp.163 a 176"

estado de Guerra e, no plano internacional, ao Direito Internacional dos Conflitos Armados[122] *e ao Direito Internacional dos Direitos Humanos*."[123]

No domínio da prossecução criminal," os *ciberataques são vistos e definidos como actos criminalmente relevantes, passíveis de sancionamento dentro do edifício jurídico do respectivo país*"[124]. Quanto à proteção simples, são referenciadas as empresas privadas que executam atividades de proteção dos ativos digitais de outras empresas e dos indivíduos. A Figura 6 esquematiza a divisão destas três dimensões.

Figura 6 - Domínios de atuação na proteção do ciberespaço

	Protecção Simples	**Prossecução criminal**	**Defesa do Estado**
Caracterização	Os ciberataques são vistos como ameaças à disponibilidade, integridade e confidencialidade da informação e de outros activos.	Os ciberataques são vistos como actos criminalmente relevantes.	Os ciberataques são vistos como um acto de Guerra, pondo em risco a existência do Estado.
Objectivos	Proteger potenciais alvos contra ciberataques.	Prevenir crimes e identificar e condenar os responsáveis.	Eliminar uma ameaça que coloque em causa a Soberania Nacional ou ganhar uma vantagem competitiva sobre outro Estado.
Aspectos legais e constitucionais	Salvaguarda dos direitos individuais e da privacidade dos cidadãos.	Actuação dentro do quadro da legislação aplicável e segundo as regras do sistema judicial.	Actuação sujeita à Constituição da Republica, Lei do Estado de Sítio e do Estado de Guerra, bem como ao Direito Internacional dos Conflitos Armados e dos Direitos Humanos.
Actores	Técnicos de sistemas e de redes, Indústria TIC, autoridades reguladoras sectoriais, CSIRT, utilizadores TIC.	Órgãos de polícia criminal, Ministério Público e Magistrados Judiciais.	Forças Armadas e Serviços de Informações.

Fonte*:* C. Guedes Soares, A. P. Teixeira, C. Jacinto (Eds), "Riscos, Segurança e Sustentabilidade" Edições Salamandra, Lisboa, 2012, (ISBN 978-972-689-247-2), pp.163 a 176" *https://comum.rcaap.pt/bitstream/10400.26/3578/1/Artigo_ENRSF_Revisto.pdf*

[122] O Direito Internacional dos Conflitos Armados é composto pelas Convenções de genebra e Protocolos adicionais, sendo definido como "*o conjunto de normas internacionais, de origem convencional ou consuetudinária, especificamente destinado a ser aplicado nos conflitos armados, internacionais ou não internacionais, e que limita, por razões humanitárias, o direito das Partes em conflito de escolher livremente os métodos e os meios utilizados na guerra, ou que protege as pessoas e os bens afetados, ou que possam ser afetados pelo conflito."* SWINARSKI, Christophe. Introdução ao direito internacional humanitário, Brasília: Comitê Internacional de Direitos Humanos, 1996, p. 18.
[123] C. Guedes Soares, A. P. Teixeira, C. Jacinto. (2012), op.cit., pp.163 a 176.
[124] Ibidem.

Em Portugal, a criminalidade informática envolve duas realidades criminológicas diferentes. A primeira, os crimes previstos e punidos no nosso sistema jurídico contra os sistemas informáticos, previstos e punidos no Capítulo II da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime) – que engloba os crimes de falsidade informática (artigo 3.º), dano relativo a programas ou outros dados informáticos (artigo 4.º), sabotagem informática (artigo 5.º), acesso ilegítimo (artigo 6.º), interceção ilegítima (artigo 7.º) e reprodução ilegítima de programa protegido (artigo 8.º).[125]

A segunda realidade criminológica, prende-se com os crimes praticados por meio de um sistema informático, aqui englobando-se todo o crime perpetrado com o recurso aos meios tecnológicos, por exemplo a burla informática artigo 221.º do Decreto-Lei nº 48/95, de 15 de Março (Código Penal), a pornografia de menores (artigo 176.º do Código Penal), a devassa por meio de informática (artigo 193.º do Código Penal), e em geral, os crimes de falsificação, os crimes contra a honra, entre outros.[126]

A competência legal para prevenção[127] e a investigação[128] criminal dos crimes informáticos está atribuída por lei à Polícia Judiciária[129]. Esta dispõe de uma Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), cujas competências se encontram definidas no artigo 33º do Decreto-Lei n.º 137/2019 de 13 de Setembro, do qual se transcreve parte:

"(…)

2 - À UNC3T compete a prevenção, deteção e investigação dos seguintes crimes, sem prejuízo de outros cuja competência lhe seja atribuída pelo diretor nacional:

a) Os crimes previstos na Lei n.º 109/2009, de 15 de Setembro;

b) Praticados com recurso ou por meio de tecnologias ou de meios informáticos, previstos, designadamente:

i) No regime legal de proteção de dados pessoais;

ii) No Código dos Direitos de Autor e Direitos Conexos, incluindo a interferência e o desbloqueio de formas de proteção tecnológica de bens e de serviços;

[125] Ministério Público (Abril 2019) "Meios de Obtenção de Prova e Medidas Cautelares e de Polícia", Coleção formação, Centro de Estudos Judiciários.
[126] Ibidem.
[127] Artigo 3.º, al. f) da Lei n.º 38/2009, de 20 Julho (Lei de Política Criminal); e art. 4.º e 5.º da Lei n.º 37/2008, de 06 de Agosto (Orgânica da Polícia Judiciária);
[128] Artigo 1.º da Lei n.º 49/2008, de 27 de Agosto (Lei de Organização da Investigação Criminal)
[129] Artigo 7.º, n.º3, al. l) e n) da Lei n.º 49/2008, de 27 de Agosto (Lei de Organização da Investigação Criminal)

c) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes:

i) Contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistema informático;

ii) De devassa por meio da informática;

iii) De burla informática e nas comunicações;

iv) Relativos à interferência, utilização ou manipulação ilegítima de meios de pagamento eletrónicos e virtuais;

v) De espionagem, quando cometido na forma de um qualquer programa informático concebido para executar ações nocivas que constituam uma ameaça avançada e permanente;

vi) De ciberterrorismo, em articulação com a UNCT."

Relativamente à cooperação internacional, o principal mecanismo transnacional nesta matéria é a Convenção sobre o Cibercrime, que procurou definir "*uma política criminal comum*" visando "*proteger a sociedade da criminalidade no ciberespaço, nomeadamente através da adopção de legislação adequada e da melhoria da cooperação internacional*"[130]

Em terreno nacional, com a entrada em vigor da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), o legislador transpôs para o direito interno a Convenção sobre o Cibercrime e a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24/2, relativa a ataques contra sistemas de informação.

Conforme vem consignado no artigo 1º da Lei do Cibercrime, o objeto desta lei é estabelecer "*as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico*,", reforçando nos artigos 20.º a 26.º, as medidas específicas no plano da cooperação internacional, fazendo, no entanto, a ressalva no artigo 28º que "*Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respectivamente, as*

[130] Parágrafo 4 do Preâmbulo da Convenção do Cibercrime do Conselho da Europa, de 23 de Novembro de 2001.

disposições do Código Penal, do Código de Processo Penal e da Lei n.º 144/99, de 31 de Agosto (Lei Da Cooperação Judiciária Internacional Em Matéria Penal)".[131]

A nível de medidas concretas para fins de cooperação nacional, o artigo 21º estabelece a necessidade de um ponto de contacto centralizador e permanente disponível 24h por dia 7 dias por semana. No artigo 22.º e 23.º encontra-se estabelecida a possibilidade legal de se proceder, em Portugal, à preservação e revelação expeditas de dados informáticos em cooperação internacional, e motivos da sua recusa. Existe ainda o acesso a dados informáticos em cooperação internacional, artigo 23.º, e o acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento e a interceção de comunicação de comunicações em cooperação internacional, nos termos previstos do artigo 26.º, todos da Lei da Cibercrime.

6. Falta de sensibilização nas empresas e a promoção de boas práticas

A integração de sistemas de segurança de Endpoint, de rede, de aplicações e nuvem são requisitos essenciais para as operações de uma qualquer empresa, mas a adoção de meios tecnológicos de defesa não são por si só suficientes, uma vez que para além de explorar essas fraquezas tecnológicas, os criminosos também exploram o comportamento e as emoções das pessoas. Num dos mais recentes estudos levados a cabo pela Verizon[132], e utilizados também pela ENISA[133], demonstram que cerca de 82% das violações de dados ocorrem por erro humano.

Atualmente, os golpes de *Business Email Compromise (BEC)*[134] e *phishing* são a técnica mais comum e eficaz utilizada pelos criminosos, dada a variedade de táticas que

[131] A este propósito cumpre trazer à colação a Nota Prática n.º 3/2014, de 12 de Junho de 2014, relativa à cooperação judiciária com os Estados Unidos da América, nomeadamente à Google, ao Facebook e à Microsoft, com a menção da possibilidade de cooperação informal, sem recurso a cartar rogatórias, através de pedido direto, mediante a apresentação do formulário específico para o efeito, disponível no SIMP, desde que o respetivo pedido seja formulado com respeito pela lei interna do país em causa e pelas leis dos Estados Unidos. Este documento de cooperação encontra-se disponível para consulta em https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_3_isp_eua.pdf

[132] Verizon (2023). *Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/dbir/

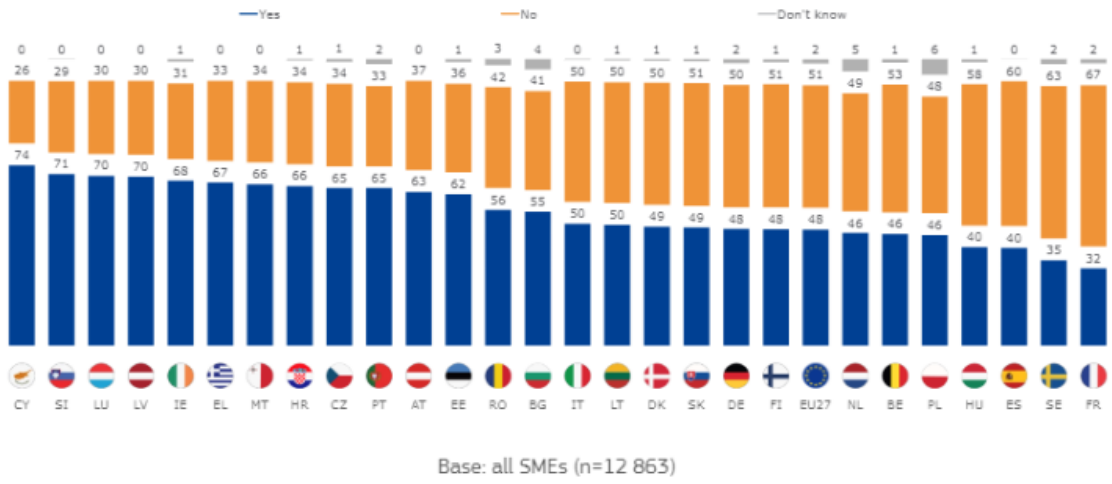
[133] ENISA (Novembro, 2022) *ENISA THREAT LANDSCAPE 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport*

[134] Business email compromisse, comumente conhecido como BEC, é um tipo de cibercrime em que o criminoso utiliza o correio electrónico para enganar alguém e fazê-lo enviar dinheiro ou divulgar informações confidenciais da empresa. O criminoso faz-se passar por uma pessoa de confiança e depois pede o pagamento de uma conta falsa ou dados confidenciais que podem ser utilizados noutra burla. Microsoft (2023). *What is business email compromisse.), in https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec*

permite utilizar para persuadir as pessoas a fornecer dados ou informações pessoais e até induzir os utilizadores a clicar em links que os levam a sites comprometidos, o que por sua vez leva a um ataque cibernético completo e a avultados danos financeiros e reputacionais para a empresa, podendo em último caso determinar o fim da atividade da empresa.[135]

Alinhada com o erro humano e a falta de conhecimentos nesta área, existem outros comportamentos que nos permitem inferir da falta de sensibilização e conhecimentos para esta área, por exemplo, num estudo levado a cabo pela Ipsos European Public Affairs a pedido da Comissão Europeia[136], realizado em 2021 e publicado em 2022, a cerca de 12.000 funcionários de PME's com funções executivas, revela que 48% dos funcionários das suas empresas utilizam os seus dispositivos eletrónicos pessoais para atividades regulares relacionadas com a empresa (Figura 7).

Figura 7 – Trabalhadores que utilizam dispositivos eletrónicos pessoais para desempenhar funções relacionadas com o seu trabalho



Fonte: Comissão Europeia, Direcção-Geral da Justiça e dos Assuntos Internos, (2022). SMEs and cybercrime: summary, Publications Office of the European Union. https://data.europa.eu/doi/10.2837/89101

[135] O FBI testemunhou um aumento de 65% nas perdas sofridas entre Julho de 2019 e Dezembro de 2021 para esses tipos de golpes. Além disso, as perdas são avultadas e têm tendência a aumentar; as perdas nacionais e internacionais relacionadas com o BEC ascenderam a 43 mil milhões de dólares entre Junho de 2016 e Dezembro de 2021, e em 2021 as perdas financeiras do BEC foram 64 vezes piores do que as do *Ransomware*. FBI (2021) Internet Crime Report/Internet Crime Complaint Center *https://www.ic3.gov/Media/Y2022/PSA220504*

[136] European Commission, Directorate-General for Migration and Home Affairs, (2022). "*SMEs and cybercrime: summary, Publications Office of the European Union.*" https://data.europa.eu/doi/10.2837/89101

Em Portugal, a média de trabalhadores que utilizam os seus dispositivos pessoais para executar tarefas relacionadas com o seu trabalho é de 65%, este número é preocupantemente superior à média global dos países da UE. Tendo como referência a nossa vizinha, Espanha, com uma média de 40%.

Deste modo é essencial que colaboradores, gerência e administração de uma empresa estejam sensibilizados e bem informados sobre as potenciais ameaças e riscos a que estão expostos, de modo a que se possam tornar mais vigilantes e melhor preparados para detetar, prevenir e combater as ameaças cibernéticas.

Constante nesta base, as empresas devem promover boas práticas que, incentivem a reflexão sobre os desafios da segurança no mundo digital, e, simultaneamente capacitem os seus funcionários. Estas práticas podem envolver:

a) Estabelecimento de canais de comunicação eficazes para manter os colaboradores informados sobre as últimas ameaças cibernéticas, ataques ocorridos, avanços na tecnologia e novas políticas de segurança. Esta prática pode facilmente ser concretizada através do envio de emails, newsletters, cartazes ou mesmo divulgação nas redes sociais. Ao implementar estes canais de comunicação, as empresas conseguem manter os seus funcionários atualizados sobre as últimas noticias da área e também fortalecer a cultura de cibersegurança dentro da organização[137].
b) Estabelecer procedimentos e políticas internas de cibersegurança é extremamente importante para assegurar que toda a organização segue o mesmo conjunto de directrizes e regras para assegurar um nível de segurança uniforme em todos os sectores da organização. Ademais, a eficácia destes procedimentos também se pode revelar de cabal importância dado que se tratam de documentos que podem ser acedidos a qualquer momento e que informam todos os funcionários do plano de resposta a incidentes de cibersegurança, além disso, proporciona a capacidade de compreender claramente as funções e obrigações individuais no caso de um ciberataque, bem como identificar os principais interlocutores internos da empresa para notificar ciberincidentes da forma mais rápida possível.[138]

[137] Alshaikh, Moneer (2020). "*Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security", 98(), 102003–*. doi:10.1016/j.cose.2020.102003
[138] Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In 29th European Safety and Reliability Conference (pp. 4036-4043).

c) A realização de programas regulares de formação em cibersegurança para funcionários é uma excelente forma de promover a sensibilização e a formação sobre as últimas ameaças, vulnerabilidades, e melhores práticas em contexto de cibersegurança. Com as atuais ameaças cibernéticas mais sofisticadas e persistentes do que nunca, revela-se fundamental conhecer em profundidade alguns conceitos essenciais e medidas de segurança. Uma das melhores formas de promover estes conhecimentos é através de ações de formação. Estes programas podem incluir módulos de formação on-line, workshops, e ataques simulados de phishing.[139][140]

É evidente que quanto mais se explora a cibersegurança, que a complexidade do tema se densifica. Contudo, uma formação que abranja tópicos simples, mas pertinentes, como a deteção de emails questionáveis (*phishing*), resgates (*ransomware*), segurança física de dispositivos no local de trabalho[141], planos de reação a ameaças (resposta ao risco), segurança de redes, e outros processos, revela-se absolutamente necessária de modo a sensibilizar e educar os colaboradores, assim como para demonstrar a dimensão e consequências que uma simples ação irrefletida pode tomar.

Como tal, qualquer formação ministrada deve incluir a apresentação de perigos que os trabalhadores possam enfrentar no seu dia a dia, quer através dos seus dipositivos pessoais, caixas de correio de e-mail, redes sociais, ou outras tecnologias que utilizem regularmente.

Em Portugal, os avisos para a sensibilização têm sido frequentes e com origem em diversos interlocutores. O CNCS ocupa um lugar de destaque, com publicações frequentes de boletins e newsletters sobre o estado da cibersegurança nos vários contextos

[139] Alshaikh, Moneer (2020). "Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security," 98(), 102003–. doi: 10.1016/j.cose.2020.102003

[140] A este propósito a International Telecommunication Union (ITU), é a agência especializada das Nações Unidas para as tecnologias da informação e da comunicação – TIC, sugere que os países e as agências nacionais de cibersegurança deveriam promover a existência de programas de formação profissional específicos em cibersegurança para sensibilizar o público em geral (através por exemplo de um dia, semana ou mês nacional de sensibilização para a cibersegurança), promover a cibersegurança para a população activa de diferentes perfis (técnicos, ciências sociais, etc.) e promover a certificação de profissionais do sector público e privado. -International Telecommunication Union (ITU).. "*ITU-D Cybersecurity Program Global Cybersecurity Index – GCIv5 Reference Model,"* disponível em https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2E.pdf

[141] Conhecer os procedimentos e regras da empresa, Procedimentos defensivos - Utilização de senhas fortes, securização de dados em computadores, dispositivos móveis, redes, e na nuvem.

da sociedade, oferece formação e apoio regular à administração pública e ao setor privado, mas também existem outros órgãos públicos que têm contribuído para o aprofundamento da cibersegurança, designadamente:

1. a Comissão Nacional da Proteção de Dados, no dia 10 de Janeiro aprovou a Diretriz/2023/1, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais, destinadas aos responsáveis pelos tratamentos e aos subcontratantes, pretendendo sensibilizá-los para as suas obrigações legais no domínio da segurança dos tratamentos e para a necessidade de realizarem um maior investimento nesta área.[142]
2. o Conselho de Prevenção da Corrupção, criado pela Lei n.º 54/2008, de 4 de Setembro, é uma entidade administrativa independente que tem como fim desenvolver uma atividade de âmbito nacional no domínio da prevenção da corrupção e infrações conexa, também prestou um contributo na área da cibersegurança, ao emitir uma recomendação sobre "As Boas Práticas de Cibersegurança"[143]
3. o Ministério Público através do Gabinete Cibercrime, em funcionamento desde Dezembro de 2011, *"Tem como escopo geral a coordenação interna, do Ministério Público, em tal área da criminalidade, a formação específica nesta matéria e o genérico estabelecimento de canais de comunicação com fornecedores de serviço de acesso às redes de comunicação, que permitam facilitar a sua colaboração na investigação criminal."*, partilhando regularmente conteúdo relevante nesta área desde newsletters, formações e documentos relevantes.[144]

---

142 «Os crescentes ataques a sistemas de informação, verificados no último ano, afetaram na sua grande Maioria dados pessoais. Tais incidentes de segurança revelaram que se as organizações estivessem dotadas de medidas de segurança adequadas, os riscos teriam sido menores e o impacto nos direitos dos titulares dos dados mais reduzidos. A CNPD elenca um conjunto de medidas organizativas e de medidas técnicas que devem ser consideradas pelas organizações nos seus planos de prevenção e de minimização dos riscos.» Comissão Nacional de Proteção de Dados, Diretriz/2023/1, de 10 de Janeiro *https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122048*

[143]CONSELHO DA PREVENÇÃO DA CORRUPÇÃO. "*Recomendação do Conselho de Prevenção da Corrupção sobre Boas Práticas de Cibersegurança* (Abril, 2022) https://www.cpc.tcontas.pt/documentos/recomendacoes/recomendacao_cpc_20220405.pdf

[144] Ministério Público. "Gabinete Cibercrime" https://cibercrime.ministeriopublico.pt/divulgacao-mp

4. a Polícia Judiciária, através da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T). A este propósito consultar o ponto 2.6 (Identificação dos responsáveis e os problemas de jurisdição) desta dissertação na página 58.

CAPÍTULO 3 – Causas (Influência, Poder, Dinheiro)

Todas as empresas, independentemente da sua dimensão, podem ser alvo de um ciberataque. Com já foi evidenciado até aqui, este ataque pode ser concretizado através de vários métodos, agentes e pode ter motivações distintas, individuais ou sociais, e consequências a várias escalas.

O objectivo deste capítulo é analisar algumas das principais causas que poderão estar por de trás deste tipo de ataques, pois ao reconhecer os motivos por detrás dos ciberataques, é possível construir uma melhor compreensão dos riscos a que uma organização se encontra exposta e compreender a melhor forma de os prevenir.

1. A monetização do cibercrime

Os dados são agora o recurso mais valioso do mundo, ou aplicando a famosa expressão do matemático e empresário Clive Humby "*Data is the new oil",* com empresas e governos a confiarem neles para tomarem decisões críticas e impulsionarem a inovação. No entanto, o valor dos dados também os torna um alvo principal para os cibercriminosos e outros atores maliciosos que procuram lucrar com eles.

Com um risco mínimo para os criminosos, existe um número de pessoas cada vez maior a recorrer à cibercrime devido aos requisitos de entrada pouco qualificados e à promessa de taxas de lucro financeiro extremamente elevadas.

O relatório publicado pela Verizon Business 2020 *Data Breach Investigations Report* demonstra que os ganhos financeiros continuam a ser o principal motor do cibercrime com quase nove em cada 10 (86%) dos ataques investigados terem como motivação ganhos financeiros.

Os criminosos informáticos procuram lucrar com as suas actividades através do roubo de dados sensíveis, tais como informações pessoais ou dados financeiros, e depois vendendo-os em mercados clandestinos tais como a Deepweb.[145]

A venda destes dados pode resultar em consequências muito graves para as empresas e, principalmente, para os titulares dos dados.

[145] Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. The Palgrave handbook of international cybercrime and cyberdeviance, 91-116.

Obtendo o acesso a informação suficiente, os dados relativos à identificação de determinado titular de dados podem ser utilizados para inúmeros fins ilícitos. O roubo de identidade, por exemplo, é um crime em que a informação pessoal da vítima é utilizada para obter benefícios à custa da vítima. Muitos serviços online exigem que os utilizadores preencham dados pessoais tais como nome completo, morada e número de cartão de crédito. Os criminosos roubam estes dados de contas online para cometerem roubo de identidade, assim como utilizam o cartão de crédito da vítima para contrair empréstimos em seu nome, abrir contas bancárias, ou fazer-se passar por si em sites ou redes sociais.[146]

Outra forma dos hackers conseguirem obter lucros monetários é através da extorsão de empresas ou indivíduos. A extorsão ocorre quando um hacker ganha acesso a sistemas ou dados sensíveis ameaçando posteriormente divulgá-los publicamente, a menos que a pessoa ou a organização pague um resgate. Estes resgates podem variar desde grandes somas de dinheiro a pedidos de outros tipos de pagamento, normalmente pagas com recurso a criptomoedas[147]. Nesta situação, o extorsionário pode divulgar publicamente os dados roubados ou mesmo atacar os sistemas da organização se a exigência não for satisfeita. Podem até divulgar estes dados, apesar de serem pagos.

Quando se trata de indivíduos, muitos deles são vítimas de sextorção, isto é, quando um hacker se aproveita de imagens ou vídeos comprometedores de uma pessoa e depois ameaça libertá-los, a menos que paguem o valor do resgate.

Para além da fonte de lucro com este tipo de ações, os criminosos também desenvolveram outras formas de capitalizar com o cibercrime, através do desenvolvimento de "*Toolkits do Crime*" assistimos a uma verdadeira produtização do Cibercrime.[148]

---

[146] Alguns cuidados e boas práticas recomendados pela GNR acerca do Furto de Identidade. https://www.gnr.pt/cyberFurtoIdentidade.aspx

[147] Para a definição de criptomeoda será considerada a definição avançada pelo Banco de Portugal "*E o que são criptoativos? São representações digitais de valores ou de direitos que podem ser transferidos e armazenados eletronicamente. Apesar de poderem ser usados para fazer pagamentos, como o valor dos criptoativos oscila muito, são sobretudo utilizados como ativos de investimento. Um dos mais conhecidos é a bitcoin."* Banco de Portugal. "*Criptoativos, stablecoins e euro digital? Descubra as diferenças."* *https://www.bportugal.pt/page/criptoativos-stablecoins-e-euro-digital-descubra-diferencas-1*

[148] Alazab, Ammar; Abawajy, Jemal; Hobbs, Michael; Layton, Robert; Khraisat, Ansam (2013). *[IEEE 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) - Melbourne, Australia (2013.07.16-2013.07.18)] 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications - Crime Toolkits: The Productisation of Cybercrime. , (), 1626–1632.* doi:10.1109/TrustCom.2013.273

Produzir um malware e escrever um código malicioso eficaz é uma tarefa difícil, que requer um elevado nível de conhecimentos sobre sistemas informáticos. Este facto significa que os atacantes e os autores de malware eram altamente qualificados tecnicamente.

No entanto, rapidamente se tornou obvio que o malware podia ser vendido em vez de utilizado. Isto reduz os riscos para os autores, uma vez que a dificuldade e o risco dos ataques não é roubar credenciais, mas convertê-las em dinheiro. Além disso, as organizações criadas em torno do cibercrime, muitas vezes aproveitam-se de redes de crime organizado existentes, significa que estes criminosos se estão a tornar especializados no cibercrime, alocando pessoas e recursos exclusivamente para o desenvolvimento de malware.[149]

Como exemplo da produtização do cibercrime, os criadores do *Tool Kit* "*Blackhole*", conhecido como o *"Toyota Camry" dos kits de exploração - barato, facilmente disponível e fiáveis."*[150], vendiam uma subscrição do seu malware, permitindo aos seus clientes que obtenham as mais recentes funcionalidades à medida que estas são desenvolvidas e a possibilidade de personalizar o ataque. Esta forma de venda do malware, utiliza o mesmo modelo de subscrição utilizado por um número crescente de empresas de software na economia digital legítima.

Este tipo de atuação, demonstra a crescente complexidade do cibercrime e a necessidade de continuar a formar e a informar os cidadãos sobre os perigos aos quais estão sujeitos no mundo digital, a necessidade das autoridades e instituições intensificarem os seus esforços para combater o cibercrime, e as empresas a investirem na sua proteção de cibersegurança, de forma a tentar estar um passo à frente dos cibercriminosos, e, na eventualidade, de sofrer um ciberataque, diminuir o impacto dos danos.

[149] Ibidem.
[150] White, Joshua S.; Matthews, Jeanna N. (2013). [IEEE 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE) - Fajardo, PR, USA (2013.10.22-2013.10.24)] 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE) - It's you on photo?: Automatic detection of Twitter accounts infected with the Blackhole Exploit Kit. , (), 51–58. doi:10.1109/malware.2013.6703685

2. Influência em processos democráticos e a desinformação

Com tantas fontes de informação na internet, torna-se um verdadeiro desafio compreender qual o conteúdo que se baseia em factos reais, meias verdades ou mentiras.

As novas tecnologias e software permitem propagar a desinformação facilmente e de forma comparativamente barata através das redes sociais e de outros meios em linha. A desinformação concentra-se geralmente em temas sensíveis que, por poderem polarizar opiniões e agitar emoções, serão provavelmente mais partilhados.[151] Estes temas incluem as questões de saúde (por exemplo, campanhas contra a vacinação), a migração, as alterações climáticas ou as questões de justiça social.

Com a velocidade atual da informação, facilitada pela utilização de plataformas de redes sociais, a preocupação com a desinformação nunca constituiu um desafio estratégico tão grande para as democracias. Isto pode ser particularmente problemático no período que antecede as eleições, quando informações falsas ou enganosas podem ser utilizadas para influenciar o resultado da votação ou perturbar a ordem pública.

As notícias falsas podem também contribuir para a erosão da confiança nas fontes e agências noticiosas tradicionais, tornando mais difícil para os cidadãos separar os factos da ficção e tomar decisões informadas. Além disso, sabe-se que atores estrangeiros têm utilizado notícias falsas como um instrumento de interferência nos processos democráticos, ao criarem e divulgarem informações falsas a fim de influenciar a opinião pública e semear a discórdia no país alvo.[152]

Por conseguinte, é muito importante que os indivíduos avaliem criticamente a informação com que se deparam, e que os governos e as empresas de comunicação social tomem medidas para combater a difusão de notícias falsas.

---

[151] Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, *64*(6), 763-774. DOI: 10.1016/j.bushor.2021.07.012

[152]Durante as eleições presidenciais americanas de 2016, foram divulgadas notícias falsas nos meios de comunicação social e outras plataformas online, numa tentativa de influenciar o resultado das eleições. Estas histórias, frequentemente sensacionais e enganadoras, visavam questionar a idoneidade dos candidatos políticos e semear a divisão e a desconfiança entre os eleitores. De acordo com um estudo do Pew Research Center, 64% dos adultos norte-americanos acreditavam que notícias falsas tinham causado "muita" confusão e desconfiança durante as eleições, conclusões apuradas no estudo de Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211-236

De entre as principais técnicas utilizadas para difundir informações erradas e perturbar processos democráticos destacam-se as seguintes[153]:

- Criação e distribuição de notícias falsas ou desinformação através dos meios de comunicação social e outras plataformas online;
- Hacking em campanhas ou organizações políticas e divulgação de informação sensível para influenciar a opinião pública;[154]
- Utilização de ciberataques para perturbar os sistemas de votação e adulterar os resultados eleitorais;
- Divulgação de informação falsa para criar confusão e semear a discórdia entre o público;
- Criação e utilização de *bots* e outras formas de software automatizado para ampliar o alcance e impacto da desinformação.[155]

3. Desinformação COVID-19

Durante a pandemia COVID-19, houve uma quantidade significativa de desinformação e notícias falsas a circular em várias plataformas, incluindo meios de comunicação social, sites de notícias, e aplicações de mensagens como Whatsapp.

A desinformação abrangeu uma vasta gama de tópicos, incluindo as origens do vírus, os seus sintomas, a eficácia dos tratamentos e vacinas, e as ações dos governos e

[153] Exemplos retirados de Comité de Contacto das Instituições Superiores de Controlo da União Europeia. (2020, Dezembro). "Compêndio de auditoria, " A cibersegurança na EU e nos seus Estados Membros" https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_PT.pdf

[154] Em 2022, uma equipa de jornalistas de todo o mundo liderada pela organização *Forbidden Stories*, revelou a existência de um grupo Israelita responsável pela manipulação de mais de 30 campanhas de eleições em todo o mundo, entre outros atos de relacionadas com atividades ilícitas praticadas no espaço digital, como, acesso indevido, sabotagem informática e desinformação. Para lançar campanhas de desinformação, este grupo detinha mais de 30.000 avatares cada um dotado por um complexo histórico de atividade que se estendia por vários anos, levando a crer que de um verdadeiro ser humano se passava. Estas contas partilhavam noticias falsas, interagiam com usuários e entre sim, sempre com o propósito de manipular indivíduos a adotarem certas ideias ou comportamentos. Kirchgaessner, S. et. al. (2023, Fevereiro) "*Revealed: the hacking and disinformation team meddling in elections*". The Guardian. Europe Edition. https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan

[155] Estes robots ou "*bots*" podem publicar conteúdo e interagir uns com os outros, assim como com utilizadores reais através de conexões sociais, este tipo de interações programas faz crer que se tratam de pessoas reais, quando não o são, induzindo pessoas com parcos conhecimentos tecnológicos e induzindo-os numa teia de mentiras, desta forma defendido por Shao, C., Ciampaglia, G., Varol, O., Flammini, A. & Menczer, F. (2017). "*The spread of fake news by social bots"*. arXiv:1707. https://www.researchgate.net/publication/318671211_The_spread_of_fake_news_by_social_bots

organizações de saúde. Algumas destas informações foram deliberadamente difundidas por aqueles que querem criar confusão ou semear a discórdia, enquanto outras desinformações são o resultado de rumores ou mal-entendidos.

Resultando em divulgação de informações tão absurdas como[156]:

- "*beber lixívia ou álcool puro pode curar a infeção pelo coronavírus*", O centro antivenenos da Bélgica registou um aumento de 15% do número de incidentes relacionados com a lixívia.
- teorias da conspiração, como a alegação de que o coronavírus é *«uma infeção causada pelas elites mundiais para reduzir o crescimento demográfico»*.
- alegações de que as *«instalações 5G estariam a propagar o vírus»*. Estas teorias, sem qualquer fundamento, estiveram na origem de ataques a postes com antenas.

A propagação da desinformação foi exacerbada pelo facto de a pandemia ser uma situação em rápida evolução, e de a informação exata ser muitas vezes difícil de obter. Além disso, a utilização crescente das redes sociais e de outras plataformas online durante a pandemia facilitou a rápida e ampla difusão da desinformação.

Para fazer frente a esta verdadeira avalanche de informação falsa, em Março de 2020, a Comissão, a ENISA, a CERT-UE e a Europol emitiram uma declaração conjunta sobre ameaças relacionadas com a COVID-19[157], na qual afirmam que intervenientes mal-intencionados estavam a aproveitar-se deliberadamente das circunstâncias difíceis da crise de saúde pública para visar teletrabalhadores, empresas e indivíduos.

4. O impacto económico dos ciberataques

Nos últimos anos, tem havido um aumento significativo do número de empresas que procuram soluções de cibersegurança, números de 2022 demonstram que o mercado de cibersegurança aumentou para 121 mil milhões de Euros, revelando um crescimento

[156] COMUNICAÇÃO CONJUNTA DO PARLAMENTO EUROPEU, DO CONSELHO EUROPEU, DO CONSELHO, DO COMITÉ ECONÓMICO E SOCIAL E DO COMITÉ DAS REGIÕES (Junho 2020) "*Combater a desinformação sobre a COVID-19: repor a verdade dos factos"* https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020JC0008

[157] COMISSÃO EUROPEIA (Março, 2020). *Coronavirus outbreak - Joint Statement European Commission, ENISA, CERT-EU and Europol in* https://digital-strategy.ec.europa.eu/en/news/coronavirus-outbreak-joint-statement-european-commission-enisa-cert-eu-and-europol

de 5% comparativamente ao ano de 2019, podendo vir a alcançar valores de 195.9 mil milhões de Euros em 2026[158]. Impulsionado pelo o aumento da tecnologia, a transformação digital e pela explosão das ciberameaças e do cibercrime, as empresas estão mais vulneráveis do que nunca às ameaças cibernéticas, procurando assim soluções para estes novos desafios e dificuldades.

Os resultados dos ataques cibernéticos são sobejamente conhecidos, em 2022 o impacto do cibercrime custará à economia mundial cerca de 7 biliões de dólares[159], em proporção, no ano de 2015, o valor do impacto da cibercriminalidade situava-se em 3 biliões de dólares.

Os custos decorrentes da cibercriminalidade incluem danos e destruição de dados, perdas financeiras significativas, perda de produtividade, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, perturbação da atividade corrente após os ataques, danos de reputação, e mesmo consequências legais. Segundo os estudos do Comité Europeu do Risco Sistémico (CERS), o custo médio dos ciberincidentes aumentou cerca de 72% entre 2012 e 2018.[160]

Como tal, as empresas estão a levar a segurança cibernética mais a sério do que nunca. Estudos recentes demonstram que as empresas estão a investir em tecnologias avançadas, tais como inteligência artificial e aprendizagem de máquinas, para detetar e prevenir ataques cibernéticos.[161] Estão também a contratar peritos e consultores em cibersegurança para os ajudar a desenvolver estratégias de segurança robustas. As próprias universidades têm ajudado a promover o aprofundamento desta matéria, por exemplo em Portugal atualmente existem 25 cursos superiores de cibersegurança e segurança da informação, com mais de 916 alunos inscritos[162]. O que por si só, injeta no mercado um grande volume de pessoas com conhecimentos avançados e atuais para fazer face a estas novas ameaças.

---

[158] Dados da Mordor Intelligence (2021). "Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026)" utilizados no documento de European Investment Bank. (2022). European cybersecurity investment platform. Publications Office. https://doi.org/10.2867/943253

[159] CONSELHO EUROPEU & CCONSELHO DA UNIÃO EUROPEIA (Maio 2023). "Cibersegurança: como combate a UE as ciberameaças" https://www.consilium.europa.eu/pt/policies/cybersecurity/

[160] CERS, Comité Europeu do Risco Sistémico (Fevereiro, 2020), "*Systemic cyber risk"*, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

[161] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(5).

[162] CNCS (Dezembro, 2022). *"Cibersegurança em Portugal. Relatório Sociedade", https://www.cncs.gov.pt/docs/rel-sociedade2022-observ-cncs.pdf*

A pandemia da COVID-19 também tem desempenhado um papel no aumento da procura de soluções de cibersegurança. Com a rápida mudança para trabalho remoto e serviços online, as empresas tornaram-se ainda mais vulneráveis a ataques cibernéticos dada a necessidade de acesso remoto seguro, questões relacionadas com a proteção de dados, confidencialidade da informação e a criação de canais de comunicação seguros tornou-se mais crítica do que nunca.

Outro fator que impulsionou a procura de soluções de cibersegurança foi o aumento dos regulamentos e dos requisitos de conformidade. Muitas indústrias, tais como os sectores críticos e prestadores de serviços digitais, têm requisitos regulamentares rigorosos[163] em torno da proteção de dados e da privacidade. O não cumprimento destes regulamentos pode resultar em multas significativas e consequências legais que podem ascender a milhões de euros.

Num caso recente ocorrido em 2021, a empresa de tecnologia de saúde *CaptureRx* sofreu uma violação de dados que afetou 2,4 milhões de pessoas. Poucos meses depois, a empresa viu-se confrontada com 10 processos judiciais, muitos dos quais alegavam medidas de proteção de dados inadequadas e negligência, bem como invasão de privacidade. Em Fevereiro de 2022, o CEO da empresa afirmou que a empresa estava a considerar declarar falência face a um potencial acordo de 4,75 milhões de dólares ao atribuir 25 dólares a cada titular de dados afetador, porém o acordo não foi aceite e a indemnização poderá ascender a 75 dólares por titular segundo as leis de proteção de dados da Califórnia. O caso ainda aguarda decisão. [164]

Noutro caso, ocorrido a um prestador de serviços de psicoterapia finlandês da empresa *Vastaamo* também sofreu uma violação de dados que resultou na falência da empresa. A empresa informou que a sua base de dados de pacientes tinha sido hackeada em Outubro de 2020 por extorsionários cibernéticos que exigiam 450 000€ em bitcoins e ameaçavam publicar os registos roubados. A Vastaamo acabou por ser multada em 608 000 € um ano depois, por não ter cumprido com as disposições do RGPD, acabando por declarar falência em Fevereiro de 2021.[165] Algumas das infrações que a empresa cometeu

[163] NIS e RGPD

[164] McKeon, J. (Fevereiro 2022). "HealthIT Security. CaptureRx to Consider Filing For Bankruptcy if $4.75M Settlement Not Approved", HealthITSecurity disponível em https://healthitsecurity.com/news/capturerx-to-consider-filing-for-bankruptcy-if-4.75m-settlement-not-approved

[165] EDPB. EUROPEAN DATA PROTECTION BOARD (Janeiro, 2022). *"Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations,* disponível em

foram: a não comunicação da violação de dados à autoridade de controlo no prazo geral de 72h conforme o artigo 33º do RGPD; a não comunicação de uma violação de dados pessoais ao titular dos dados nos termos do artigo 34º do RGPD; violação dos princípios relativos ao tratamento de dados pessoais consagrados nos artigos 5º do RGPD e 25º do RGPD, nomeadamente, o principio da integridade e confidencialidade dos dados; a não realização de uma avaliação de impacto sobre a proteção de dados nos termos do artigo 35º do RGPD, uma vez que a empresa realizava um tratamento regular de dados de categoria especial, em concreto, dados de saúde dos pacientes, impunha-se que realizasse esta avaliação; e, ainda, a inobservância das regras de segurança no tratamento de dados pessoais impostas pelo artigo 32º do RGPD.

Estes exemplos ilustram algumas das consequências mais graves que podem resultar de um ciberataque, tendo como denominador comum, a fraca aderência a procedimentos de segurança, políticas de segurança de dados pessoais, boas práticas na gestão de dados e da informação, bem como o incumprimento da lei de proteção de dados pessoais.

Com a combinação de perdas financeiras, perturbações operacionais, danos à reputação e demais consequências legais que lhe possam ser imputadas, uma empresa pode ver-se incapaz de recuperar e acabar por ser forçada a declarar falência. Além disso, o roubo de propriedade intelectual e de informações de caráter confidencial têm o potencial de infligir danos à vantagem competitiva, comprometendo a sua capacidade para gerar receitas. Deste modo, a importância da implementação de medidas robustas de cibersegurança e de estratégias proactivas de gestão do risco cibernético não deveram ser menosprezadas, devendo ser vistas como um investimento, não como um custo.

Paralelemente, é imperativo garantir a conformidade com os requisitos legais referentes à proteção de dados pessoais, de modo a salvaguardar a confidencialidade, a integridade, a disponibilidade e a autenticidade da informação, assim como a conformidade com outros procedimentos pertinentes aplicáveis.

https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en

5. Entraves à economia e cibersegurança

Conforme já foi referido diversas vezes ao longo desta dissertação, a cibersegurança já chegou à atenção dos responsáveis políticos, configurando-se como um problema incontornável. No entanto, um dos principais problemas de cibersegurança tem caráter económico, isto é, a falta de recursos económicos das empresas para investir em cibersegurança e a falta de incentivos públicos para que as empresas adotem sistemas fortes de cibersegurança, são dois dos principais desafios que as empresas atualmente enfrentam.

Uma das principais razões da falta de recursos económicos para o investimento em cibersegurança é a perceção desta ser considerada como uma despesa opcional.[166] Muitas empresas, particularmente pequenas e médias empresas (PMEs), podem ver a cibersegurança como uma despesa adicional que não gera receitas imediatas ou diretas, e por isso podem não a priorizar. [167][168] Outro fator que contribui para isso é a complexidade da cibersegurança. Estas ameaças estão em constante evolução, e as empresas devem manter-se a par das mais recentes ameaças e vulnerabilidades a fim de protegerem adequadamente os seus sistemas. Isto, requer um investimento contínuo em investigação, formação e tecnologia, o que se pode revelar uma atividade muito dispendiosa. Adicionalmente, muitas organizações podem não compreender completamente os riscos das ameaças cibernéticas, e podem não reconhecer os danos potenciais que um ataque cibernético bem-sucedido pode causar ao seu negócio.

Em Portugal, quase metade das empresas das 641 empresas inquiridas no âmbito do Relatório Economia 2022 desenvolvido pelo CNCS, identifica que a principal entrave à implementação de mais e melhores sistemas de proteção contra ciberameaças é o custo das mesmas e dos recursos a alocar[169].

A implementação da cibersegurança numa PME envolve normalmente várias despesas. Os custos específicos podem variar consoante a sua dimensão, a sua

[166] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision support systems, 86, 13-23. https://doi.org/10.1016/j.dss.2016.02.012.
[167] Ibidem.
[168] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580. https://doi.org/10.1016/j.dss.2021.113580.
[169] CNCS (Maio, 2022). "*Relatório Economia 2022*", disponível em https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf

infraestrutura existente, os requisitos do sector e o nível de cibersegurança pretendido. Algumas das despesas comuns a considerar são:[170]

- Custos de tecnologia: o investimento nas últimas tecnologias de cibersegurança, tais como *firewalls*, sistemas de deteção de intrusão e software de encriptação, pode ser caro. Além disso, o custo de manutenção e atualização destas tecnologias pode somar-se ao longo do tempo.
- Formação dos funcionários: garantir que os funcionários estejam conscientes dos riscos da cibersegurança e saibam lidar com dados sensíveis pode exigir um investimento significativo em programas de formação e educação.
- Custos de conformidade: muitas indústrias estão sujeitas a regulamentos rigorosos de proteção de dados e privacidade, tais como RGPD e o NISD, que podem exigir investimento adicional em conformidade e relatórios.
- Custos de terceirização: algumas empresas podem optar por externalizar as suas necessidades de cibersegurança a fornecedores terceiros, o que também pode ser dispendioso.

A urgência de alertar e sensibilizar as PMEs é de cabal importância, uma vez que estas empresas representam 99,9% do tecido empresarial português[171] e 99% do tecido empresarial europeu na Europa.[172] Como tal, e de forma a alcançar um quadro de cibersegurança uniforme e eficaz, há que abranger todos os vértices da economia, principalmente aqueles que têm uma maior presença e impacto a nível global.

Outro dado importante que pode ser retirado do estudo elaborado pelo supracitado relatório de Economia do Centro Nacional de Cibersegurança revela que mais de 40% das pequenas empresas (41,6%) dedicam menos de 3.000 euros anuais às funções de cibersegurança, enquanto que apenas 24,8% das empresas médias possuem orçamentos inferiores a esse limiar. Sendo que em apenas 7,2% das pequenas empresas e em 4,3%

[170] IBM Security (2023). "*Cost of a Data Breach Report 2023*" https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

[171] PORDATA (2023). "*Pequenas e médias empresas em % do total de empresas: total e por dimensão*" https://www.pordata.pt/portugal/pequenas+e+medias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimensao-2859

[172] "A*s micro, pequenas e médias empresas (PME) constituem 99 % das empresas na UE. São responsáveis por dois em cada três empregos no setor privado e contribuem para mais de metade do valor acrescentado total criado pelas empresas na UE."* Cordina, Corinne (Abril, 2023). "*Fichas temáticas sobre a União Europeia: Pequenas e médias empresas.*" https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/pt/FTU_2.4.2.pdf

das médias não existe qualquer orçamento para funções de cibersegurança. Por sua vez, "*Mais de metade das empresas médias (53,9%) têm um orçamento de cibersegurança superior a 3.000 euros; 18,4% entre 3.000 e 8.000 euros; 12,8% entre 8.000 e 15.000 euros; e, 14,9% entre 15.000 e 50.000. Só 7,8% das empresas médias dedicam mais de 50.000 euros a cibersegurança."*

Já nas pequenas empresas*, "o investimento anual em cibersegurança é superior a 3.000 euros em menos de 30% das empresas (29,8%). O orçamento em cibersegurança só é superior a 50.000 euros em uma em cada cem empresas."*

Não obstante o custo da implementação e da prevenção de medidas de cibersegurança, há que ter também em consideração o custo de um ciberataque, que em certos casos, pode ultrapassar largamente o investimento na prevenção de ciberataques.

O custo de um ciberataque contra uma empresa é muito difícil de determinar, uma vez que os danos atingem diversos vértices da atividade económica da empresa e não existe um histórico de danos que permita estimar, com segurança, o valor objetivo do custo de um ciberataque. Porém, de acordo com o estudo publicado no relatório anual "*Cost of a Data Breach de IBM Security*"[173,174,175], o custo médio global em 2022 de um acesso indevido a dados ascende já a 4,35 milhões de dólares para as empresas.[176], incluindo perda de receitas, danos à reputação, taxas legais, e contraordenações legais.

Atendendo ao gráfico na Figura 8, os ataques à indústria hospitalar e de cuidados de saúde são os que têm um custo mais elevado.

---

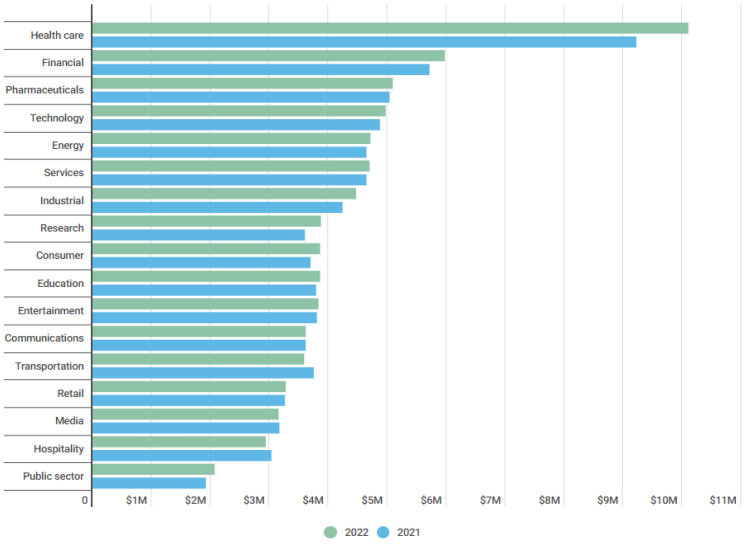
[173] O relatório de 2022, o 17.º anual da IBM, baseia-se em 3600 entrevistas a 550 organizações, em 17 países e regiões e em 17 setores, que foram afetadas por violações de dados entre Março de 2021 e Março de 2022. Nos Estados Unidos, o custo médio de uma violação de dados foi ainda mais elevado, atingindo 9,44 milhões de dólares em 2022. A seguir aos Estados Unidos, o Médio Oriente (7,46 milhões de dólares), o Canadá (5,64 milhões de dólares), o Reino Unido (5,05 milhões de dólares) e a Alemanha (4,85 milhões de dólares) apresentaram os custos mais elevados das violações de dados, IBM Security (2023). "*Cost of a Data Breach Report 2023*" https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

[174] Barati, M., & Yankson, B. (2022). Predicting the occurrence of a data breach. *International Journal of Information Management Data Insights*, *2*(2), 100128.

[175] Almulihi, A. H., Alassery, F., Khan, A. I., Shukla, S., Gupta, B. K., & Kumar, R. (2022). Analyzing the Implications of Healthcare Data Breaches through Computational Technique. *Intelligent Automation & Soft Computing*, *32*(3).

[176] Este relatório teve como base de referência o custo com as despesas de quatro áreas de atividades associadas a incidentes de violação de dados em organizações: deteção e agravamento, notificação, resposta pós violação e lucros cessantes.

Figura 8 - Custo médio de violação de dados em 2021 e 2022 por setor



Fonte: *IBM Security (2023). "Cost of a Data Breach Report 2023"* *https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs*

Os hospitais dependem fortemente de sistemas e redes interligados para prestar serviços de saúde de forma eficaz. Estes sistemas incluem registos de saúde eletrónicos, dispositivos médicos, equipamento de diagnóstico, ferramentas de comunicação, entre outros. A natureza interligada destes sistemas aumenta o potencial de agentes mal-intencionados explorarem as vulnerabilidades do sistema. Para além dos danos financeiros e digitais que os hospitais possam sofrer, os principais danos resultantes de um ciberataque poderão ter um impacto direto na saúde de utentes e chegar mesmo a custar vidas humanas, uma vez que, ocorrendo um ciberataque que provoque uma eventual paragem dos serviços pode levar a atrasos nos cuidados aos utentes, ao cancelamento de cirurgias, reencaminhamento de doentes, perda do acesso aos registos de saúde eletrónico, podendo desencadear uma situação de calamidade pública.

6. Falta de incentivos públicos

A falta de incentivos públicos para que as empresas adotem sistemas de cibersegurança fortes é outro desafio. Embora os governos e outras organizações públicas tenham tomado medidas para encorajar as empresas a dar prioridade à cibersegurança, tais como através de regulamentos e directrizes, muitas vezes existe pouco apoio financeiro ou incentivos para o fazer. Isto pode tornar difícil para as empresas,

particularmente as mais pequenas, justificar os custos de implementar medidas fortes de cibersegurança.

Na União Europeia, em 2023, as despesas públicas no âmbito da cibersegurança situam-se entre mil e dois mil milhões de euros,[177] enquanto nos EUA, em 2023, este as despesas ascendem a aproximadamente 10,8 mil milhões de dólares[178], tendo em 2020 ocorrido o maior investimento de 18.79 mil milhões de dólares.[179]

Existem, no entanto, iniciativas tomadas por alguns governos para abordar esta questão:

- Créditos fiscais de cibersegurança: Alguns governos oferecem créditos fiscais a empresas que investem em medidas de cibersegurança. Por exemplo, o estado americano de Maryland oferece um crédito fiscal de até $50.000 doláres por ano para empresas que adquirem e implementam tecnologias de cibersegurança qualificadas. Dentro da EU, destaca-se o exemplo dado por Espanha que oferece créditos fiscais até 40% para empresas que invistam em tecnologias e serviços de cibersegurança.
- Subsídios e programas de financiamento: Muitos governos e organizações públicas oferecem subsídios e programas de financiamento para ajudar as empresas a melhorar a sua cibersegurança. Por exemplo, o governo britânico atribuiu 1,9 mil milhões de libras ao "*National Cyber Security Programme*", que fornece financiamento e apoio a iniciativas de cibersegurança.
- Programas de financiamento da UE: O Programa Europa Digital 2021-2027 trata-se de um programa de investimento de cerca de 7 mil milhões de euros para apoiar a investigação e inovação em matérias digitais, incluindo a cibersegurança. Este programa fornece apoio financeiro à administração pública, empresas e particulares, e, ainda, organizações de investigação, graças a este programa de

[177] Na União Europeia o "*Digital Europe Programme*", ou em português "*O Programa Europa Digital 2021-2027* "é o primeiro programa de financiamento da UE centrado em levar a tecnologia digital às empresas e aos cidadãos. Com um orçamento total previsto de 7,5 mil milhões de euros para 7 anos. Este programa teve início em 2021, e foi criado pelo Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29 de Abril de 2021, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32021R0694, Documento 32021R0694

[178] WhiteHouse, "*Cybersecurity budget fiscal year 2022: INFORMATION TECHNOLOGY AND CYBERSECURITY FUNDING*" https://www.whitehouse.gov/wp-content/uploads/2022/03/ap_16_it_fy2023.pdf

[179] USA.gov, Government Information, "*Cybersecurity budget fiscal year 2020: CYBERSECURITY FUNDING*" https://www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf

investimento foi possível desenvolver outras ações, desde logo o Horizon Europe.[180]

- Ferramentas e recursos cibernéticos de segurança gratuitos: A UE fornece gratuitamente ferramentas e recursos de cibersegurança às empresas, particularmente às PME. A ENISA fornece um repositório de ferramentas e recursos, tais como orientação e normas de segurança cibernética, para ajudar as empresas a melhorar a sua postura de segurança cibernética.

7. STUXNET – Irão "o primeiro cibermíssil teleguiado"

O rápido desenvolvimento da tecnologia trouxe muitos benefícios à sociedade, mas também criou novos perigos, especialmente no domínio da guerra cibernética.

Até há pouco tempo ninguém imaginaria que um conjunto de indivíduos reunidos num quarto munidos com os seus computadores fossem capazes de lançar ataques capazes provocar um impacto negativo na economia de um país ou até provocar a perda de vidas humanas. Alarmados por este risco iminente, Governos em todo o mundo tomaram ação e têm vindo a investir somas incalculáveis de dinheiro de forma a criar infraestruturas resilientes que possam prevenir e combater esta ameaça dos tempos modernos.

Um dos primeiros casos registados deste tipo de ataques contra uma Nação, foi o caso do "STUXNET" no Irão em 2010, qualificado como "o primeiro cibermíssil teleguiado", destinado a sabotar ou destruir infraestruturas críticas, tais como centrais elétricas ou nucleares.

O malware "STUXNET" foi desenvolvido especificadamente para atacar o sistema operacional SCADA desenvolvido pela Siemens utilizado para controlar as centrífugas de enriquecimento de urânio iranianas. A infeção terá sido transmitida por via de uma pen ou um CD e ter-se-á propagado por todo o sistema da central nuclear. O *worm* foi desenvolvido tendo em vista duas funções. A primeira delas era fazer com que as centrífugas iranianas começassem a girar 40% mais rapidamente por quinze minutos, o

[180] Os programas de investigação do Horizonte 2020 da UE atribuíram cerca de 600 milhões de euros a projetos relativos à cibersegurança e à cibercriminalidade no período de 2014-2020, incluindo 450 milhões de euros para a PPPc para a cibersegurança para 2017-2020, com o objetivo de atrair mais 1,8 mil milhões de euros do setor privado, criado pelo Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho de 28 de Abril de 2021 que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021R0695 , Documento 32021R0695

que causava brechas nas centrífugas de alumínio. A segunda forma, inicialmente gravava dados telemétricos de uma típica operação normal das centrífugas nucleares, sem que o alarme soasse, para depois reproduzir esse registo junto dos operadores dos equipamentos de forma a que não se apercebessem de nenhum funcionamento anormal enquanto as centrífugas eram progressivamente danificadas.[181]

Aquando do ataque, Evgueni Kaspersky, especialista russo de segurança de uma das mais reputadas empresas de produção de softwares de segurança, frisa o caráter inédito do "cibermíssil" Stuxnet. "*O seu fim não é roubar dinheiro, enviar spam, desviar dados pessoais. Foi concebido para sabotar e danificar sistemas industriais. É um ponto de viragem que nos fez entrar num novo mundo. Na década de 90 havia cibervândalos e, na de 2000, cibercriminosos. Entramos na década do ciberterrorismo, das ciberarmas e das ciberguerras*.[182](tradução nossa)"

O "STUXNET" marcou indelevelmente a entrada num novo paradigma onde os Governos entenderam que a Segurança Nacional vai além do território terreste, marítimo e aéreo, sendo também necessário proteger o território digital. Este ataque demonstrou também a vulnerabilidade das infraestruturas críticas a ciberataques e as suas potenciais consequências. A paralisação de infraestruturas essenciais para o funcionamento da sociedade moderna, tais como: redes elétricas, sistemas de transporte, instituições bancárias e serviços de saúde pode provocar repercussões devastadoras.

Por exemplo, um ataque a uma rede elétrica poderia levar a apagões que não só perturbariam a vida quotidiana, deixando casas sem luz, sem eletricidade e sem aquecimento, como também teria graves consequências económicas uma vez que sem eletricidade as empresas e fábricas não podem funcionar. A perda de energia poderia ainda levar ao encerramento de sistemas críticos, tais como hospitais, serviços de emergência e estações de tratamento de água, colocando em risco vidas humanas.

Da mesma forma, um ataque cibernético aos sistemas de transporte, tais como companhias aéreas ou ferroviárias, poderia causar caos e perturbações graves dado que a Maioria das pessoas e empresas depende do transporte, quer se trate de chegar ao trabalho a tempo, enviar bens ou receber material médico. Se, por hipótese, um ataque perturbar

---

[181] J.Broad, William, et al. (2011, Janeiro) "*Israeli Test on Worm Called Crucial in iran Nuclear Delay).* The New York Times. Disponível em https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[182] Kapersky (2010, Setembro). "*Kaspersky Lab provides its insights on Stuxnet worm*". Corporate News. *https://www.kaspersky.com/about/press-releases/2010_kaspersky-lab-provides-its-insights-on-stuxnet-worm*

as operações de transporte e logística, cadeias inteiras de abastecimento podem ser interrompidas.[183] A perturbação do sistema de semáforos ou do transito ferroviário pode causar danos físicos graves.[184,185]

Ataques cibernéticos a instituições financeiras podem ter consequências imediatas como resultar no roubo de dados pessoais, mas pode ainda ter consequências mais gravosas e duradouras levando a cenários de instabilidade económica. [186] Como referiu Christine Lagarde em 2020, enquanto presidente do Banco Central Europeu, exortando a necessidade de investir em estruturas complexas de segurança; e, como um ataque cibernético pode provocar uma crise de liquidez nas instituições, podendo colocar em risco a sobrevivência da instituição financeira e colocar em causa o seu importante papel no financiamento da economia e das famílias, originado, consequentemente, custos económicos elevadíssimos e uma quebra de confiança junto do público, possivelmente, irremediável.[187]

Aqui chegados, é possível constatar que o impacto dos ciberataques pode influenciar a dinâmica do poder entre países. Um país ou uma organização com capacidades cibernéticas avançadas pode utilizá-los para obter vantagens estratégicas sobre outros países. Além disso, os ciberataques também podem ser utilizados para roubar dinheiro directamente, através de táticas como a fraude bancária online ou ataques de resgates. Os *hackers*, ou *crakers*, podem também utilizar ataques para perturbar as operações comerciais e causar perdas financeiras a empresas e organizações.

Acresce que, os ataques cibernéticos a infraestruturas críticas podem ter efeitos que perduram no tempo, uma vez que podem causar danos permanentes a infraestruturas

[183] ENISA. (Março, 2023) "ENISA *Threat landscape: transport sector* (January 2021 to October 2022" MARCH 2023 disponível em https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape/@@download/fullReport

[184] Ibidem.

[185] Li, Z., & Shahidehpour, M. (2017). Deployment of cybersecurity for managing traffic efficiency and safety in smart cities. The Electricity Journal, 30(4), 52-61. https://doi.org/10.1016/j.tej.2017.04.003

[186] Em Fevereiro de 2016, s hackers atacaram digitalmente o banco central do Bangladesh e exploraram vulnerabilidades no SWIFT, que é o sistema de comunicação que liga bancos de todo o mundo para transações e pagamentos financeiros internacionais rápidos e seguros, tentando roubar mil milhões de dólares. Embora a Maioria das transacções tenha sido bloqueada, ainda assim desapareceram cerca de 81 milhões de dólares. O "assalto" foi um alerta para o mundo financeiro de que os riscos cibernéticos no sistema financeiro tinham sido severamente subestimados e que precisavam de ser considerados com outra seriedade. Fonte, Reuters (2016) "*Empresas de cibersegurança afirmam que hackers que invadiram BC de Bangladesh atacaram outros bancos"* disponível em https://www.reuters.com/article/tech-hackers-bc-idBRKCN0YI1PY,

[187] Maurer,T. & Nelson, Arthur. (2021) "*The Global Cyber Threat".* International Monetary Fund https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

físicas ou levar à perda de dados que podem levar anos a recuperar. O processo de recuperação pode ser dispendioso e demorado, e pode nem sempre ser possível restaurar totalmente os sistemas ao seu estado anterior.

Tudo isto nos leva a compreender que, os ataques cibernéticos a infraestruturas críticas constituem uma ameaça significativa à nossa sociedade, sendo essencial que os governos e as organizações tomem medidas robustas para proteger estes sistemas. Ao investir em medidas de cibersegurança e ao desenvolver estratégias de resposta eficazes, é possível minimizar o impacto dos ataques cibernéticos e proteger a segurança das infraestruturas críticas bem como o bem-estar dos cidadãos.

CAPÍTULO 4 – Possíveis Soluções

1. Soluções adotadas pela União Europeia

A União Europeia tem trabalhado ativamente em políticas de cibersegurança para garantir a segurança da sua infraestrutura digital e para proteger a privacidade e os dados pessoais dos seus cidadãos. Uma das estratégias mais relevantes a salientar em matéria de segurança do ciberespaço é a Estratégia da UE para a União da Segurança[188]. Este plano foi apresentado pela Comissão Europeia a 24 de Julho 2020 e assenta sobre quatro pilares estratégicos: terrorismo e crime organizado; ambiente de segurança a longo prazo; ecossistema de segurança sólido; e, fazer face a ameaças em permanente evolução. De forma global, o principal objectivo é reforçar a segurança e promover a cooperação entre os Estados Membros da UE na abordagem aos desafios de segurança comuns.

A Cibersegurança surge associada ao pilar "Ambiente de Segurança a Longo prazo"[189], contudo, é inegável que a cibersegurança é indissociável de qualquer atividade, quer do combate ao terrorismo e crime organizado, quer da construção de um ecossistema europeu de segurança sólido.

A ideia da criação de uma União de Segurança não é desconhecida dos dirigentes europeus, constante na base de que nenhum Estado sozinho é capaz de fazer face aos desafios de segurança que se impõem no mundo tecnológico moderno. O conceito de União da Segurança surgiu pela primeira vez numa comunicação da Comissão Europeia de 2016 visando abrir o caminho para uma União da Segurança genuína e eficaz.[190]

Este conceito foi desenvolvido com base na Agenda Europeia para a Segurança de 2015[191] - que teve como objetivo melhorar a aplicação da lei e a resposta judicial á cibercriminalidade, principalmente através da renovação ou atualização das políticas e da legislação em vigor - e propôs uma nova abordagem baseada na responsabilidade

---

[188] COMISSÃO EUROPEIA (Julho, 2020), "*Comunicação Da Comissão Ao Parlamento Europeu, Ao Conselho Europeu, Ao Conselho, Ao Comité Económico E Social Europeu E Ao Comité Das Regiões Sobre A Estratégia Da Ue Para A União Da Segurança"* disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0605

[189] Ibidem.

[190] COMISSÃO EUROPEIA (Abril 2016). *"Comunicação Da Comissão Ao Parlamento Europeu, Ao Conselho Europeu E Ao Conselho Dar Cumprimento À Agenda Europeia Para A Segurança Para Combater O Terrorismo E Abrir Caminho À Criação De Uma União Da Segurança Genuína E Eficaz". https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52016DC0230&from=DA*

[191] COMISSÃO EUROPEIA (Maio, 2015) "*Agenda Europeia para a Segurança*". https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM:2015:0185:FIN, Documento 52015DC0185

partilhada entre a União Europeia e os Estados Membros da UE. Para liderar o Plano de Execução com vista a implementar as medidas da Agenda Europeia para a Segurança de 2015[192], foi criada em Setembro de 2016, uma pasta específica de comissário da União da Segurança, que contou com a assistência de um grupo de trabalho que reuniu os conhecimentos especializados de toda a Comissão Europeia.

No âmbito de todo este contexto estratégico, em 16 de Dezembro de 2020, foi apresentado em conjunto pela Comissão Europeia e pelo Serviço Europeu de Ação Externa, a "Nova Estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais"[193], que "*visa reforçar a resiliência coletiva da Europa(…)",* promovendo a cooperação intergovernamental em matéria de cibersegurança, "(…) *contra as ciberameaças e contribuir para garantir que todos os cidadãos e todas as empresas possam beneficiar plenamente de serviços e ferramentas digitais seguros e fiáveis.*"[194]

Esta nova Estratégia para a Cibersegurança propõe implementar a cibersegurança em todos os elementos da cadeia de abastecimento e agrupar ainda mais as atividades e os recursos da UE nas quatro comunidades de cibersegurança: mercado interno, aplicação da lei, diplomacia e defesa[195]. Para tal, a concretização desta estratégia está estruturada em torno de três eixos fundamentais:

a) Resiliência, soberania tecnológica e liderança (proposta da Diretiva SRI 2; construção de um "escudo para a cibersegurança" europeu que permita a deteção antecipada de ciberataques);
b) Reforço da capacidade operacional para prevenir, dissuadir e reagir (criação de uma ciberunidade conjunta envolvendo organismos da UE e autoridades nacionais responsáveis pela prevenção, dissuasão e resposta a ciberataques);

[192] CONSELHO DA UNIÃO EUROPEIA (2016). "Implementation Plan on Security and Defence*"* *https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf, 14392/16*
[193] COMISSÃO EUROPEIA (Dezembro, 2020) "*Joint Communication To The European Parliament And The Council The Eu's Cybersecurity Strategy for the Digital Decade"* https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, Documento 52020JC0018
[194] Ilbidem
[195] COMISSÃO EUROPEIA (Dezembro, 2020). "*Nova Estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais"* https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391

c) Promoção de um ciberespaço à escala mundial aberto através do reforço da cooperação com os parceiros internacionais da UE (intensificação de colaboração com parceiros internacionais, desenvolvimento de ciberdiplomacia).

A nova Estratégia de Cibersegurança da UE para a Década Digital constitui um componente essencial do Programa Europa Digital (DIGITAL)[196], do Plano de Recuperação da Comissão para a Europa[197] e da Estratégia da União de Segurança 2020-2025[198].

Além das iniciativas referenciadas cumpre ainda fazer uma menção a outra Estratégia da UE que também aborda questões relacionadas com a cibersegurança, a Estratégia para o Mercado Único Digital (2015)[199], que visa melhorar o acesso a bens e serviços digitais: para este efeito, é essencial reforçar a segurança, a confiança e a inclusão em linha; (rever texto), repeti Agenda Europeia para a Segurança"

2. Joint Cyber Unit

Como já foi referido, um dos principais papéis da ENISA no contexto da UE é o de apoiar a cooperação operacional entre Estados Membros, Instituições da União, Órgãos, Gabinetes e Agências. Para além disso, a ENISA está também mandatada para assegurar a existência de um quadro de cooperação eficaz entre os intervenientes operacionais no seio da União em caso de ciberataques e crises transnacionais em grande escala. Ao coordenar tanto o secretariado do UE CyCLONe[200] como a Rede CSIRTs, a ENISA tem como missão sincronizar os níveis técnicos e operacionais de todos os intervenientes envolvidos na UE para colaborar e responder a incidentes e crises em larga

[196] Para a execução deste programa está previsto um orçamento de 7.6 mil milhões de euros, e tem como principal objetivo a aceleração e transformação digital da indústria e administração pública, em benefício dos cidadãos, empresas e estado.

[197] COMISSÃO EUROPEIA (2023). *"Plano de Recuperação Europeia"* https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_pt

[198] Comunicação Da Comissão Ao Parlamento Europeu, Ao Conselho Europeu, Ao Conselho, Ao Comité Económico E Social Europeu E Ao Comité Das Regiões Sobre A Estratégia Da Ue Para A União Da Segurança. Documento 52020DC0605, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0605

[199] Comissão Europeia, *Estratégia para o Mercado Único Digital na Europa*, COM (2015) 192 final, de 6 de Maio de 2015.

[200] "*A CyCLONe é a Rede de Organização de Ligação para Crises do Ciberespaço da UE22. Foi criada em 2020 no âmbito do Programa HORIZON 2020, tendo como objetivo contribuir para a implementação do Plano da Comissão Europeia para uma resposta de emergência rápida em caso de incidente ou crise cibernética em grande escala.*" CNCS "Relatório Cibersegurança em Portugal. *Políticas Públicas.*" https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriociberseguranca-cncs.pdf, a este propósito consultar também https://cyclone-project.eu/ .

escala, fornecendo as melhores ferramentas e apoio. Porém, apesar dos grandes progressos alcançados, ainda não existe uma plataforma comum na UE onde as informações recolhidas em diferentes comunidades de cibersegurança possam ser trocadas de forma eficiente e segura e onde as capacidades operacionais possam ser coordenadas e mobilizadas pelos atores relevantes. Consequentemente, ameaças e incidentes de cibersegurança correm o risco de ser tratados com eficiência limitada e vulnerabilidade acrescida.

De forma a dar resposta a todas estas limitações, tornou-se imperativa a criação de uma entidade que suprisse esta necessidade, surgindo assim a Joint Cyber Unit.[201]

A *Joint Cyber Unit* "*Deverá tirar partido e acrescentar valor às estruturas, recursos e capacidades existentes enquanto plataforma para uma cooperação operacional e técnica segura e rápida entre as entidades da UE e as autoridades dos Estados-Membros. Deve também reunir todas as comunidades de cibersegurança, ou seja, civis, policiais, diplomáticas e de defesa*."[202]

Joint Cyber Unit funcionará como um elemento central de coordenação entre: Agência da União Europeia para a Cibersegurança (ENISA); Equipa de Resposta Informática de Emergência para as instituições, organismos e agências da UE (CERT-EU); Centro Europeu de Cibercriminalidade da Europol (EC3); Equipas Nacionais de Resposta a Incidentes de Segurança Informática (CSIRTs); Rede de Organizações Cibernéticas de Ligação de Crise da UE (CyCLONe); Serviço Europeu para a Acção Externa (SEAE); Agência Europeia de Defesa (EDA), e outros. A sua construção será desenvolvida através de um processo gradual composto por 4 etapas, o objectivo é assegurar que esta Ciberunidade Conjunta passe à fase operacional até 30 de Junho de 2022 e que seja plenamente estabelecida até 30 de Junho de 2023.

3. Centro Europeu de Competências

Após o início da execução desta nova e atualizada Estratégia de Cibersegurança para a UE, tornou-se evidente a necessidade da criação de uma plataforma que interligasse

[201] COMISSÃO EUROPEIA (Julho 2021) *"RECOMENDAÇÃO (UE) 2021/1086 DA COMISSÃO de 23 de Junho de 2021 relativa à criação de uma Ciberunidade Conjunta"* https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021H1086, L 237/1

[202] Considerando n.º 9 da COMISSÃO EUROPEIA (Julho 2021) *"RECOMENDAÇÃO (UE) 2021/1086 DA COMISSÃO de 23 de Junho de 2021 relativa à criação de uma Ciberunidade Conjunta"* https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021H1086, L 237/1

Instituições, agências, organismos e autoridades nacionais dos Estados Membros para prevenir, dissuadir e responder a ciberataques. Como tal, foi desenvolvido o Centro Europeu de Competências em Cibersegurança (ECCC)[203], com sede em Bucareste, tem por objetivo reforçar as capacidades europeias em matéria de cibersegurança, proteger a economia e a sociedade dos ciberataques, manter e promover a excelência da investigação e reforçar a competitividade da indústria da União neste domínio.[204]

Ao contrário das equipas de respostas de incidentes de segurança informática, como os CSIRT, o ECCC não desempenhará tarefas operacionais de cibersegurança. A principal missão do ECC, em conjunto com a Rede de Centros Nacionais de Coordenação[205], é desenvolver uma agenda comum de investimento, nos Estados Membros da UE, no âmbito na investigação, tecnologia e desenvolvimento industrial no domínio da cibersegurança, agregar recursos e canalizar investimentos para executar projetos e iniciativas relevantes.[206]

O Centro de Competências deverá gerir o apoio financeiro relacionado com a cibersegurança ao abrigo do Horizonte Europa – Programa-Quadro de Investigação e Inovação («Horizonte Europa»), criado pelo Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho[207], e do Programa Europa Digital, criado pelo Regulamento (UE)

[203] The European Cybersecurity Competence Centre (2023). *"European Cybersecurity Competence Centre and Network."*, disponível em https://cybersecurity-centre.europa.eu/index_en

[204] COMISSÃO EUROPEIA. "*Comissão congratula-se com o acordo político sobre o Centro e a Rede de Competências em matéria de Cibersegurança*" https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2384, IP/20/2384

[205] Considerando n.º 25 do 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 e a Rede de Centros Nacionais de Coordenação "*A Rede deverá ser constituída por um centro nacional de coordenação de cada Estado-Membro. Os centros nacionais de coordenação que tenham sido reconhecidos pela Comissão como tendo a necessária capacidade de gerir os fundos de modo a cumprirem a missão e os objetivos estabelecidos no presente regulamento, deverão receber apoio financeiro direto da União, nomeadamente subvenções concedidas sem convite à apresentação de propostas, a fim de efetuarem as suas atividades relacionadas com o presente regulamento.*» https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021R0887&from=PT, Documento 32021R0887

[206] Considerando n.º 14 do 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 e a Rede de Centros Nacionais de Coordenação https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021R0887&from=PT

[207] Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho, de 28 de Abril de 2021, que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação, que define as suas regras de participação e difusão, e que revoga os Regulamentos (UE) n.o 1290/2013 e (UE) n.o 1291/2013 (JO L 170 de 12.5.2021), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021R0695 Documento 32021R0695

2021/694 do Parlamento Europeu e do Conselho[208], devendo ainda estar aberto a outros programas que de futuro venham a ser implementados. Esta abordagem deverá contribuir para criar sinergias e coordenar o apoio financeiro relacionado com iniciativas da União em matéria da investigação e desenvolvimento, da inovação, da tecnologia e do desenvolvimento industrial no domínio da cibersegurança e deverá evitar uma duplicação desnecessária.[209]

4. Compliance e gestão de riscos

Na acessão da norma de Gestão de Risco ISO 31000:2018, o risco é definido como o evento, situação ou circunstância futura com probabilidade de ocorrência e potencial consequência positiva ou negativa na consecução dos objetivos de uma unidade organizacional.

Sobre a perceção dos riscos decorrentes das ameaças digitais é de salientar o estudo realizado pela Marsh em parceria com a Microsoft a 1.300 executivos de todo o mundo, a Fevereiro de 2018, que revelou que 70% dos membros dos conselhos da administração classificam as ameaças digitais, ou o ciberrisco, como uma das principais preocupações, e, mais surpreendente ainda, foi o facto de apenas 14% ter referido que estavam muito confiantes na capacidade de resposta das suas empresas.[210]
Atualmente, esse mesmo estudo foi atualizado, tendo 19% dos executivos respondido que estavam muito confiantes na capacidade de resposta a um ciberincidente. Adicionalmente, o novo estudo apresenta novos indicadores que são úteis para fazer um exercício de retrospetiva.

Desde logo, as empresas identificam os ciberataques como um dos principais riscos e fazem referência às consequências dos impactos dos últimos três anos de perturbações constantes no local de trabalho, da crescente transformação digital e dos

[208] Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29 de Abril de 2021, que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32021R0694 , Documento 32021R0694
[209] Considerando n.º 14 do 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 e a Rede de Centros Nacionais de Coordenação https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021R0887&from=PT
[210] MARSH & MICROSOFT (Fevereiro 2018). "*By the Numbers: Global Cyber Risk Perception Survey" https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20Microsoft%20Global%20Cyber%20Risk%20Perception%20Survey%20February%202018.pdf*

recorrentes ataques de *ransomware* e da forma como abalaram fortemente a confiança dos líderes das empresas na sua capacidade de gerir o risco cibernético, referindo mesmo que não estão mais confiantes do que estavam há dois anos atrás. Esta é uma das conclusões do *2022 Marsh and Microsoft Cyber Risk Survey*, a terceira colaboração deste género que as empresas articularam nos últimos quatro anos.[211]

Contudo, existem outros dados que indicam que houve uma melhoria nas medidas adotadas pelas empresas para diminuir os riscos de exposição a ameaças cibernéticas, por exemplo, 79% das empresas inquiridas revelam que têm implementado um plano de resposta a ciberincidentes e revelam também que tem havido um maior envolvimento de dos profissionais de IT e Cibersegurança com a gestão de topo e acionistas.

Nestas circunstâncias, estamos perante uma realidade indissociável da atividade desenvolvida pelas instituições, na qual, não sendo eliminàveis, os riscos têm de ser identificados, comunicados, aceites, categorizados e geridos através de planos eficientes, eficazes e adaptados à realidade organizativa e funcional da instituição.

No contexto da Segurança da Informação e Cibersegurança, o modelo de gestão do risco operacional nas empresas deve ter como finalidade proteger o valor, melhorar o desempenho, apoiar na tomada de decisão, promover a inovação e suportar a consecução dos objetivos, propiciando a mitigação das situações que possam expor a organização a riscos de incidentes de cibersegurança e/ou violação de dados.[212]

A gestão de riscos na cibersegurança é o processo de identificação, avaliação, priorização de potenciais riscos para os sistemas de informação e dados da organização, e a implementação de medidas para reduzir esses riscos para um nível aceitável. Envolve um ciclo contínuo de avaliação, implementação, e monitorização dos controlos de segurança.

[211] Marsh & Microsoft (2022). "2022 Global Cyber Risk Survey" https://www.marsh.com/ug/services/cyber-risk/insights/global-cyber-risk-survey.html

[212] Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), 81-85. https://doi.org/10.1145/636772.636774

As etapas envolvidas na gestão de riscos de cibersegurança incluem tipicamente[213]:

1. Avaliação dos riscos: Identificação e avaliação dos impactos potenciais das ameaças e vulnerabilidades de segurança;
2. Priorização do risco: Determinação dos riscos que representam a maior ameaça para a organização e requerem atenção imediata;
3. Gestão dos riscos: Identificação e implementação de medidas para eliminar ou mitigar o impacto ou probabilidade de ocorrência dos riscos, tais como a implementação de sistemas de deteção de intrusão ou encriptação de dados;
4. Monitorização e revisão: Monitorizar e rever regularmente a eficácia das medidas de atenuação dos riscos e fazer os ajustamentos necessários.

Para empresas que estejam numa fase primária e queiram melhorar a sua estrutura de segurança da informação, um primeiro passo a tomar, poderá ser implementar um padrão (ou *standard)* internacional de segurança da informação, utilizados em várias indústrias e sectores para auxiliar as organizações a alinhar a sua atividade com as melhores práticas de segurança da informação.

Alguns destes *standards* utilizados como ponto de partida são, a ISO 31000:2018, fornecendo orientações para a identificação e avaliação de riscos globais, enquanto outros, tal como a ISSO/IEC 27001 (Sistema de Gestão de Segurança da Informação)[214], ISO/IEC 27701 (Sistema de Gestão de Privacidade), ou a SOC 2 (Controles de Sistema e Organização), são utilizados para definir e implementar um conjunto de políticas, procedimentos, processos e sistemas que gerem os riscos de segurança da informação bem como da proteção de dados pessoais, decorrentes de ciberataques, exfiltração de dados ou outros atos maliciosos.

5. Plano de gestão e prevenção de riscos

É reconhecido que alguns elementos devem sempre constar nos planos de prevenção de riscos de modo a que cumpram os mínimos exigidos e se provem eficazes.

[213] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart, A review of cyber security risk assessment methods for SCADA systems, Computers & Security, Volume 56, 2016, Pages 1-27,https://doi.org/10.1016/j.cose.2015.09.009.

[214] International Organization fo Standardization (2022). "*ISO/IEC 27001, Information security management systems"* https://www.iso.org/standard/27001

Elementos como: uma estrutura interna de auditoria, avaliações periódicas, identificação e classificação dos riscos, plano de implementação de medidas de gestão de risco; são pontos transversais a qualquer plano de gestão de riscos.

No Guia disponibilizado pelo CNCS para auxiliar as entidades da Administração Pública, os operadores de infraestruturas críticas e de serviços essenciais, a cumprir com as exigências formais decorrentes do Artigo 10.º do Decreto-Lei n.º 65/2021 de 30 de Julho[215] – não descurando o cumprimento de outras peças de legislação nacional e internacional – são adotados alguns desses elementos, que tem por base algumas das melhores práticas e standards internacionais de gestão de riscos da Segurança da Informação e Cibersegurança.

Noutra mão, existem Standards Internacionais que podem ser seguidos para implementar sistemas de gestão de risco. A vantagem de seguir os *Standards* internacionais é que, segundo a ENISA, permitem "*alcançar uma maior coesão e harmonização da cibersegurança, apoia a promoção de um mercado único de produtos de cibersegurança e a segurança de todos os elementos das cadeias de fornecimento.*"

Desta forma, ao fazer a utilização de normas ISO, a gestão de riscos pode trazer diversas vantagens a nível de coesão e harmonização, mas também a nível de consistência, uma vez que as normas ISO fornecem uma abordagem consistente e estruturada à gestão do risco, independentemente da indústria ou sector em que uma organização opera.

Esta coerência permite às organizações estabelecer um entendimento e uma linguagem comum de conceitos e terminologias para a gestão do risco, facilitando a comunicação e a colaboração entre os diversos intervenientes.
Assim permite: [216, 217]

- Estar a par das melhores práticas uma vez que as normas ISO não são estáticas, estão em constante evolução para acompanhar os diversos desenvolvimentos

[215] Artigo 10º n.º.1 do Decreto-Lei n.º 65/2021 de 30 de Julho "- As entidades da Administração Pública e os operadores de infraestruturas críticas, bem como os operadores de serviços essenciais, devem realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, no caso dos operadores de serviços essenciais, também em relação aos ativos que garantam a prestação dos serviços essenciais (…)"
[216] Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176-185.
[217] INSTITUTO PORTUGUÊS DA QUALIDADE (2023). "*10 razões para usar Normas*". https://www.ipq.pt/normalizacao/a-importancia-da-normalizacao/razoes-para-o-uso-das-normas/

tecnológicos, de maneira que, a evolução das normas decorre da partilha de informações sobre a eficácia das medidas de cibersegurança em cenários do mundo real;

- facilita a entrada em novos mercados, a garantia de que os produtos estão conformes com normas e requisitos setoriais, facilita a entrada nos mercados nacionais e externos, uma vez que as normas são reconhecidas, compreendidas e respeitadas tanto nacional como internacionalmente, também enquanto suporte das atividades da avaliação da conformidade;
- diminui a margem do erro, pois ao implementar uma norma implica seguir uma metodologia e requisitos que foram analisados e ensaiados por peritos e que sugerem uma produção com menos erros de processos e menos desperdícios de tempo; e, entre outras vantagens,
- permite uma redução dos custos, uma vez que não terão de ser despendidos tempo e recursos no desenvolvimento e inovação de soluções, além do mais, o objectivo da utilização das normas é tornar a organização mais eficiente e rentável.

Em suma, as normas de padrão assentam as suas bases na coesão e harmonização das práticas de gestão de riscos para uma organização, proporcionando: consistência, estar a par das melhores práticas defendidas internacionalmente, oportunidades de conformidade e certificação, interoperabilidade e integração, e um enfoque na melhoria contínua, permitindo às organizações estabelecer processos eficazes de gestão do risco que sejam globalmente reconhecidos e aceites, levando a capacidades otimizadas de gestão do risco e a uma melhor resiliência organizacional.

5.1 Gestão de riscos Toyota

A gestão do risco de cibersegurança é importante porque auxilia as organizações a compreenderem a sua postura de segurança, a darem prioridade aos seus esforços e a atribuírem recursos de forma eficaz. Também ajuda as organizações a cumprir os requisitos legais, regulamentares e específicos da indústria relacionados com a proteção da informação. Ao gerir eficazmente os riscos de cibersegurança, as organizações podem melhorar a sua postura global de segurança, reduzir a probabilidade de um ataque bem-sucedido, e minimizar o impacto de quaisquer violações de segurança que possam ocorrer.

Um exemplo de um grupo multinacional de empresas que desenvolvem práticas para desenvolver nas suas organizações práticas de cibersegurança, é a Toyota, um dos maiores fabricantes mundiais de automóveis, que promove a implementação da "*All Toyota Security Guidelines*" (ATSG), para todas as empresas do *Toyota Motor Corporation*, sociedades subsidiárias e participadas, para assegurar uma abordagem consistente e coordenada da gestão da segurança ao longo de toda a cadeia de fornecimento da organização, funcionando como um mecanismo destinado a prevenir fugas de informação do interior e para responder a ataques cibernéticos que se estão a tornar cada vez mais sofisticados e complexos ao longo dos anos.[218] Esta diretriz interna resulta do cruzamento das melhores práticas de cibersegurança reconhecidas pela ISO 27001/27002, *NIST Cybersecurity Framework* (*National Institute of Standards and Technology*)[219], *The Ministry of Economy, Trade and Industry* ('METI'), entre outras. Tendo sido concebida para fornecer uma abordagem abrangente e padronizada à gestão da segurança em todas as operações globais da Toyota, com o objetivo de proteger os bens de informação da empresa e assegurar a confidencialidade, integridade, e disponibilidade dos seus dados e sistemas críticos.

O ATSG baseia-se nos princípios da gestão de risco e segue uma abordagem holística que engloba pessoas, processos e tecnologia. A sua abordagem abrange uma vasta gama de áreas de segurança, incluindo segurança da informação, segurança física, controlo de acesso, gestão de incidentes, continuidade de negócios, e gestão de terceiros, entre outras. Esta abordagem estruturada e abrangente para a gestão de riscos cibernéticos, inclui, entre outras coisas: Um quadro exaustivo para identificar, avaliar e mitigar os principais riscos de segurança; Divulgação de orientações sobre políticas, normas e procedimentos de segurança; monitorização contínua, medição e melhoria das medidas de segurança para se adaptar às ameaças e tecnológicas em constante evolução; e, envolvimento dos colaboradores através de ações de sensibilização e formação. É latente o esforço e o forte compromisso da liderança da Toyota com a segurança, e a promoção de uma cultura de segurança que valoriza a segurança informática como uma componente central das suas operações.

[218] Toyota. "*Privacy Initiatives"* https://global.toyota/en/sustainability/privacy/initiatives/
[219] National Institute Of Standards and Technology (NIST) (2023, Janeiro). "*NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework"* https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

Apesar de todos estes cuidados, a Toyota não se torna infalível a ataques cibernéticos, porém, torna-se, sem dúvida, muito mais resiliente na hipótese da ocorrência de um incidente de cibersegurança.

Exemplos como este e outros como o *Microsoft Security Development Lifecycle* (SDL), devem ser seguidos e adotados pelas empresas, pois só assim se poderá caminhar para um futuro com mais segurança, mais conhecimentos e infraestruturas mais resilientes aos impactos dos ataques cibernéticos.

6. White hat hackers

Os *White Hat Hackers* são especialistas em segurança informática que se especializam na identificação e correção de vulnerabilidades em sistemas informáticos, redes e aplicações de software. Utilizam os seus conhecimentos de técnicas de hacking para simular ataques aos sistemas de uma organização e, em seguida, comunicam as suas descobertas à organização para que esta possa corrigir as vulnerabilidades antes que os hackers maliciosos as possam explorar.

Segundo Eduardo Gelbstein é possível clarificar a distinção entre hackers maliciosos e hackers éticos. Os *White Hat Hackers* ou "*Hackers* Éticos" são os que usam as suas habilidades para identificar vulnerabilidades, com ou sem o consentimento dos proprietários dos sistemas. Por sua vez os *Black Hat Hackers* ou Crackers ou "*Hackers* Maliciosos" são os que têm a intenção de perturbação ou outras atividades maliciosas. [220]

Conforme verificado até agora, os ataques informáticos são uma ameaça constante e o custo de uma violação de dados pode ser devastador para uma empresa, como tal é necessário que as empresas assumam todas as medidas possíveis para que possam diminuir eficazmente os riscos e vulnerabilidades nesta matéria.

Os *Black Hat Hackers* e os *White Hat Hackers* utilizam as mesmas ferramentas para descobrir vulnerabilidades e explorá-las. Especialmente no que diz respeito à segurança das grandes empresas, esta corrida para encontrar falhas antes dos seus pares com más intenções é implacável. Uma vez que todos os dias aparecem novas

[220] Gelbstein, E. (2012). Protecting critical information infrastructures. Nação e defesa, 133, 128–146. http://hdl.handle.net/10400.26/42468

vulnerabilidades, a única coisa que se pode fazer para proteger contra as vulnerabilidades de dia zero é corrigir as falhas à medida que vão aparecendo.[221]

Como tal, ao saber que ferramentas e estratégias são aplicadas por um atacante significa que uma empresa pode defender-se repetindo os diferentes passos executados para comprometer a sua organização.[222] Os *White Hat Hackers* permitem fazer este tipo de trabalho, e, para além disso, também poderão auxiliar as empresas a implementar outras medidas de segurança preventivas e operacionais, através de procedimentos e formação, para fortalecer a resiliência da empresa. Nesta senda, a implementação de uma equipa de *White Hat Hackers* ou a sua consulta periódica, poderá grandemente beneficiar qualquer empresa que queira reforçar a sua integridade digital.

7. A perceção da cibersegurança pelas grandes empresas portuguesas

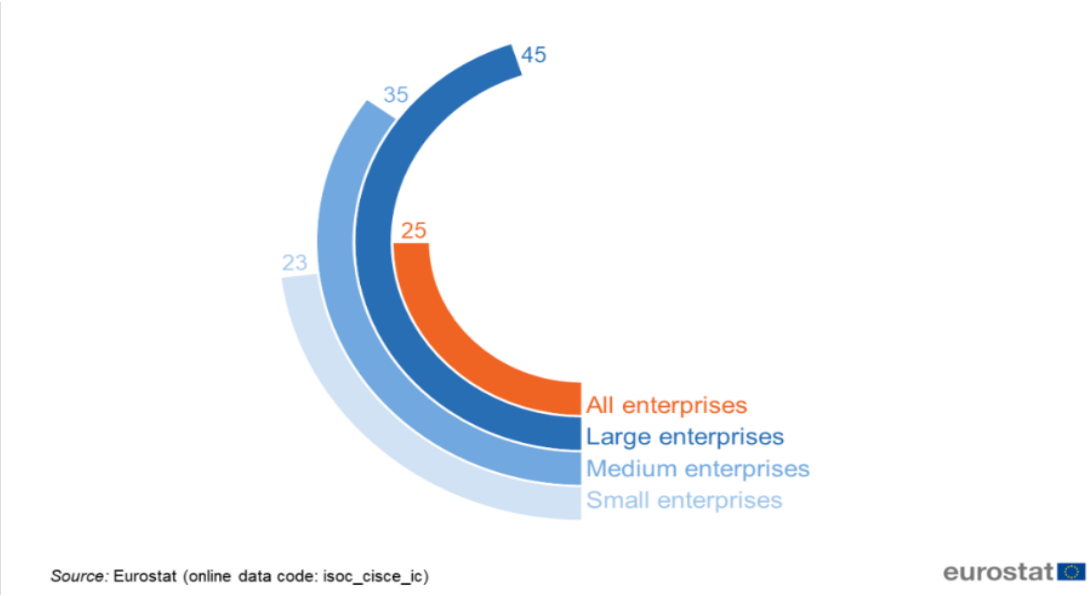
A perceção da cibersegurança nas grandes empresas sofreu uma mudança significativa nos últimos anos. Com a proliferação de violações de dados e ciberataques de alto nível, as organizações passaram a reconhecer que a cibersegurança não se trata de uma preocupação periférica, mas de um aspeto fundamental das suas operações. Como tal, a perceção da cibersegurança deixou de ser encarada como uma mera questão de TI e passou a ser um imperativo estratégico que requer a atenção dos mais altos níveis da liderança empresarial, a qual engloba: pessoas, processos e tecnologia.

Esta perspetiva mais ampla também alterou a ação das empresas na medida da gestão do risco, passando de uma postura reativa para uma postura proativa, agindo preventivamente, antecipando os riscos, e, quando possível, transferindo as consequências do evento de risco, nomeadamente, através da contratação de seguros contra incidentes de cibersegurança.

Na figura 9, observam-se dados da Eurostat de 2022 recolhidos de mais de 150.400 mil empresas europeias que, demonstram que cerca de 45% das grandes empresas possui seguros de cibersegurança, contra quase 35% das PME e 23% das pequenas empresas.

[221] Lamberti, Lorenzo (2019), Analysing and protecting agains existing cyber attacks. In https://urn.fi/URN:NBN:fi:amk-2019052913332
[222] Ibidem.

Figura 9 - Percentagem de empresa com seguro contra incidentes de segurança TIC, por tamanho, UE, 2022



Fonte: *Eurostat (Dezembro, 2022). "ICT security in enterprises", disponível em https://ec.europa.eu/eurostat/statistics-explained/images/a/a7/ICT_security_2022_-_graphs_and_tables.xlsx (código de pesquisa: isoc_cisce_ra)*

Os seguros de cibersegurança são uma das opções que as empresas têm ao seu dispor para se prevenirem dos elevados custos relacionados com um incidente de cibersegurança. Na UE a média de utilização deste tipo de seguros ronda os 25%, em Portugal, este indicador situa-se abaixo da média europeia, revelando que apenas 10% das empresas portuguesas possuem seguros para este tipo de situações.[223]

Para além do investimento em seguros para acautelar o impacto de um potencial incidente de cibersegurança, as grandes empresas também já se aperceberam que a cibersegurança não se trata apenas de uma questão de ameaças externas. Também estão expostas a vulnerabilidades internas que importa acautelar. Funcionários negligentes ou com más intenções, podem representar riscos significativos.

Esta consciencialização levou a um maior enfoque nos programas de formação e sensibilização dos funcionários, bem como à implementação de controlos de acesso e

[223] Eurostat (Dezembro, 2022). "*ICT security in enterprises*", disponível em https://ec.europa.eu/eurostat/statistics-explained/images/a/a7/ICT_security_2022_-_graphs_and_tables.xlsx

sistemas de monitorização rigorosos. Ao fomentar uma cultura consciente da segurança e promover as melhores práticas, as organizações estão melhor equipadas para se defenderem contra ameaças internas e externas. A consciencialização e preocupação com o tema é latente nos relatórios anuais de algumas das principais empresas portuguesas.

Por exemplo, no Relatório Anual Integrado da Sonae SGPS[224], os "Ciberataques" ocupam o quadrante mais grave da matriz de riscos, estando identificado como o risco que poderá consubstanciar o impacto mais grave para o Grupo. Nessa medida, o Grupo elenca as principais ações de mitigação do risco de modo a reduzir a probabilidade e o impacto, entre outras, as seguintes:

- Modelo de governo de cibersegurança
- Equipas dedicadas de cibersegurança
- Programa de sensibilização de cibersegurança
- Procedimento de gestão de incidentes
- Informação sobre ameaças cibernéticas (com o centro Nacional de Cibersegurança)
- Rating de cibersegurança da *Bitsight*
- Perímetro de segurança da rede
- Testes de *hacking* éticos periódicos a sítios na Internet
- Testes de *phishing* éticos periódicos dirigidos aos colaboradores
- Recuperação de desastre para sistemas críticos
- Gestão de acesso e identidade
- Adoção de duplo fator de autenticação como melhor prática
- Encriptação de informação crítica
- EDR, antivírus, anti-spam e deteção de malware

Para além destas ações a SONAE tornou-se também membro fundador da Aliança Nacional para a Cibersegurança. Fazem parte desta aliança alguns dos maiores e influentes grupos portugueses como a NOS, a ANA, os CTT, a EDP, o Grupo Nabeiro, a Jerónimo Martins, a José de Mello Saúde, a SIBS e a Sonae. A Aliança Nacional para a

[224] SONAE SGPS S.A (2022), "*Relatório Anual Integrado 2022"* disponível para consulta em https://www.sonae.pt/fotos/dados_fin/relatoriointegrado_2022_pt_1277178973642cbcbfd0004.pdf

Cibersegurança foi promovida pelo CNCS e pretende promover uma cultura de cibersegurança de boas práticas, fomentando a literacia digital e apostar na prevenção e sensibilização para os riscos digitais.[225]

O grupo NOS, S.A, grupo de renome na área da comunicação, tecnologia, informação e entretenimento português, coloca a cibersegurança no principal quadrante da matriz de riscos[226]. A empresa reconhece o aumento preocupante do número de ciberataques a nível global e dos impactos que podem provocar na organização ao explorar eventuais vulnerabilidades na rede ou nos sistemas de forma a provocar uma paragem das atividades da empresa com graves consequências para a empresa e para aqueles que usufruem dos seus serviços. Como medidas de mitigação deste risco a empresa tem implementado uma série de mecanismos que realizam um monitoramento contínuo do sistema de proteção de cibersegurança e contingência de ameaças, acresce a existência de Politicas e Procedimentos de Segurança que são regulamente atualizados e difundidos por todos os colaboradores, existe uma incidência elevada na formação específica de competências dos colaboradores que fazem parte da equipa de Cibersegurança nas áreas ciberestratégia, ciberarquitectura, ciberinteligência e ciberdefesa, está nomeado um CISO – *Chief Information Security Officer*, entre outras medidas.

O grupo GALP[227], empresa de referência Internacional no sector da energia, coloca a cibersegurança no 2º Nível mais importante da matriz dos principais riscos a que a empresa se encontra exposta, situando-a no quadrante que classifica a "*Cyber*" como capaz de provocar um "impacto muito elevado" na atividade da empresa[228]. No relatório

[225] A Aliança Nacional para a cibersegurança apresenta-se como uma plataforma de cooperação promotora das melhores práticas, que pretende juntar entidades públicas e privadas na proteção da economia digital. Esta aliança tem como principais objetivos: Contribuir para atingir os objetivos da Estratégia Nacional de Segurança do Ciberespaço, promover a literacia e partilha de informação, promover ações de formação para executivos e recursos técnicos na área da Cibersegurança sobre as capacidades necessárias para uma defesa eficaz de modo a aumentar o nível de maturidade das organizações e atuar como incubador de projetos colaborativos. Aliança para a Cibersegurança (2023). https://www.aliancacibersegurança.pt/

[226] NOS SGPS, S.A. (2022). "*Anual Integrated Report 2022".* disponível para consulta em https://web3.cmvm.pt/sdi/emitentes/docs/PC84994.pdf

[227] *Caçador, Fátima (Maio, 2022). "Davos: Galp junta-se a 17 gigantes petrolíferas em acordo para proteção contra ataques informáticos". SapoTek. Disponível em https://tek.sapo.pt/noticias/computadores/artigos/davos-galp-junta-se-a-17-gigantes-petroliferas-em-acordo-para-protecao-contra-ataques-informaticos*

[228] GALP Energia SGPS, S.A. "*Relatório Integrado de Gestão 2022".* Disponível para consulta em https://www.galp.com/corp/Portals/0/Recursos/Investidores/SharedResources/Relatorios/pt/2022/AIRGalp2022PT1Book1IMRFull.pdf

de contas de 2022 a empresa dá conta da rápida evolução tecnológica e dos desafios em monitorizar os riscos de Cibercrime associados a estas novas tecnologias. Ademais, são também destacados os perigos relacionados com a forte dependência de sistemas e dados digitais, e das consequências que podem advir caso ocorra alguma falha de segurança acidental (devido a falhas de rede, hardware ou software), provocada por ações maliciosas (cibercrime), ou por negligência (interna ou devida a prestadores de serviços).

De forma a mitigar este risco a GALP adopta, entre outras, as seguintes medidas de mitigação[229]:

- Estruturas de Governance e equipas dedicadas pela definição e monitorização, através da sua equipa de segurança de dados, de políticas, procedimentos e ações relacionadas com a cibersegurança,
- Avaliação prévia de risco de ciber-resiliência de prestadores de serviço com quem se relacione:
- Promoção de uma cultura de dados e literacia comum a toda a empresa;
- Reforço das capacidades de cibersegurança e ciber-resiliência que asseguram a Identificação, Proteção, Deteção e Resposta/Recuperação de ciberameaças e riscos para a Empresa.
- O quadro normativo do Sistema de Gestão da Continuidade dos Negócios (SGCN) aplicado em todo o Grupo Galp inclui a Política de Continuidade de Negócios, a Norma de Gestão da Continuidade do Negócio e a Estrutura de Resposta na Gestão de Crises. No âmbito do SGCN existem 19 Planos de Continuidade de Negócios (PCN), incluindo o Plano de Comunicação em Crise, o Plano de Recuperação Tecnológica, o Plano de Continuidade de Negócios de Fornecimentos Críticos, que cobrem as instalações industriais críticas da Galp em Portugal.

Para além destas medidas o Grupo subscreveu o Compromisso de Resiliência Cibernética lançado pelo Fórum Económico Mundial, em Davos, e do qual fazem parte outras grandes corporações petrolíferas como a Aker ASA, Aker BP, Aramco, Check Point Software Technologies, Claroty, Cognite, Dragos, Ecopetrol, Eni, EnQuest, Global

[229] GALP Energia SGPS, S.A. (2022).” *Relatório do Governo Societário”.* Disponível para consulta em https://www.galp.com/corp/Portals/0/Recursos/Investidores/SharedResources/Relatorios/pt/2022/AIRGalp2022PT3Book3CorporateGovernance.pdf

Resilience Federation, Maire Tecnimont, Occidental Petroleum, OT-ISAC, Petronas, Repsol e Suncor.

Estes são alguns dos exemplos de medidas adotadas por grandes empresas portuguesas evidenciando um maior sensibilização e participação na prevenção e reforço das medidas de cibersegurança dentro das suas organizações.

8. Fator Social na cibersegurança

O fator social desempenha um papel crítico na cibersegurança. A cibersegurança não se trata apenas de tecnologia, mas também das pessoas que utilizam e interagem com a tecnologia. Os fatores sociais referem-se ao comportamento humano, cultura, e valores que influenciam a forma como as pessoas interagem com a tecnologia.[230] Um dos fatores sociais mais significativos na cibersegurança é o erro humano. Muitas violações de segurança ocorrem devido a erros cometidos por empregados, tais como clicar em ligações maliciosas ou abrir anexos suspeitos em e-mails. É por esta razão que a formação de sensibilização para a cibersegurança é crucial para todos os empregados que utilizam dispositivos e sistemas digitais. Outro fator social importante é a cultura da organização. As atitudes e valores de uma organização em relação à cibersegurança podem ter um impacto significativo na sua postura global de segurança, uma vez que uma cultura organizacional que valoriza a cibersegurança coloca a proteção dos ativos de informação como uma prioridade estratégica.[231] Isso significa que a liderança e os funcionários reconhecem a importância da cibersegurança e estão dispostos a investir os recursos necessários para implementar medidas adequadas de segurança.[232] Acresce que uma cultura organizacional sólida em relação à cibersegurança promove a comunicação aberta e a conscientização entre os funcionários, encorajando a colaboração e a responsabilidade coletiva.[233] Além disso, o fator social desempenha um papel crítico nos ataques de engenharia social. Os ataques de engenharia social visam a exploração do fator humano e não as vulnerabilidades técnicas de um sistema. Os cibercriminosos utilizam táticas de

[230] Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: an emerging national security requirement. Military review, 99(2), 117. https://apps.dtic.mil/sti/tr/pdf/AD1108494.pdf
[231] Anna Georgiadou, Spiros Mouzakitis, Kanaris Bounas & Dimitrios Askounis (2022) A Cyber-Security Culture Framework for Assessing Organization Readiness, Journal of Computer Information Systems, 62:3, 452-462, DOI: 10.1080/08874417.2020.1845583
[232] Ibidem.
[233] Huang, K., & Pearlson, K. (2019). "*For what technology can't fix: Building a model of organizational cybersecurity culture"*. http://hdl.handle.net/10125/60074

engenharia social para enganar as pessoas a revelarem informações sensíveis ou a tomarem medidas que comprometam a segurança dos seus sistemas.[234] Como tal, o fator social é incontornável na cibersegurança. Influencia o comportamento humano, a cultura e os valores, e pode ter um impacto significativo na segurança dos sistemas e dos dados. Compreender e abordar os fatores sociais é crucial para desenvolver uma estratégia eficaz de cibersegurança que possa proteger as organizações das ameaças cibernéticas.

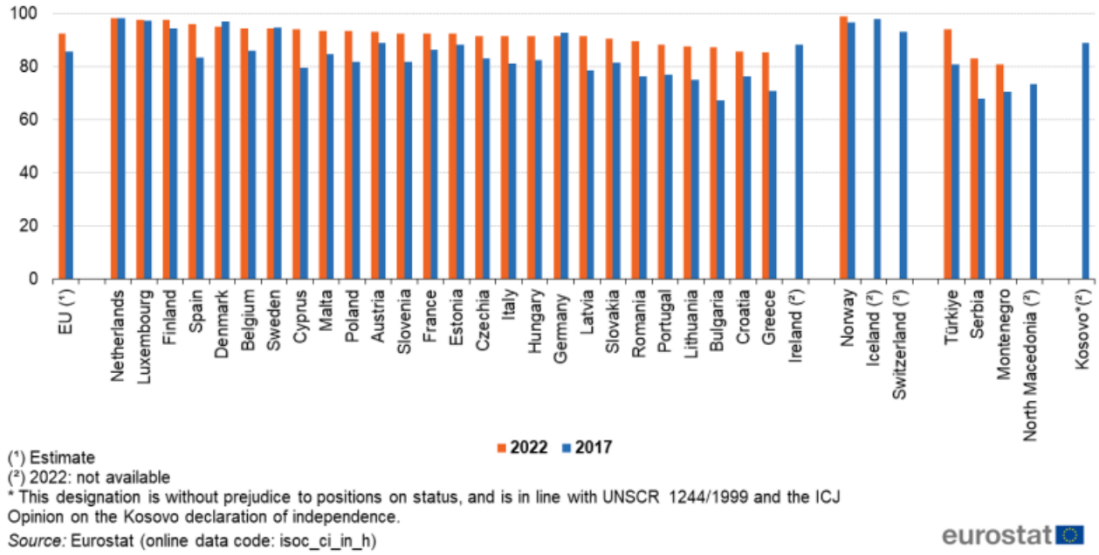
No relatório de Sociedade 2022 do Observatório do CNCS, são identificadas quatro áreas temáticas em Portugal, mas que podem também ser aplicadas a nível Europeu quando se aborda a vulnerabilidade humana como vetor de ataque no ciberespaço, são elas:

- Ambiente sociotécnico, em que se analisa a evolução dos usos da Internet e serviços digitais;
- Pesquisas *online*, onde se apresentam dados sobre o interesse pela pesquisa da palavra "cibersegurança";
- Atitudes e comportamentos, momento em que se expõem os indicadores disponíveis sobre as perceções e as boas práticas relativos à cibersegurança em indivíduos e organizações;
- Sensibilização e educação, etapa dedicada à evolução das ações de sensibilização em ciber-higiene e aos cursos especializados em cibersegurança e segurança de informação.

No plano do ambiente sociotécnico, verifica-se um grande aumento da utilização da internet e do número de aparelhos conectados a ela. Impulsionado pela crise pandémica do COVID-19 e da necessidade de ligações à Internet para o funcionamento normal das economias modernas e trabalho remoto, atualmente estima-se que 93% das casas na União Europeia têm acesso à Internet, segundo dados do Eurostat.[235] (Figura 10)

[234] Para exemplos das táticas de engenharia social, consultar Capitulo 2.5 (As Ciberameaças).
[235] Eurostat (Dezembro, 2022) "Digital economy and society statistics - households and individuals", disponível em https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access

Figura 10 - Acesso à internet nas habitações, entre 2017 e 2022



Fonte: *Eurostat (Dezembro, 2022) "Digital economy and society statistics - households and individuals", disponível em https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access*

Este aumento na utilização de dispositivos e sistemas ligados à internet resulta naturalmente numa maior exposição a eventuais riscos de cibersegurança, desta forma, também deverão aumentar os cuidados a ter relacionados com a ciber-higiene.

É importante ter também uma consciência de quem são os seus utilizadores, embora a Internet possa ser um recurso valioso para os mais velhos, é importante estar consciente dos riscos que advêm da sua utilização. As gerações mais velhas podem ser mais vulneráveis aos ciberataques devido à falta de conhecimento e experiência com a tecnologia.[236]

Em 2022, 90 % dos indivíduos da UE com idades compreendidas entre os 16 e 74 anos utilizaram a Internet pelo menos uma vez nos três meses que antecederam a data do inquérito da Eurostat[237], além disso, os propósitos com que a Internet é utilizada são

[236] Nicole M. Lee (2018) Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom, Communication Education, 67:4, 460-466, DOI: 10.1080/03634523.2018.1503313
[237] Ibidem.

principalmente para e-learning, ações de cidadania e políticas, e a procura de informação sobre saúde[238]. Contudo, estes conteúdos podem ser utilizados para manipular os utilizadores a cair em esquemas de *Phishing*, burlas online, roubo de identidade, vírus e malware ou desinformação.

Embora se verifique uma tendência positiva nos comportamentos dos utilizadores, com um aumento de pesquisa sobre o que é a cibersegurança[239], e algumas das vulnerabilidades mais comuns online já mencionadas, muitas pessoas estão cada vez mais conscientes dos riscos da cibersegurança e estão a tomar medidas para proteger os seus dados pessoais. Por exemplo, as pessoas estão a utilizar palavras-passe mais fortes, estão a adotar a autenticação de dois fatores, evitam links e anexos suspeitos, e atualizam mais regularmente os seus dispositivos e software. No entanto, noutras áreas, ainda existe uma discrepância relevante entre a perceção e a realidade. Por exemplo, relativamente a compras online a ideia de que a segurança e a privacidade são um problema, é muito maior entre os indivíduos que percecionam aí uma barreira ao ponto de não as realizarem, quando comparando com a exposição a situações de fraude efetiva como phishing, entre os que fazem esse tipo de compras.[240]

No plano da sensibilização, educação e formação, também se verificam cada vez mais ações deste género promovidas pelos Governos, pelas Universidades, escolas e empresas. Esta forma massiva de abordar a cibersegurança e alguns conceitos importantes revela-se extremamente frutífera pois só quando se promove uma cultura de cibersegurança é que se consegue adotar uma postura resiliente para combater as vulnerabilidades e ameaças que têm vindo a ser discutidas.

Em Portugal, o Centro Nacional de Cibersegurança tem vindo a realizar diversas ações de formação e treino em contexto profissional, através de cursos online, desde 2019, tendo formado mais de 100 mil pessoas. Outras entidades também contribuem para a difusão do conhecimento sobre a cibersegurança, entre elas, o IAPMEI - Agência para a Competitividade e Inovação, I.P., Polícia Judiciária e a Polícia de Segurança Pública.

[238] Ibidem.
[239] CNCS (Dezembro, 2022). "Relatório Sociedade 2022", https://www.cncs.gov.pt/docs/rel-sociedade2022-observ-cncs.pdf
[240] Ibidem.

A nível de contexto mundial, entre 194 países, Portugal está situado no 14º lugar, segundo o Índice Global de Cibersegurança de 2021, realizado pela União Internacional das Telecomunicações (organismo das Nações Unidas)[241], e 9º lugar a nível europeu.

Portugal, tem investido nesta área, de forma a continuar o desenvolvimento desta matéria, 47 Milhões de euros do Plano de Recuperação e Resiliência serão destinados "*ao reforço do quadro geral da cibersegurança, e que se destinam a dar resposta a algumas das principais questões da atualidade nesta matéria*, segundo o comentário do Secretário de Estado da Digitalização e da Modernização Administrativa, Mário Campolargo.[242]

Por conseguinte, embora haja uma tendência positiva para melhorar as práticas de cibersegurança entre a sociedade e os utilizadores privados, ainda há muito trabalho a fazer para sensibilizar e educar as pessoas sobre a importância da cibersegurança, principalmente nas faixas etárias mais velhas e nas pessoas das classes sociais menos favorecidas, onde este tema requer mais atenção.

9. Relação entre cibersegurança e os indicadores Environmental, Social and Governance (ESG)

Nos últimos anos, o panorama digital sofreu um crescimento exponencial, com a cibersegurança a emergir como uma preocupação primordial na proteção de dados, pessoais e confidenciais, e das infraestruturas digitais.

Os critérios ambientais (E- *Environmental*), sociais (S-*Social*) e de governação (G-*Governance*) – que formam a sigla "ESG" – tornaram-se parte integrante na tomada de decisões das empresas, moldando estratégias e iniciativas que equilibram a rentabilidade com práticas responsáveis e sustentáveis. A interseção entre ESG e cibersegurança constitui um ponto fulcral, onde as empresas podem abordar proactivamente as responsabilidades governamentais nesta matéria, demonstrando de forma transparente, os indicadores de desempenho utilizados e o modo como abordam este tema, tão importante e que pode vir a colocar em risco a organização no futuro.

[241] International Telecommunication Union (ITU) (2020). *Global Cybersecurity Index*. Disponível em https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

[242] Portugal.Gov. "*PRR vai investir 47 milhões na formação em cibersegurança*". Portugal.Gov.pt. https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=prr-vai-investir-47-milhoes-na-formacao-em-ciberseguranca

A cibersegurança pode incluir-se no ponto "G" (*Governance*), de ESG, constituindo-se como um elemento relevante dentro da governança corporativa, especialmente no que se refere à proteção contra ameaças cibernéticas, gestão de riscos de segurança digital, conformidade com regulamentações e normas existentes como o NISD e o RGPD, engobando também todas as políticas e procedimentos relacionados com a gestão e proteção dos ativos digitais e da segurança da informação de uma empresa.

Embora a Cibersegurança não faça parte formal dos objetivos ESG da diretiva Diretiva (UE) 2022/2464 do Parlamento Europeu e do Conselho de 14 de Dezembro de 2022, também conhecida como *Corporate Sustainability Reporting Directive* ou CSRD[243][244], o tema faz parte integrante das preocupações de muitas empresas[245]. Na verdade, trata-se de um ponto absolutamente crucial para muitos investidores e para a própria competitividade da empresa no mercado, assim como para muitos dos investidores e acionistas que utilizam estes indicadores para avaliar potenciais investimentos e monitorizar o desempenho ambiental, social e de governação de uma empresa.

De acordo com a *Principles for Responsible Investment* (PRI) – uma rede de investidores apoiada pela ONU criada em 2006 com o objetivo de promover a integração de critérios ambientais, sociais e de governança (ESG) nas práticas de investimento e processos de tomada de decisão dentro da indústria financeira – os investidores que se comprometem a investir em ESG controlavam mais de 100 biliões de dólares de ativos em 2020.[246]

O quadro ESG é atualmente um quadro amplamente aceite pela comunidade de investidores a nível mundial para compreender e gerir os riscos empresariais.[247] Dada esta tendência, com vista a atrair investidores e facilitar parcerias para projetos de

[243] Diretiva (UE) 2022/2464 do Parlamento Europeu e do Conselho de 14 de Dezembro de 2022 que altera o Regulamento (UE) n.o 537/2014, a Diretiva 2004/109/CE, a Diretiva 2006/43/CE e a Diretiva 2013/34/UE no que diz respeito ao relato de sustentabilidade das empresas, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2464, Documento 32022L2464

[244]Esta Diretiva impõe a todas as PME, cujos valores mobiliários estão admitidos à negociação num mercado regulamentado na União, a divulgação de informações não financeiras sobre os seus impactos a nível ambiental, social, nos direitos humanos e noutros fatores de governação ESG.

[245] Conforme referido no ponto 7 deste Capítulo "*A perceção da cibersegurança pelas grandes empresas Portuguesas*".

[246] Principal for Responsible Investment (2022). "*Annual Report 2022)".* https://www.unpri.org/annual-report-2022/signatories

[247] Escrig-Olmedo, E., Fernández-Izquierdo, M. Á., Ferrero-Ferrero, I., Rivera-Lirio, J. M., & Muñoz-Torres, M. J. (2019). Rating the raters: Evaluating how ESG rating agencies integrate sustainability principles. Sustainability, 11(3), 915. https://doi.org/10.3390/su11030915

investimentos, as empresas têm vindo a divulgar voluntariamente, mais informações sobre as suas políticas e compromissos em matéria de ESG que, por sua vez, são utilizados para atribuir uma classificação pelas agências externas[248], como a MSCI[249] e a Refinitiv[250].

Tal como qualquer gestor de uma carteira de ativos, a consideração de uma estratégia a longo prazo para o desempenho dos ativos inclui uma gestão dos riscos de forma a maximizar a resiliência em diversos cenários.

Como tal, empresas que priorizam as regras ESG, e em particular o tema da cibersegurança, estão mais preparadas para lidar com desafios regulatórios, ciberincidentes, incidentes de proteção de dados – nunca é de mais recordar, podem ascender a 20 Milhões de Euros ou 4% do volume global de faturação da empresa – e mesmo evitar danos significativos à sua reputação e ao valor da marca.

A nível de resiliência empresarial, a cibersegurança é vital para garantir a continuidade e a resiliência das operações comerciais. Empresas que dão prioridade à cibersegurança estão melhor equipadas para resistir a ciberameaças, adaptar-se aos avanços tecnológicos e recuperar mais eficazmente face a eventuais perturbações. Os investidores valorizam essa resiliência, uma vez que reduz os riscos associados à continuidade do negócio.

Deste modo, ao gerir os riscos de uma forma previsível e determinável, a probabilidade de ocorrência e/ou as consequências do impacto, serão menores. Com efeito, a empresa transparece mais segurança e diminui o risco, melhorando o seu desempenho governativo e contribuindo para a sua valorização.

---

[248] Avetisyan, E., & Hockerts, K. (2017). The consolidation of the ESG rating industry as an enactment of institutional retrogression. Business Strategy and the Environment, 26(3), 316-330. https://doi.org/10.1002/bse.1919

[249] A MSCI é uma empresa de serviços financeiros sediada nos Estados Unidos que oferece uma variedade de soluções para investidores e gestores de ativos. Eles são conhecidos por serem líderes em fornecer índices de referência (benchmarks) para mercados globais e também por fornecerem avaliações de ESG (Environmental, Social, Governance) para empresas e investimentos, mais informação em https://www.msci.com/who-we-are/about-us

[250] A Refinitiv é uma empresa global de dados financeiros e análises, fornecendo informações, insights e soluções para profissionais da indústria financeira, investidores e empresas. "Com uma receita de 6,25 mil milhões de dólares, mais de 40.000 clientes e 400.000 utilizadores finais em 190 países, a Refinitiv está a impulsionar os participantes no mercado financeiro global.", mais informações em https://www.refinitiv.com/en/about-us

CAPÍTULO 5 - Incidentes de cibersegurança e a Proteção de Dados

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ou Regulamento Geral de Proteção de Dados (RGPD)[251], representa um marco significativo na evolução do quadro de proteção de dados no contexto europeu,– sendo considerado um direito fundamental consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, e um direito Constitucional consagrado no artigo 35.º da Constituição da República Portuguesa,– regulamenta de forma abrangente as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, dos dados pessoais relativos a pessoas singulares na EU[252]. Efetivamente, foi implementado em Maio de 2018, com o objectivo de conceder aos titulares mais controlo sobre os seus dados e harmonizar as leis de proteção de dados em todos os Estados Membros. Para além do reforço da proteção jurídica dos direitos dos titulares dos dados, o RGPD define novas regras e procedimentos do ponto de vista tecnológico.

Em Portugal, a Lei n.º 58/2018, de 8 de Agosto, assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

1. Violações de dados e a cibersegurança

Fundamentalmente, o RGPD impõe obrigações às organizações públicas e privadas que realizem um tratamento lícito, leal e transparente em relação ao titular de dados. Para o efeito, estabelece os direitos dos titulares de dados: acesso, retificação,

[251] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE), Documento 32016R0679 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

[252] Artigo 3.º do RGPD (Âmbito de aplicação territorial)"
1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.
2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:
a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;
b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União. (…)"

eliminação, limitação ou oposição de tratamento;[253] estabelece os princípios relativos ao tratamento de dados pessoais: licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e responsabilidade e a responsabilidade; estabelece a licitude tratamento dos dados, consentimento, execução de um contrato, obrigação jurídica do responsável de tratamento de dados, defesa do interesse vital, função de interesse público ou autoridade pública, e interesse legítimo; entre outras disposições de grande relevância no plano do tratamento de dados como a implementação de medidas de segurança, a realização de avaliações de impacto sobre a proteção de dados[254] ou a notificação de violações de dados.

A não conformidade com as disposições do RGPD pode resultar em advertências, ou coimas significativas que podem ir até 20 milhões de euros ou 4 % do volume de negócios total anual da empresa a nível mundial.

Os incidentes de cibersegurança e a proteção de dados são dois temas indissociáveis, no entanto, nem sempre são considerados quando determinada empresa sofre um incidente desta natureza. Isto ocorre, primeiro, por falta de sensibilidade para esta matéria uma vez que muitas empresas tendem a focar-se na parte tecnológica acabando por descurar a proteção de dados – por exemplo, investindo em servidores e VPN's, mas não definindo períodos de conservação de dados –, e, segundo, porque muitas vezes se relaciona o ciberataque ataque como uma intrusão não autorizada ao sistema, não relacionando o incidente como uma violação de dados. Embora o acesso não autorizado configure uma violação de dados nos termos do 4º n.º 12 do RGPD. De maneira que, cumpre fazer um fazer uma reflexão sobre esta relação.

Desde logo, um dado pessoal é qualquer "*informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por*

[253] Os titulares têm ainda o direito de retirar o seu consentimento a qualquer momento, e de apresentar uma reclamação à autoridade nacional competente, em Portugal a autoridade de controlo portuguesa é a Comissão Nacional de Proteção de Dados, caso entenda que o tratamento não seja correto, direito decorrente do artigo 77.º do RGPD.

[254] A realização de uma avaliação de impacto sobre a proteção de dados (AIPD) trata-se de uma obrigação legal prevista no artigo 35.º do RGPD e é executada sempre que o tratamento de dados pessoais em causa assim o exigir, designadamente quando ocorrerem atividades de tratamento de em larga escala dos dados pessoais previstos no artigo 9.º ou no artigo 10.º do RGPD; assim como quando houver um controlo sistemático de zonas acessíveis ao público em larga escala (por exemplo, através de sistemas de videovigilância); ou, ainda, quando forem feitas definições de perfis (profiling) e, subsequentemente, forem tomadas decisões automatizadas que afetem significativamente a pessoa singular, entre outras situações identificadas no referido artigo do RGPD.

referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;" na aceção do artigo 4º n.º 1 do RGPD.

Por sua vez, uma violação de dados pessoais é uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento de acordo com o consignado no artº 4º nº 12 RGPD.

Deste modo, qualquer incidente de cibersegurança em que o *hacker/craker* tenha acesso a dados pessoais nos termos do artigo supramencionado, resulta inequivocamente num caso de violação de dados. Saliente-se que, um dos principais motivos por de trás dos ciberataques é o ganho financeiro, na maior parte das vezes proveniente da venda de informações pessoais de titulares de dados, como informações bancárias, ou outras informações de identificação pessoal, que por sua vez são utilizadas para cometer fraudes, efetuar transações não autorizadas e transacionadas em mercados paralelos, como a DeepWeb.

Como temos vindo a assistir em vários casos, muitas vezes, as empresas só se apercebem que foram vítimas de um ciberataque, quando vêm as suas bases de dados de clientes e fornecedores à venda nesses mercados paralelos, pelo que, o simples facto desses dados estarem à venda, configura desde logo uma violação de dados, podendo resultar um dano na esfera jurídica do titular de dados, uma vez que estes poderão ser utilizados para fins ilícitos, à revelia da vontade do titular de dados. Esta situação, poderá dar origem a uma indemnização em sede de responsabilidade civil por danos patrimoniais (por exemplo, um prejuízo financeiro) ou não patrimoniais (por exemplo, sofrimento ou danos à reputação).

Suponhamos, a título de exemplo, um caso em que alguém faz uma compra online num site de compras. Esse site sofre um ciberataque por não dispor de medidas de segurança adequadas e os dados do cartão de crédito dessa pessoa são exfiltrados e vendidos a outra entidade. É permitido ao titular de dados apresentar um pedido de indemnização à empresa em causa ou em alternativa apresentar uma ação nos tribunais nacionais para do Estado Membro onde o responsável pelo tratamento ou o subcontratante têm o seu estabelecimento, dispondo ainda da possibilidade de intentar a ação junto dos

tribunais do Estado-Membro da UE onde tem a sua residência habitual, de acordo com o disposto no artigo 82º do RGPD ("Direito de Indemnização e Responsabilidade"). O valor a pagar pela indemnização a um titular de dados poderá não ser expressivo quando se trate de uma empresa com elevado valor de faturação, porém, se a indemnização tiver de ser atribuída a vários milhões de titulares de dados, o valor pode aumentar substancialmente de alguns milhares ou centenas de euros, para algumas centenas de milhares ou milhões de euros[255]. Valor que, acrescido a uma contraordenação por não dispor de medidas adequadas de proteção dos dados, poderemos estar a falar de várias dezenas de milhões de euros que, em último caso, poderá determinar o encerramento da empresa.

No âmbito dos pedidos de indemnização e exercício de direitos, os titulares de dados têm ainda o direito e a legitimidade de mandatar um organismo, organização ou associação sem fins lucrativos, que esteja devidamente constituído ao abrigo do direito de um Estado-Membro, para exercer o direito de receber uma indemnização nos termos do artigo 80º do RGPD ("Representação dos titulares dos dados"). Esta possibilidade conferida pelo RGPD, confere aos titulares de dados uma oportunidade muito maior de poder exercer os seus direitos e de vê-los reconhecidos. A este respeito, uma das organizações sem fins lucrativos mais ativas na área da proteção de dados é a NOYB (*None of Your Business*), com sede em Viena Áustria, fundada em 2018, pelo advogado e ativista de privacidade e proteção de dados, o austríaco Max Schrems. Conhecido internacionalmente pela queixa apresentada na autoridade nacional de proteção de dados Irlandesa (*Irish Data Commissioner*) contra o Facebook, sobre as transferências internacionais de dados para os Estados Unidos, na sequência das revelações de Edward Snowden, que culminaria na invalidação do acordo de transferência de dados entre UE e USA ("Safe Harbor"), na decisão C-362/14 – conhecida como Schrems I[256] –, e, mais tarde, pela queixa formalizada contra o Facebook, na mesma autoridade de controlo, contra as transferências internacionais ao abrigo das cláusulas-tipo de proteção de dados

[255] De acordo com o considerando 146 do RGPD " (…) O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento. (…) Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido.(…)."

[256] Acórdão de 6 de Outubro de 2015, Schrems, C-362/14, ECLI:EU:C:2015:650 https://curia.europa.eu/juris/liste.jsf?num=C-362/14

da Comissão Europeia ao abrigo do "*Privacy Shield*", entretanto também invalidado pelo TJUE na decisão C-311/18 – conhecida como Schrems II[257].

2. Notificação de uma violação de dados pessoais à autoridade de controlo

Em Portugal, a autoridade nacional de controlo de dados pessoais é a Comissão Nacional de Proteção de Dados. Em 2022, ao abrigo do artigo 33º do RGPD, foram registados a abertura de 367 processos de violações de dados pessoais, contudo não fica claro o número de casos em que foram aplicadas coimas por essas violações, uma vez que nesse ano foram aplicadas 71 coimas, no valor de 4.802.00,00 euros, sendo que 59 por envio de marketing em violação das regras legais (spam) e as demais 12 ao abrigo das disposições do RGPD, porém, sem especificar quais. Não obstante, nos 367 processos de violações de dados não se saber se terá sido aplicada alguma coima, foram adotadas 318 deliberações, tendo a CNPD feito recomendações específicas destinadas a orientar as organizações a melhorar o nível de segurança nos seus processamentos de dados, por meio da adoção de medidas adequadas à situação em questão. De todo o modo, cumpre dar nota que a CNPD dispõe apenas de 28 trabalhadores.[258]

Não obstante as capacidades operacionais das autoridades de controlo, caso ocorra um ciberataque e se verifique que ocorreu uma situação que gerou uma violação de dados, o responsável pelo tratamento deve notificar desse facto a autoridade de controlo competente nos termos do artigo 33º do RGPD, sem demora injustificada, e sempre que possível, até 72 horas após ter tido conhecimento da mesma[259], a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

Destarte, a referida notificação à autoridade de controlo deverá conter, pelo menos:

---

[257] Acórdão de 16 de Julho, Facebook Ireland e Schrems, C-311/18, ECLI:EU:C:2020:559. https://curia.europa.eu/juris/liste.jsf?num=C-311/18&language=PT

[258] Comissão Nacional de Proteção de Dados (2022). *Relatório de Atividades de 2022. Disponível em: https://www.cnpd.pt/media/tutpevyh/relato-rio_2022.pdf*

[259] Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso – artigo 33º n.º. 1 do RGPD.

a) Descrição da natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;

b) Comunicar o nome e os contactos do Encarregado de Proteção de Dados ou de outro ponto de contacto onde possam ser obtidas mais informações;

c) Descrever as consequências prováveis da violação de dados pessoais;

d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

Adicionalmente, poderá ainda ser necessário que se comunique a violação de dados pessoais ao titular dos dados quando for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.

Em situações excecionais a comunicação poderá não ser exigida, nomeadamente quando:

a) O RT tiver aplicado medidas de proteção adequadas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;

b) O RT tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados… já não é suscetível de se concretizar;

c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.

O incumprimento das disposições do RGPD poderá resultar na aplicação de uma advertência, contraordenação, com aplicação de uma coima máxima de 20 milhões de euros ou 4 % do volume de negócios total anual da empresa a nível mundial, ou mesmo na prossecução criminal quando se aplique a moldura penal dos crimes previstos na Lei n.º 67/98, de 26 de Outubro que que assegura a execução na ordem jurídica nacional do

Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados), tais como: a utilização de dados incompatível com a finalidade da recolha (artigo 46.º da referida Lei); acesso indevido (artigo 47.º); desvio de dados (artigo 48.º); viciação ou destruição de dados (49.º); inserção de dados falsos (artigo 50.º); violação do dever de sigilo (artigo 51.º); ou, desobediência (artigo 52.º).

Como tal a premência da proteção de dados é indiscutível, não deverão apenas ser consideradas as medidas tecnológicas de prevenção e combate a ataques informáticos, a segurança de todos os dados da organização deverá ser uma preocupação que interligue ambas as áreas. Apenas quando uma organização tem implementadas as medidas técnicas e organizativas adequadas tendo em vista a proteção dos dados pessoais contra a destruição, acidental ou ilícita, a alteração, acesso não autorizado e divulgação e contra qualquer forma de tratamento ilícito, é que se consegue cabalmente prevenir dos elevados custos relacionados com consequências legais, financeiras e reputacionais com impactos ao nível da receita e valor de mercado, de um incidente de proteção de dados. Ademais, deverão também ser incluídos os prejuízos relacionados com a perda de dados comerciais confidenciais, ou mesmo a exposição pública de informações pessoais ou de negócio tais como contactos e moradas, dados de cartões de multibanco, ou dados de saúde.

Conclusão

As ameaças cibernéticas são uma das principais ameaças do nosso tempo e que nos afetam a todos, desde a nossa vida individual à nossa vida em sociedade. Como tal, é essencial uma tomada de ação contra esta ameaça e começar a traçar um caminho que considere este tema uma prioridade, promovendo a informação, consciencialização e capacitação para os temas da cibersegurança.

Esta mudança passa não só pelos agentes políticos, dado o seu maior nível de alcance e responsabilidade pela segurança pública, determinada pela nossa Constituição, mas também, pelas nossas ações individuais no dia a dia, com a utilização dos nossos dispositivos pessoais, todos nós somos responsáveis pela segurança da informação e, como tal, a todos compete a responsabilidade de zelar pela proteção dos nossos dados e dos que nos são confiados.

Embora a maturidade do tema ainda não tenha atingido o nível desejado, é necessário que seja dada prioridade à cibersegurança e aos comportamentos no ambiente digital, nomeadamente, através de um maior escrutínio na comunicação social, não apenas com temas sensacionalistas ou quando ocorre um ciberataque a uma empresa de referência, mas numa lógica pedagógica que promova o aumento da prevenção e da literacia digital.

Nas empresas, a célebre frase descrita no Relatório de Riscos Globais do *World Economic Forum*, "*Pay, Protect or Perish*" em português "*Pagar, proteger ou desaparecer*", nunca fez tanto sentido. É essencial que a perspetiva mude, e a cibersegurança passe a ser encarada como uma necessidade e um investimento e não como uma despesa. Ao longo da dissertação foram relatados diversos casos de empresas que sofreram ciberataques com consequências graves para a sua atividade, dado o impacto provocado pelas perdas financeiras resultantes da paralisação da atividade, custos com processos judiciais decorrentes da falta de medidas técnicas adequadas de proteção de dados pessoais ou informações confidenciais, custos relacionados com o restabelecimento da atividade, eventuais custos de pagamento de resgates para recuperar a informação bloqueada pelos atacantes, bem como os danos reputacionais e de imagem, que poderão ser irreversíveis resultando na falta de confiança perante potenciais clientes, clientes, fornecedores e acionistas, decorrente da vulnerabilidade e da falta de garantias de segurança dos dados nas empresas.

Além disso, as novas exigências a nível europeu no que diz respeito ao reporte da sustentabilidade empresarial, por via das recentes regras ESG vêm exigir às empresas que demonstrem um conjunto de indicadores que são utilizados para avaliar o seu desempenho e sustentabilidade em relação a questões ambientais, sociais e de governança corporativa, sendo que, neste último a proteção dos dados e a cibersegurança são pontos importantes a considerar.

Com cerca de 28% das PME Europeias a admitirem que sofreram um ciberataque em 2021, – acabou o mito de que o cibercrime só acontece aos outros – as organizações que não demonstrem uma forte governo empresarial e transparência em torno destes temas e que não possuam sistemas de controlo interno e de gestão de risco adequados, políticas e procedimentos internos para informação dos colaboradores, resposta a incidentes internos, incluindo planos de contingência e recuperação de dados, evidências de ações de formação aos colaboradores para consciencialização e capacitação para os temas da cibersegurança, arriscam-se a sofrer danos na sua reputação e aos olhos dos investidores apresentam-se como empresas pouco competitivas e de elevado risco de investimento, face ao fraco compromisso com a gestão de risco e práticas de governo empresarial.

Relativamente aos desafios para o Direito e a Cibersegurança, na esteira desta dissertação, podem ser salientados três pontos chave seguintes:

a) O direito à proteção de dados é um direito constitucionalmente consagrado e um direito fundamental, que, face ao galopante avanço tecnológico e digital, deve constituir uma das prioridades nas linhas de atuação dos Governos e das empresas, com, vista a zelarem pela segurança e garantirem a privacidade dos dados dos Cidadãos e dos intervenientes com quem se relacionem, assegurando a confiança necessária destes e assim o adequado funcionamento da atual sociedade digital;
b) a capacidade do mundo jurídico acompanhar a evolução tecnológica, é um ponto fundamental para a adaptação das leis e normas ao cenário digital em constante transformação. Só assim se poderá transpor os desafios relacionados com a prossecução criminal, jurisdição, velocidade de investigação, acesso a dados transfronteiriços ou cooperação internacional, de forma a garantir a proteção dos direitos e interesses dos cidadãos e das instituições na era digital.

c) Apenas com uma execução rigorosa das normas e disposições legais é possível alcançar um desejado nível de maturidade digital nas entidades públicas e privadas.

Não obstante, as imposições previstas no RGPD, na nossa Lei da Proteção de Dados, na Lei do Regime Jurídico da Segurança do Ciberespaço e no Decreto-Lei que regulamenta o Regime Jurídico da Segurança do Ciberespaço, Portugal ainda assim, está à aquém do que é considerado aceitável e necessário.

Na realidade, para que as entidades públicas e privadas possam cumprir efetivamente com a legislação nacional e europeia para proteger os dados pessoais dos titulares, bem como assegurar que dispõem dos requisitos de segurança das redes e sistemas de informação e dos procedimentos para a notificação de incidentes, têm efetivamente que dispor de meios humanos e técnicos.

É justamente com esta escassez de meios que as nossas autoridades nacionais neste momento se deparam. A Comissão Nacional da Proteção de Dados e o Centro Nacional de Cibersegurança, defrontam-se com a dificuldade de assegurar em pleno a prática as suas atribuições de controlo e fiscalização no estrito cumprimento da legislação em causa.

Vale isto para dizer, que existe ainda um longo caminho a percorrer até que a efetiva execução da legislação e a aplicação sistemática de sanções, por cada violação, se verifique.

Às nações e respetivas entidades competentes, cumpre o papel de garantes da segurança e defesa nacionais. No atual Séc. XXI as ciberameaças e a ciberguerra são a realidade, como mencionado no "*Caso STUXNET"*, que demonstrou como a Segurança Nacional vai muito para além do território terreste, marítimo e aéreo, sendo também necessário proteger o "território digital" sem fronteiras. Casos como este, demonstraram também a vulnerabilidade das infraestruturas críticas a ciberataques e as suas potenciais consequências. A paralisação de infraestruturas essenciais para o funcionamento da sociedade moderna, tais como, redes elétricas, sistemas de transporte e serviços de saúde podem desencadear repercussões avassaladoras, com potencial para provocar um impacto negativo na economia de um país ou mesmo colocar em risco vidas humanas.

A cibersegurança é uma parte indissociável da atividade desenvolvida por qualquer empresa, na qual, não sendo eliminâveis, os riscos de cibersegurança têm de ser identificados, comunicados, aceites, categorizados e geridos através de planos eficientes, eficazes e adaptados à realidade organizativa e funcional da organização.

A cibersegurança é também um desafio em constante evolução que merece uma reflexão séria e um debate aprofundado, sendo importante que a discussão e as medidas para a sua consolidação acompanhem essas mudanças. Com a conscientização, a colaboração e o compromisso contínuo de todas as partes interessadas, é possível melhorar as práticas de cibersegurança e proteger melhor os nossos sistemas, dados e infraestruturas críticas. Sendo ainda importante, frisar que a cibersegurança não se trata de um produto, mas sim de um processo contínuo. Processo esse que começa com a formação, por meio da educação e da sensibilização, para capacitar os cidadãos com os conhecimentos necessários para identificar e prevenir as ciberameaças.

Por fim, cumpre mais uma vez destacar o valor que um incidente de segurança dos dados pode acarretar para as empresas do ponto de vista legal, à qual acresce o valor de uma eventual condenação no âmbito da proteção de dados, que pode ascender a 4% do valor global de faturação ou 20 milhões de euros. Acresce ainda, a possibilidade de terem que pagar indemnizações aos titulares dos dados pessoais, que tenham sofrido danos materiais ou imateriais pelas violações do Regulamento Geral de Proteção de Dados (RGPD) e das respetivas leis nacionais de proteção de dados, valores esses que poderão alcançar avultadas quantias, quanto maior for o número de lesados a serem ressarcidos. Porquanto, um ponto fundamental é a necessidade efetiva de uma estreita articulação, colaboração e permanente atualização entre as equipas de segurança informática, de proteção de dados, legais e de compliance e demais colaboradores, com vista à eficaz proteção dos dados pessoais dos titulares nas empresas e demais entidades, assegurando o cumprimento dos requisitos legais, dos procedimentos de segurança e operacionais no âmbito da proteção dos dados e da informação e demais normas internas.

Em suma, pelas contingências de uma sociedade e um mundo globalizado a cibersegurança é um ónus que a todos compete e envolve.

Referências Biográficas

Anna Georgiadou, Spiros Mouzakitis, Kanaris Bounas & Dimitrios Askounis (2022) A Cyber-Security Culture Framework for Assessing Organization Readiness, Journal of Computer Information Systems, 62:3, 452-462, DOI: 10.1080/08874417.2020.1845583

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580. https://doi.org/10.1016/j.dss.2021.113580.

Agência da União Europeia para a Cibersegurança (ENISA). (Março, 2023) "ENISA Threat Landscape: transport sector (January 2021 to October 2022" disponível em https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape/@@download/fullReport

Agência da União Europeia para a Cibersegurança (ENISA) (2022). "Theath Landscape for Ransomware Attacks" https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks,

Agência da União Europeia para a Cibersegurança (ENISA) (2022, Novembro) "ENISA THREAT LANDSCAPE 2022" https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

Agência da União Europeia para a Cibersegurança (ENISA) (2022, Maio). "ENISA Mandaate and Regulatory Framework" https://www.enisa.europa.eu/about-enisa/regulatory-framework

Agência da União Europeia para a Cibersegurança (ENISA) (Fevereiro, 2017) "Incident notification for DSPs in the contexto of the NIS Directive", https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/

Agência da União Europeia para a Cibersegurança (ENISA) (Fevereiro, 2017), "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers", disponível em https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

Agência da União Europeia para a Cibersegurança (ENISA) "ENISA Threat Landscape (2022, Novembro), disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Aarti G. (2020, Março). "Cyber Insurance Market by Company Size (Large Companies and Small & Medium-sized Companies) and Industry Vertical (BFSI, IT & Telecom, Retail & E-commerce, Healthcare, Manufacturing, Government & Public Sector, and Others): Global Opportunity Analysis and Industry Forecast, 2019-2026". AlliedMarketReserarch. https://www.alliedmarketresearch.com/cyber-insurance-market

Agência Europeia de Defesa (Maio, 2023), Annual Report disponível em https://eda.europa.eu/docs/default-source/documents/eda-annual-report-2022_en-web.pdf

Alazab, Ammar; Abawajy, Jemal; Hobbs, Michael; Layton, Robert; Khraisat, Ansam (2013). [IEEE 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) - Melbourne, Australia (2013.07.16-2013.07.18)] 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications - Crime Toolkits: The Productisation of Cybercrime. , (), 1626–1632. doi:10.1109/TrustCom.2013.273

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211-236

Almulihi, A. H., Alassery, F., Khan, A. I., Shukla, S., Gupta, B. K., & Kumar, R. (2022). Analyzing the Implications of Healthcare Data Breaches through Computational Technique. Intelligent Automation & Soft Computing, 32(3).

Alshaikh, Moneer (2020). "Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security", 98(), 102003–. doi:10.1016/j.cose.2020.102003

Avetisyan, E., & Hockerts, K. (2017). The consolidation of the ESG rating industry as an enactment of institutional retrogression. Business Strategy and the Environment, 26(3), 316-330. https://doi.org/10.1002/bse.1919

Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. Computer Standards & Interfaces, 54, 176-185.

Barati, M., & Yankson, B. (2022). Predicting the occurrence of a data breach. International Journal of Information Management Data Insights, 2(2), 100128.

Bendiek, A. et al. (Novembro, 2017) «The EU's Revised Cybersecurity Strategy Half-Hearted Progress on Far-Reaching Challenges» https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf.

Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: an emerging national security requirement. Military review, 99(2), 117. https://apps.dtic.mil/sti/tr/pdf/AD1108494.pdf

Cavelty, M., 2018b. "Europe´s cyber-power. European Politics and Society", 19(3), 304-320. https://doi.org/10.1080/23745118.2018.1430718

C. Guedes Soares, A. P. Teixeira, C. Jacinto (Eds), "Riscos, Segurança e Sustentabilidade" Edições Salamandra, Lisboa, 2012, (ISBN 978-972-689-247-2), pp.163 a 176

Centro Nacional de Cibersegurança (CNCS) (Junho, 2019). "Estratégia Nacional de Segurança do Ciberespaço 2019-2023", https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

CERS, Comité Europeu do Risco Sistémico (Fevereiro, 2020), "Systemic cyber risk", https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

Christou, G. (2018). "The collective securitisation of cyberspace in the European Union". West European Politics, 42(2), 278-301.

Centro Nacional de Cibersegurança (CNCS) (2022). "Relatório Cibersegurança em Portugal – Riscos e Conflitos 2022", https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

Centro Nacional de Cibersegurança (CNCS) (Dezembro, 2022). "Cibersegurança em Portugal. Relatório Sociedade", https://www.cncs.gov.pt/docs/rel-sociedade2022-observ-cncs.pdf

Centro Nacional de Cibersegurança (CNCS) (Maio, 2022). "Relatório Economia 2022", https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf

Centro Nacional de Cibersegurança (CNCS) "Relatório Cibersegurança em Portugal. Políticas Públicas." https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriocibersegurança-cncs.pdf

Centro Nacional de Cibersegurança (CNCS) (2019) "Atividades do Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 desenvolvidas em 2019 e 2020" https://www.cncs.gov.pt/docs/ensc2019-2023-pa-2019-2020-2021-execucao2020-mai21.pdf

CNCS. "Quadro Nacional de Referência para a Cibersegurança". https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

Comissão Europeia(Abril 2016). "Comunicação Da Comissão Ao Parlamento Europeu, Ao Conselho Europeu E Ao Conselho Dar Cumprimento À Agenda Europeia Para A Segurança Para Combater O Terrorismo E Abrir Caminho À Criação De Uma União Da Segurança Genuína E Eficaz". https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52016DC0230&from=DA

Comissão Europeia (Dezembro, 2020) "Joint Communication To The European Parliament And The Council The Eu's Cybersecurity Strategy for the Digital Decade" https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, Document 52020JC0018

Comissão Europeia(Dezembro, 2020). "Nova Estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais" https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391

Comissão Europeia (Julho, 2020), "Comunicação Da Comissão Ao Parlamento Europeu, Ao Conselho Europeu, Ao Conselho, Ao Comité Económico E Social Europeu E Ao Comité Das Regiões Sobre A Estratégia Da Ue Para A União Da Segurança" disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0605

Comissão Europeia (Maio, 2015) "Agenda Europeia para a Segurança". https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM:2015:0185:FIN, Document 52015DC0185

Comissão Europeia (Março, 2020). Coronavirus outbreak - Joint Statement European Commission, ENISA, CERT-EU and Europol in https://digital-strategy.ec.europa.eu/en/news/coronavirus-outbreak-joint-statement-european-commission-enisa-cert-eu-and-europol

Comissão Europeia. "New EU Cybersecurity Strategy and new rules to make physical and digital crital entities more resilient". (Dezembro 2020). Documento IP/20/2391, disponível em https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

Comissão Nacional de Proteção de Dados, Diretriz/2023/1, de 10 de Janeiro https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122048

Comité de Contacto das Instituições Superiores de Controlo da União Europeia. (2020, Dezembro). "Compêndio de auditoria, " A cibersegurança na UE e nos seus Estados Membros" https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_PT.pdf

Committe on Commerce, Science, and Transportation. (Março, 2014). "A "Kill Chain" https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

Communication From The Commission To The European Parliament And The Council: Making the most of NIS – towards the effective implementation of Directive (UE) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union" COM/2017/0476 final, disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476

Committe on Commerce, Science, and Transportation. (2014, Março). "A "Kill Chain" Analysis of the 2013 Target Data Breach" https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

Comunicação Conjunta Do Parlamento Europeu, Do Conselho Europeu, Do Conselho, Do Comité Económico E Social E Do Comité Das Regiões (Junho 2020) "Combater a desinformação sobre a COVID-19: repor a verdade dos factos". https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020JC0008

Conceito Estratégico de Defesa Nacional, Resolução do Conselho de Ministros n.º 19/2013, de 5 de Abril, p.22

Conselho da Prevenção da Corrupção. "Recomendação do Conselho de Prevenção da Corrupção sobre Boas Práticas de Cibersegurança (Abril, 2022) https://www.cpc.tcontas.pt/documentos/recomendacoes/recomendacao_cpc_20220405.pdf

Conselho da União Europeia (2016). "Implementation Plan on Security and Defence" https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf, 14392/16

Comissão Nacional de Proteção de Dados (2022). Relatório de Atividades de 2022. Disponível em: https://www.cnpd.pt/media/tutpevyh/relato-rio_2022.pdf

CORREIA, João Conde (2014, Julho-Set), "Prova Digital: as leis que temos e a lei que devíamos ter", Revista do Ministério Público, n.º 139, https://rmp.smmp.pt/indice-do-no-139/, pp.29 a 59".

Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications, 13(5).

Despacho do Ministro da Defesa n.º 13692/2013, de 28 de Outubro. "Orientação para a política de Ciberdefesa Nacional" https://files.dre.pt/2s/2013/10/208000000/3197631979.pdf

European Data Protection Board (EDPB) (Janeiro, 2022). "Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations, disponível em https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en

Eu Monitor - Explanatory Memorandum to COM(2020)823 - Measures for a high common level of cybersecurity across the Union, disponível em https://www.eumonitor.eu/9353000/1/j4nvhdfdk3hydzq_j9vvik7m1c3gyxp/vlenlgffo5zv

Eurobarómetro (2022) "Flash Eurobarómetro 496 PMEs e crime cibernético". Disponível em: https://europa.eu/eurobarometer/surveys/detail/2280

European Commission, Directorate-General for Migration and Home Affairs, (2022). "SMEs and cybercrime : summary, Publications Office of the European Union." https://data.europa.eu/doi/10.2837/89101

European Court of Auditors. (2019), "Challenges to effective EU cybersecurity policy", disponível em https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

Eurostat (Dezembro, 2022) "Digital economy and society statistics - households and individuals", disponível em https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access

Eurostat (Dezembro, 2022). "ICT security in enterprises", disponível em https://ec.europa.eu/eurostat/statistics-explained/images/a/a7/ICT_security_2022_-_graphs_and_tables.xlsx

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision support systems, 86, 13-23. https://doi.org/10.1016/j.dss.2016.02.012

FBI (2021) Internet Crime Report/Internet Crime Complaint Center https://www.ic3.gov/Media/Y2022/PSA220504

GALP Energia SGPS, S.A. (2022). "Relatório do Governo Societário". Disponível para consulta em https://www.galp.com/corp/Portals/0/Recursos/Investidores/SharedResources/Relatorios/pt/2022/AIRGalp2022PT3Book3CorporateGovernance.pdf

GALP Energia SGPS, S.A. (2022) "Relatório Integrado de Gestão 2022". https://www.galp.com/corp/Portals/0/Recursos/Investidores/SharedResources/Relatorios/pt/2022/AIRGalp2022PT1Book1IMRFull.pdf

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), 81-85. https://doi.org/10.1145/636772.636774

Gelbstein, E. (2012). "Protecting critical information infrastructures". Nação e defesa, 133, 128–146. http://hdl.handle.net/10400.26/42468

Gordon, S.; Ford, R. "On the Definition and Classification of Cybercrime". J. Comput. Virol. 2006, 2, 13–20.

Huang, K., & Pearlson, K. (2019). "For what technology can't fix: Building a model of organizational cybersecurity culture". http://hdl.handle.net/10125/60074

IBM Security (2023). "Cost of a Data Breach Report 2023" https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

IBM Security (2023). "Cost of a Data Breach Report 2023" https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

Instituto Português da Qualidade (2023). "10 razões para usar Normas". https://www.ipq.pt/normalizacao/a-importancia-da-normalizacao/razoes-para-o-uso-das-normas/

International Organization for Standardization (2022). "ISO/IEC 27001, Information security management systems" https://www.iso.org/standard/27001

International Telecommunication Union (ITU) (2020). Global Cybersecurity Index. Disponível em https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

International Telecommunication Union (ITU). "ITU-D Cybersecurity Program Global Cybersecurity Index – GCIv5 Reference Model," disponível em https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2E.pdf

Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, Join/2013/01 Final, Document 52013JC0001, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, Join/2013/01 Final, Document 52013JC0001, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

Lamberti, Lorenzo (2019), Analysing and protecting agains existing cyber attacks. In https://urn.fi/URN:NBN:fi:amk-2019052913332

Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. The Palgrave handbook of international cybercrime and cyberdeviance, 91-116.

MARSH & MICROSOFT (Fevereiro 2018). "By the Numbers: Global Cyber Risk Perception Survey" https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20Microsoft%20Global%20Cyber%20Risk%20Perception%20Survey%20February%202018.pdf

Marsh & Microsoft (2022). "2022 Global Cyber Risk Survey" https://www.marsh.com/ug/services/cyber-risk/insights/global-cyber-risk-survey.html

Maurer, T. & Nelson, Arthur. (2021) "The Global Cyber Threat". International Monetary Fund https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

Ministério Público (2019, Abril) "Meios de Obtenção de Prova e Medidas Cautelares e de Polícia", Coleção formação, Centro de Estudos Judiciários.

Ministério Público. Nota Prática n.º 3/2014, 12 de Junho de 2014 "Pedidos de informações a fornecedores de serviços Internet dos Estados Unidos da América - pedidos à Google, à Facebook e à Microsoft - pedidos de cooperação internacional para EUA" – Gabinete Cibercrime. https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_3_isp_eua.pdf

National Institute Of Standards and Technology (NIST) (2023, Janeiro). "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework" https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

Navor, P. (2021). "The Effects of Palavra passe Length and Complexity on Palavra passe Resiliency" in http://hdl.handle.net/10790/6830,

Nicole M. Lee (2018) Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom, Communication Education, 67:4, 460-466, DOI: 10.1080/03634523.2018.1503313

NOS SGPS, S.A. (2022). "Anual Integrated Report 2022". disponível para consulta em https://web3.cmvm.pt/sdi/emitentes/docs/PC84994.pdf

Pedahzur, A. (2009). The Israeli Secret Services & the struggle against Terrorism. Nova Iorque: Columbia University Press.

Pereira, Joel Timóteo Ramos, Compêndio Jurídico da Sociedade da Informação, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1035.

Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. Business Horizons, 64(6), 763-774. DOI: 10.1016/j.bushor.2021.07.012

Phillips, K.; Davidson, J.C.; Farr, R.R.; Burkhardt, C.; Caneppele, S.; Aiken, M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sci. 2022, 2, 379-398. https://doi.org/10.3390/forensicsci2020028

Principal for Responsible Investment (2022). ''Annual Report 2022)''. https://www.unpri.org/annual-report-2022/signatories

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In 29th European Safety and Reliability Conference (pp. 4036-4043).

Shao, C., Ciampaglia, G., Varol, O., Flammini, A. & Menczer, F. (2017). ''The spread of fake news by social bots''. arXiv:1707.

Shao, C., Ciampaglia, G., Varol, O., Flammini, A. & Menczer, F. (2017). ''The spread of fake news by social bots''. Universidade de Indiana, Bloomington, Estados Unidos da América. Disponível em https://www.andyblackassociates.co.uk/wpcontent/uploads/2015/06/fakenewsbots.pdf

SONAE SGPS S.A (2022), ''Relatório Anual Integrado 2022'' disponível para consulta em https://www.sonae.pt/fotos/dados_fin/relatoriointegrado_2022_pt_1277178973642cbcbfd0004.pdf

SWINARSKI, Christophe. Introdução ao direito internacional humanitário, Brasília: Comitê Internacional de Direitos Humanos, 1996, p. 18.

The European Cybersecurity Competence Centre (2023). ''European Cybersecurity Competence Centre and Network.'', disponível em https://cybersecurity-centre.europa.eu/index_en

Thomas, D.; Loader, B. Introduction-Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age; Thomas, D., Loader, B., Eds.; Routledge: London, UK, 2000.

Tribunal de Justiça da União Europeia (TJUE). ECLI:EU:C:2010:321 disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=79665&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=541615

USA.gov, Government Information, "Cybersecurity budget fiscal year 2020: CYBERSECURITY FUNDING" https://www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf

Venâncio, Pedro Dias, "As Disposições Processuais Relativas a Dados Informáticos na Lei do Cibercrime", JusJornal, N.º 1183, 24 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer.

Verizon (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

Von Solms, R. and Van Niekerk, J. (2013) From Information Security to Cyber Security. Computers & Security, p.101. https://doi.org/10.1016/j.cose.2013.04.004

White, Joshua S.; Matthews, Jeanna N. (2013). [IEEE 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE) - Fajardo, PR, USA (2013.10.22-2013.10.24)] 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE) - It's you on photo?: Automatic detection of Twitter accounts infected with the Blackhole Exploit Kit. , (), 51–58. doi:10.1109/malware.2013.6703685

WhiteHouse, "Cybersecurity budget fiscal year 2022: INFORMATION TECHNOLOGY AND CYBERSECURITY FUNDING" https://www.whitehouse.gov/wp-content/uploads/2022/03/ap_16_it_fy2023.pdf

Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart, A review of cyber security risk assessment methods for SCADA systems, Computers & Security, Volume 56, 2016, Pages 1-27,https://doi.org/10.1016/j.cose.2015.09.009.

Legislação, normas e jurisprudência

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148 , Document 32016L1148.

Comissão Europeia, Estratégia para o Mercado Único Digital na Europa, COM(2015) 192 final, de 6 de Maio de 2015.

Comissão Europeia (2023). "Plano de Recuperação Europeia" https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_pt

Comissão Europeia (Julho 2021) "RECOMENDAÇÃO (UE) 2021/1086 DA COMISSÃO de 23 de Junho de 2021 relativa à criação de uma Ciberunidade Conjunta" https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021H1086, L 237/1

Concelho Europeu (2003). "Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems", https://rm.coe.int/168008160f

Conselho da União Europeia. 2010/427/UE: Decisão do Conselho, de 26 de Julho de 2010 , que estabelece a organização e o funcionamento do Serviço Europeu para a Acção Externa, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010D0427 JOUE L 201 de 03.08.2010, pp. 30 a 40.

Conselho Europeu. Convenção do Cibercrime. Tratado Europeu No. 185, disponível em https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185;

DECISÃO DE EXECUÇÃO (UE) 2017/179 DA COMISSÃO de 1 de Fevereiro de 2017 que estabelece as disposições processuais necessárias para o funcionamento do grupo de cooperação ao abrigo do artigo 11.o, n.o 5, da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32017D0179, Document 32017D0179.

Decreto-Lei n.º 62/2011 de 9 de Maio. Diário da República, 1.ª Série, n.º 89, 2624- 2627. Ministério da Defesa Nacional. (Estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes e transpõe a Diretiva n.º 2008/114/CE, de 8 de Dezembro).

Decreto-Lei n.º 65/2021, de 30 de Julho. Diário da República n.º 147/2021, Série I de 2021-07-30, páginas 8 - 21 (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 69/2014, de 9 de Maio. Diário da República, 1.ª Série, n.º 89, 2712- 2719. Presidência do conselho de Ministros. (Aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança).

Diretiva (UE) 2022/2464 do Parlamento Europeu e do Conselho de 14 de Dezembro de 2022 que altera o Regulamento (UE) n.o 537/2014, a Diretiva 2004/109/CE, a Diretiva 2006/43/CE e a Diretiva 2013/34/UE no que diz respeito ao relato de sustentabilidade das empresas, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2464, Document 32022L2464

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, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1690926026132, Document 32022L2555

Diretiva 2013/40/EU do Parlamento Europeu e do Concelho de 12 de Agosto de 2013 relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. Decisão 2005/222/JHA. Document 32013L0040. Disponível em https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040

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, disponível para consulta em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2557&qid=1687729156275, Document 32022L2557

Lei n.º 109/2009, de 15 de Setembro. Diário da República, 1.ª Série, n.º 179, 6319- 6325. Assembleia da República. (Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro).

Lei n.º 38/2009, de 20 de Julho. Diário da República, 1.ª série — N.º 138 — 20 de Julho de 2009. Assembleia da República. (Lei Quadro da Política Criminal)

Lei n.º 46/2018, de 13 de Agosto. Diário da República n.º 155/2018, Série I de 2018-08-13, páginas 4031 – 4037. (Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União)

Lei n.º 49/2008, l de 12 de Agosto de 2008. Diário da República n.º 165/2008, Série I de 2008-08-27. Assembleia da República. Lei de Organização da Investigação Criminal.

Lei n.º 37/2008, 6 de Agosto. Diário da República n.º 151/2008, Série I de 2008-08-06. Assembleia da República. (Aprova a orgânica da Polícia Judiciária)

Regulamento (CE) n.° 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência da União Europeia para a Cibersegurança (Texto relevante para efeitos do EEE), , disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32004R0460, Documento 32004R0460

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE), Document 32016R0679 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança), disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32019R0881, Documento 32019R0881

Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de Abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança), https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019R0881, Document 32019R0881

Regulamento (UE) 2021/241 do Parlamento Europeu e do Conselho de 12 de Fevereiro de 2021 que cria o Mecanismo de Recuperação e Resiliência, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32021R024, Document 32021R0241

Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de Abril de 2021 que cria o Programa Europa Digital, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32021R0694, Document 32021R0694

Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho de 28 de Abril de 2021 que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação, que define as suas regras de participação e difusão, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021R0695, Document 32021R0695

Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho, de 28 de Abril de 2021, que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação, que define as suas regras de participação e difusão, e que revoga os Regulamentos (UE) n.o 1290/2013 e (UE) n.o 1291/2013 (JO L 170 de 12.5.2021), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32021R0695 Document 32021R0695

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 e a Rede de Centros Nacionais de Coordenação, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32021R0887, Document 32021R0887.

Regulamento n.º 183/2022, de 21 de Fevereiro. Diário da República n.º 36/2022, Série II de 2022-02-21, páginas 34 – 39. 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) https://dre.pt/dre/detalhe/regulamento/183-2022-179325870

Resolução do Conselho de Ministros 42/2012, de 13 de Abril. Diário da República n.º 74/2012, Série I de 2012-04-13, páginas 1925 – 1926. Presidência do Conselho de Ministros. (Cria a Comissão Instaladora do Centro Nacional de Cibersegurança) https://dre.pt/dre/detalhe/resolucao-conselho-ministros/42-2012-552560

Resolução do Conselho de Ministros n.º 115/2017, de 24 de Agosto,. Diário da República n.º 163/2017, Série I de 2017-08-24. Presidência do Conselho de Ministros. (Cria o grupo de projeto denominado «Conselho Superior de Segurança do Ciberespaço») https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/115-2017-108051990

Resolução do Conselho de Ministros n.º 36/2015, de 12 de Junho, Diário da República n.º 113/2015, Série I de 2015-06-12, páginas 3738 – 3742. (Aprova a Estratégia Nacional de Segurança do Ciberespaço), https://dre.pt/dre/detalhe/resolucao-conselho-ministros/36-2015-67468089

Resolução do Conselho de Ministros n.º 92/2019, de 5 de Junho, Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962

Tratado sobre o Funcionamento da União Europeia (2016) C 202/47, disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF

TJUE. Acórdão de 6 de Outubro de 2015, Schrems, C-362/14, ECLI:EU:C:2015:650 https://curia.europa.eu/juris/liste.jsf?num=C-362/14

TJUE. Acórdão de 16 de Julho, Facebook Ireland e Schrems, C-311/18, ECLI:EU:C:2020:559. https://curia.europa.eu/juris/liste.jsf?num=C-311/18&language=PT

Referências Bibliográficas Eletrónicas (Webgrafia):

Agência Lusa (2022, Maio) "PJ defende que precisa de metadados para investigar cibercrime" DNotícias. https://www.dnoticias.pt/2022/5/4/309372-pj-defende-que-precisa-de-metadados-para-investigar-cibercrime/#

Banco de Portugal. "Criptoativos, stablecoins e euro digital? Descubra as diferenças." https://www.bportugal.pt/page/criptoativos-stablecoins-e-euro-digital-descubra-diferencas-1

Caçador, Fátima (Maio, 2022). "Davos: Galp junta-se a 17 gigantes petrolíferas em acordo para proteção contra ataques informáticos". SapoTek. Disponível em https://tek.sapo.pt/noticias/computadores/artigos/davos-galp-junta-se-a-17-gigantes-petroliferas-em-acordo-para-protecao-contra-ataques-informaticos

Centro Nacional de Cibersegurança (CNCS) (2022). Quadro Nacional de Certificação da Cibersegurança https://www.cncs.gov.pt/pt/quadro-nacional-de-certificacao-da-ciberseguranca/

Centro Nacional de Cibersegurança (CNCS) (2023). "Certificação QNRCS", https://www.cncs.gov.pt/pt/certificacao-nacional/

Centro Nacional de Cibersegurança (CNCS). (2022). "Quadro Nacional de Certificação da Cibersegurança" https://www.cncs.gov.pt/pt/quadro-nacional-de-certificacao-da-ciberseguranca/

Comissão Europeia. "Comissão congratula-se com o acordo político sobre o Centro e a Rede de Competências em matéria de Cibersegurança" https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2384, IP/20/2384

Conselho Europeu e Conselho da União Europeia (Maio 2023). "Cibersegurança: como combate a UE as ciberameaças" https://www.consilium.europa.eu/pt/policies/cybersecurity/

Cordina, Corinne (Abril, 2023). "Fichas temáticas sobre a União Europeia: Pequenas e médias empresas." https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/pt/FTU_2.4.2.pdf

Cybersecurity & Infrastructure Security Agency (2021, Fevereiro). "Understanding Denial-of-Service Attacks", https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

ENISA. (Março, 2023) "ENISA Threat landscape: transport sector (January 2021 to October 2022" MARCH 2023 disponível em https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape/@@download/fullReport

Eurojust. Joint Investigation Teams (2023) https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams

EUROPOL (Março, 2022). "European Cybercrime Centre" disponível em https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Europol. (2018, Abril). "World's biggest marketplace selling internet paralysing DDoS attacks taken down" https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down.

Google. (Consultado em 2023). "As bases de dados de registo funcionam como grossistas para o registo de domínios. Os domínios utilizam extensões de nomes de domínios, também conhecidas como domínios de nível superior ou TLDs. Por exemplo, a empresa Verisign gere o registo dos domínios .com e .net." "Bases de Dados de Registo"

Imprensa Nacional Casa da Moeda. "Certificação de Maturidade Digital" https://selosmaturidadedigital.incm.pt/

International Organization for Standardization. "ISO/IEC 27001 Information security management systems", disponível no site https://www.iso.org/standard/27001

Ivan B. (2019, Novembro). "O que é o ransomware Petya?" Academy Avast. https://www.avast.com/pt-br/c-petya

J.Broad, William, et al. (2011, Janeiro) "Israeli Test on Worm Called Crucial in iran Nuclear Delay). The New York Times. Disponível em https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Jonathan S., Jim F. (2017, Outubro). "Yahoo says all three billion accounts hacked in 2013 data theft". Reuters. https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1

Kaspersky "What is WannaCry ransomware?", Resource Center. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Kelly, S and Resnick-ault. (2021, Junho). "One palavra passe allowed hackers to disrupt Colonial Pipeline, CEO tells senators". Reuters. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

Kapersky (2010, Setembro). "Kaspersky Lab provides its insights on Stuxnet worm". Corporate News. https://www.kaspersky.com/about/press-releases/2010_kaspersky-lab-provides-its-insights-on-stuxnet-worm

Kirchgaessner, S. et. al. (2023, Fevereiro) "Revealed: the hacking and disinformation team meddling in elections". The Guardian. Europe Edition. https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan

Li, Z., & Shahidehpour, M. (2017). Deployment of cybersecurity for managing traffic efficiency and safety in smart cities. The Electricity Journal, 30(4), 52-61. https://doi.org/10.1016/j.tej.2017.04.003

McKeon, J. (Fevereiro 2022). "HealthIT Security. CaptureRx to Consider Filing For Bankruptcy if $4.75M Settlement Not Approved", HealthITSecurity disponível em https://healthitsecurity.com/news/capturerx-to-consider-filing-for-bankruptcy-if-4.75m-settlement-not-approved

Microsoft (2023). What is business email compromisse.), in https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec?

Office of Public Affairs. U.S. Department of Justice. (2021, Junho) "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside" https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside;

Office of Public Affairs. U.S. Department of Justice. (2023, Janeiro)." U.S. Department of Justice Disrupts Hive Ransomware Variant" https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

OVHcloud. "O Domain Name System (DNS)" em https://www.ovhcloud.com/pt/domains/dns-server/

PORDATA (2023). "Pequenas e médias empresas em % do total de empresas: total e por dimensão" https://www.pordata.pt/portugal/pequenas+e+medias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimensao-2859

Portugal.Gov. "PRR vai investir 47 milhões na formação em cibersegurança". Portugal.Gov.pt. https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=prr-vai-investir-47-milhoes-na-formacao-em-ciberseguranca

Reuters (2016) “Empresas de cibersegurança afirmam que hackers que invadiram BC de Bangladesh atacaram outros bancos” disponível em https://www.reuters.com/article/tech-hackers-bc-idBRKCN0YI1PY,

Toyota. “Privacy Initiatives” https://global.toyota/en/sustainability/privacy/initiatives/

World Economic Forum (2023, Janeiro). “2023 Global Risk Report” disponível em https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/