bilingual edition

ptsoc {news}

NIS2: a caminho de uma política de soberania digital

3 perguntas a Gonçalo Silva

CSIRT in a Box por Carlos Friaças

15

NIS2: On the road to a digital sovereignty policy

3 questions to Gonçalo Silva

CSIRT in a Box by Carlos Friaças

.pt

NIS2: a caminho de uma política de soberania digital

Há cerca de dois anos, na PTSOC News #8, falámos sobre a diretiva europeia EU 2022/2055, que conhecemos pela designação NIS 2, publicada no Jornal Oficial da EU a 27 de dezembro de 2022.

Em termos simples, a Diretiva NIS2 é a legislação da UE em matéria de cibersegurança e, nesse sentido, prevê medidas jurídicas para aumentar o nível geral de cibersegurança nos países membros da Comunidade.

Esta diretiva vem modernizar o quadro jurídico existente para acompanhar o aumento da digitalização e a evolução do panorama das ameaças à cibersegurança. Ao alargar o âmbito de aplicação das regras de cibersegurança a novos setores e entidades, melhora ainda mais a resiliência e a capacidade de resposta a incidentes das entidades públicas e privadas, das autoridades competentes e da UE no seu conjunto.

A Diretiva prevê medidas jurídicas para aumentar o nível geral de cibersegurança na UE, assegurando, nomeadamente:

- a preparação dos Estados-Membros, exigindo-lhes que estejam devidamente equipados. Por exemplo, com uma equipa de resposta a incidentes de segurança informática e uma autoridade nacional competente em matéria de redes e sistemas de informação;
- a cooperação entre todos os Estados-Membros, através da criação de um grupo de cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros;

NIS2: On the road to a digital sovereignty policy

About two years ago, in PTSOC News #8, we talked about the European directive EU 2022/2055, which we know as NIS 2, published in the Official Journal of the EU on 27 December 2022.

In simple terms, the NIS2 Directive is the EU's cybersecurity legislation, providing for legal measures to increase the general level of cybersecurity in the Community's member countries.

This directive modernises the existing legal framework to keep up with the increase in digitalisation, and the evolution of the cybersecurity threat landscape. By extending the scope of cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacity of public and private entities, competent authorities, and the EU as a whole.

The Directive provides for legal measures to increase the general level of cybersecurity in the EU, namely ensuring:

- That Member States are prepared, by requiring them to be properly equipped. For example, with a computer security incident response team and a competent national authority for networks and information systems;
- Co-operation between all Member States, through the creation of a co-operation group to support and facilitate strategic co-operation and the exchange of information between Member States;

- uma cultura de segurança em setores vitais para a nossa economia e sociedade e que dependem fortemente das TIC, como a energia, os transportes, a água, a banca, as infraestruturas do mercado financeiro, os cuidados de saúde e as infraestruturas digitais.

Quando a diretiva for transcrita para o quadro legislativo português, as empresas identificadas pelos Estados-Membros como operadores de serviços essenciais nos setores acima referidos terão de tomar medidas de segurança adequadas e notificar as autoridades nacionais competentes de incidentes graves. Além disso, os principais prestadores de serviços digitais, como os motores de busca, os serviços de computação em nuvem e os mercados online, terão de cumprir os requisitos de segurança e de notificação previstos.

- A culture of security in sectors that are vital to our economy and society and that rely heavily on ICT, such as energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructures.

When the directive is transposed into the Portuguese legislative framework, companies identified by Member States as essential service operators in the above-mentioned sectors will have to take appropriate security measures and notify the competent national authorities of serious incidents. In addition, the main digital service providers, such as search engines, cloud computing services, and online marketplaces will have to fulfil the envisaged security and notification requirements.

Foto: mattegg

Trata-se de uma diretiva com elevado grau de complexidade, como o prova o facto de, dois anos depois, terem sido poucos os estados-membros que realizaram a sua transposição para o respetivo quadro legislativo

This is a highly complex directive, as evidenced by the fact that, two years on, few member states have transposed it into their national legislative framework - the deadline set by the European Commission

nacional – o prazo-limite dado pela Comissão Europeia expirou em 17 de outubro de 2024 e, à data, 23 países (entre eles, Portugal) não tinham ainda realizado essa transposição.

Em Portugal, o processo aproxima-se agora do seu termo, tendo a consulta pública relativa à transposição da diretiva decorrido entre 22 de novembro e 31 de dezembro de 2024. João de Araújo Ferraz, senior associate da VdA e jurista especializado na área da cibersegurança, explica que há ainda alguns passos a cumprir: "o diploma entrará em vigor 30 dias após a sua publicação, sendo que uma parte considerável das suas obrigações apenas produzirá efeitos 18 meses após a entrada em vigor." Além disso, "a proposta poderá ainda vir a sofrer alterações, em resultado da consulta pública".

Num evento recente Rui Pereira, consultor do Centro Nacional de Cibersegurança, salientou a importância desta diretiva, defendendo que ela irá "contribuir, e em muito, para melhorar a cibersegurança em Portugal" e que, face à lei anterior, apresenta "maior detalhe, mais transparência e objetividade: há agora uma harmonização mais completa."

Mas, talvez mais importante, salienta o mesmo responsável, é o facto de que esta é uma diretiva muito mais abrangente do que a anterior. Rui Pereira chama a atenção para o facto de "NIS" corresponder às iniciais de "Network Information Systems"; contudo, apesar da manutenção do acrónimo, essa

expired on 17 October 2024 and, to date, 23 countries (including Portugal) had still not transposed it.

In Portugal, the process is now nearing its end, with the public consultation on the transposition of the directive having taken place between 22 November and 31 December 2024. João de Araújo Ferraz, senior associate at VdA and a lawyer specialised in cybersecurity, explains that there are still some steps to be taken: 'The law will come into force 30 days after its publication, and a considerable part of its obligations will only take effect 18 months after its entry into force.' What's more, 'the proposal may yet be amended as a result of the public consultation.'

At a recent event, Rui Pereira, a consultant for the Portuguese National Cybersecurity Centre, stressed the importance of this directive, arguing it will 'contribute greatly to improving cybersecurity in Portugal' and that, compared to the previous law, it presents 'greater detail, more transparency, and objectivity: there is now a more complete harmonisation.'

But perhaps more importantly, Ferraz emphasises, is that this is a much more comprehensive directive than the previous one. Rui Pereira points out that 'NIS' stands for 'Network Information Systems'; however, despite keeping the acronym, this terminology has simply disappeared from

terminologia simplesmente desapareceu da nova Diretiva, a qual coloca sobretudo a ênfase no nível de proteção e preparação, relativamente à cibersegurança, das empresas (e organismos públicos) dos setores mais críticos – ou seja, muito para além das próprias infraestruturas de TI.

A Diretiva impõe aos estados-membros da União Europeia a adoção de um quadro estratégico nacional de cibersegurança (Portugal tem essa estratégia desde 2015, revista em 2019 sob a designação Estratégia Nacional de Segurança do Ciberespaço), para estabelecer os recursos necessários e as medidas políticas e regulamentares adequadas a manter um elevado nível de cibersegurança.

A quem se destina a NIS 2?

A NIS 2 classifica as entidades abrangidas pela diretiva, "para efeitos de cumprimento das obrigações relativas às medidas de gestão dos riscos de cibersegurança e à notificação", em duas categorias: entidades "essenciais" e "importantes", refletindo a medida em que são fundamentais no que respeita ao seu setor ou ao tipo de serviço que prestam, bem como a sua dimensão (ficam de fora as micro e pequenas empresas).

São os Estados-membros quem estabelece e comunica à Comissão a lista e categoria destas entidades – ver nesta edição o artigo "NIS2: a quem se aplica e o que se

the new Directive, which emphasises the level of protection and cybersecurity preparedness of companies (and public bodies) in the most critical sectors - in other words, far beyond the IT infrastructures themselves.

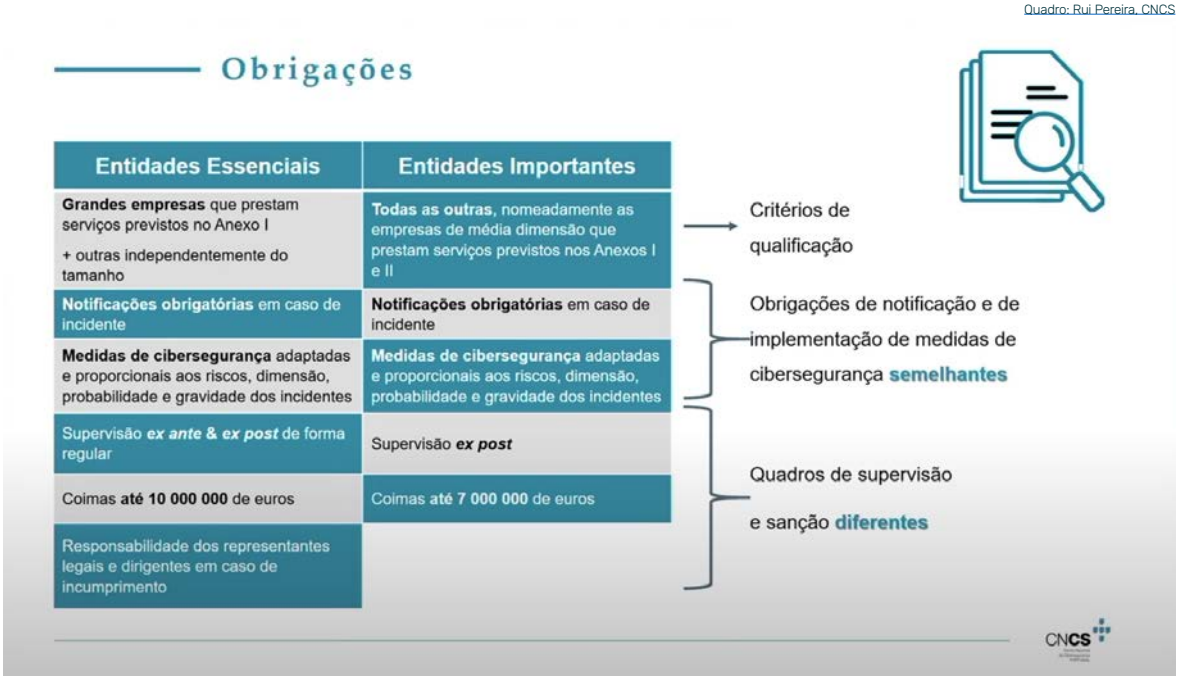
The Directive requires EU member states to adopt a national cybersecurity strategy framework (Portugal has had this strategy since 2015, revised in 2019 under the name National Strategy for Cyberspace Security), to establish the necessary resources and the appropriate political and regulatory measures to maintain a high level of cybersecurity.

NIS2: Whom does it applies to?

NIS 2 classifies the entities covered by the directive 'for the purpose of complying with the cybersecurity risk management measures and notification obligations', into two categories: 'essential' entities and 'important' entities, reflecting the extent to which they are essential with respect to their industry or the type of service they provide, as well as their size (micro and small companies are excluded).

The Member States are the ones who establish and communicate to the Commission the list and category of these entities - refer to article 'NIS2: who it applies to and what's next for the companies covered' by João de Araújo Ferraz, in this issue.

Quadro: Rui Pereira, CNCS



segue para as empresas abrangidas" de João de Araújo Ferraz.

No entanto, a própria Diretiva, nos seus Anexos I (Setores de Importância Crítica) e II (Outros Setores Críticos), define desde já quais os setores de atividade que irão ser impactados por estas medidas – um total de 11 setores no Anexo I e mais sete no Anexo II.

Impactos da implementação

A par dos benefícios que a conformidade pelo NIS 2 irá trazer, existe a questão relacionada com os custos da implementação das medidas – não apenas para as entidades abrangidas, mas para os consumidores em geral. A consultora Frontier Economics, es-

However, the Directive itself, in its Annexes I (Sectors of Critical Importance) and II (Other Critical Sectors), already defines which sectors of activity will be impacted by these measures - a total of 11 sectors in Annex I and a further 7 in Annex II.

Impacts of implementation

Alongside the benefits that NIS 2 compliance will bring, there is the question of the costs of implementing the measures - not just for the entities covered, but for consumers in general. The consultancy firm Frontier Economics, which specialises in economic consultancy services ranging from public policies, regulation, and competition to energy and climate change, recently

pecializada em serviços de consultoria económica que vão desde as políticas públicas, regulamentação e concorrência até à energia e alterações climáticas, publicou recentemente um estudo especificamente sobre as implicações da NIS 2 em Portugal.

A sua conclusão é que "o reforço das medidas de cibersegurança é bem-vindo", mas é também importante "que os decisores políticos garantam que os benefícios dessas medidas compensam os custos para os consumidores, as empresas e a sociedade em geral". Esta consultora estima em cerca de 530 milhões de euros o custo da implementação das medidas da Diretiva NIS 2 em Portugal.

E, como refere João de Araújo Ferraz, mesmo que uma determinada empresa ou entidade não esteja abrangida pela necessidade de implementação das medidas contidas na NIS2, é provável que muitas delas "venham a ter de ser implementadas (em maior ou menor medida), uma vez que as entidades abrangidas irão exigir aos seus fornecedores e prestadores de serviços a prova de que cumprem requisitos importantes de cibersegurança, sob pena de poderem eles próprios ser responsabilizados pelo incumprimento do diploma."

Marta Moreira Dias, do Board of Directors .PT, no artigo "O Goldilocks Effect na transposição da Diretiva NIS2" nesta edição, salienta a necessidade de encontrar equilíbrios quando escreve que "a perceção do chamado efeito

published a study specifically on the implications of NIS 2 in Portugal.

It concludes that 'enhanced cybersecurity measures are welcome', but it is also important for 'policymakers to ensure that the benefits of these measures outweigh the costs to consumers, businesses and the wider society.' The consultancy firm estimates that implementing the NIS 2 Directive in Portugal will cost around 530 million euros.

And, as João de Araújo Ferraz points out, even if a particular company or entity is not covered by the need to implement the measures contained in NIS2, it is likely that many of them 'will have to be implemented (to a greater or lesser extent), since the entities covered will require their suppliers and service providers to prove that they fulfil important cybersecurity requirements, otherwise they themselves could be held liable for non-compliance with the law.'

Marta Moreira Dias, from the Board of Directors of .PT, in the article 'The Goldilocks Principle in the transposition of the NIS2 Directive', in this issue, emphasises the need to find balances when she writes that 'the perception of the so-called Goldilocks Principle in the wording of national laws of EU origin on cybersecurity seems to be, consciously or not, a response by national legislators to the ultra-regulation that has characterised EU

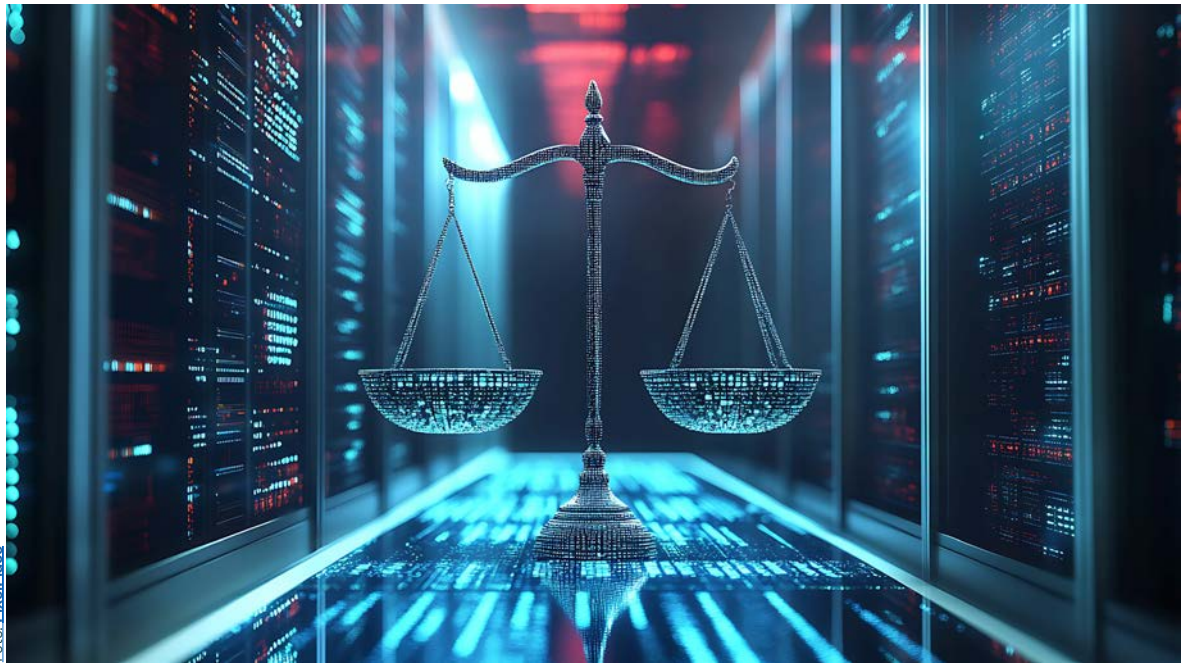


Foto: PixelPlace

Goldilocks, no articulado de leis nacionais de fonte comunitária no âmbito da Cibersegurança, parece ser, de forma consciente ou não, uma resposta do legislador nacional à ultra-regulação que tem marcado o edifício legislativo comunitário, muitas vezes associada a efeitos adversos, como seja a criação de espaços pouco propícios à inovação e à concorrência, num mercado saturado de elevados requisitos de conformidade."

O Centro Nacional de Cibersegurança tem uma página dedicada à NIS 2 que tenta responder às principais dúvidas que se colocam face a esta nova diretiva, e que pode ser consultado aqui. A partir da mesma página é também possível aceder a um email específico para responder a questões sobre a aplicação da NIS 2

legislation, often associated with adverse effects, such as the creation of spaces not conducive to innovation and competition in a market saturated with high compliance requirements.'

The Portuguese National Cybersecurity Centre has a page dedicated to NIS 2 which tries to answer the main questions raised by this new directive, which can be consulted here. The same page also shares a specific email address to answer questions on the application of NIS 2

O Goldilocks Principle na transposição da Diretiva NIS2
The Goldilocks Principle in the transposition of the NIS2 Directive

Marta Moreira Dias, Board of Directors, .PT

O "Princípio Goldilocks" – assim batizado a partir dos ensinamentos da história infantil dos "Três Ursinhos" – resume o que nos parece ter guiado aquela que foi a opção do legislador nacional no âmbito da atual proposta de transposição da Diretiva NIS 2.

O diploma – cuja versão consolidada refletirá, expectavelmente, alguns dos muitos contributos que resultaram do período em que o articulado esteve em discussão pública – assumirá as vestes de Regime Jurídico da Cibersegurança o que na prática unifica dois conceitos, segurança e ciberespaço, que emergiam da Lei n.º 46/2028, de 13 de agosto. Esta foi a lei que transpôs a Diretiva NIS e cristalizou no quadro jurídico nacional o Regime Jurídico da Segurança do Ciberespaço.

A perceção do chamado Princípio Goldilocks no articulado de leis nacionais de fonte comunitária no âmbito da Cibersegurança parece ser, de forma consciente ou não, uma resposta do legislador nacional à ultra-regulação que tem marcado o edifício legislativo comunitário. Esta tem surgido muitas vezes associada a efeitos adversos, como seja a criação de espaços pouco propícios à inovação e à concorrência, num mercado saturado de elevados requisitos de conformidade.

The "Goldilocks Principle" - so named after the teachings of the children's story of the "Three Little Bears" - summarises what seems to have guided the national legislator's choice in the current proposal to transpose the NIS 2 Directive.

The law - the consolidated version of which will hopefully reflect some of the many contributions that resulted from the period during which its wording was under public discussion - will take on the guise of the Cybersecurity Legal Framework, in practice unifying two concepts, security and cyberspace, that emerged from Law no. 46/2028, of 13 August. This was the law that transposed the NIS Directive and crystallised the Portuguese legal framework for the Cyberspace Security Legal Framework.

The perception of the so-called Goldilocks Principle in the wording of national laws of EU origin on cybersecurity seems to be, consciously or not, a response by national legislators to the ultra-regulation that has characterised EU legislation. It has often been associated with adverse effects, such as the creation of spaces not conducive to innovation and competition in a market saturated with high compliance requirements.

Refira-se, a título de parêntesis, que no passado dia 8 de novembro, o Conselho Europeu publicou a Declaração de Budapeste sobre o Novo Acordo de Competitividade Europeia, muito inspirada nos relatórios anteriores de Enrico Letta e Mario Draghi, para reforçar a importância de fortalecer justamente a concorrência, a soberania, a segurança, a resiliência e a influência global da UE nestes domínios.

A procura de um equilíbrio ideal parece estar agora na mira dos nossos legisladores. Mas não é fácil e, sobretudo, torna o processo (ainda mais) moroso. O dia 17 de outubro chegou e, por este ou outro(s) motivos, Portugal não conseguiu cumprir o prazo limite de transposição. Mas com ele estiveram mais 22 Estados-Membros, o que pode revelar que o processo foi, pelo menos à partida, mais complexo que o antecipado.

A centralidade do tema e a urgência de um quadro legislativo sólido, plurissetorial, uniforme na geografia europeia e gerador de confiança e segurança jurídica para cidadãos e organizações serão incontornáveis naquele labor legislativo. Não se pense, contudo, que navegamos num vazio legal ou que o novo Regime Jurídico da Cibersegurança é o icónico farol de La Jument.

Em momento oportuno, já tivemos a oportunidade de nos debruçar sobre muitos dos diplomas legais satélite à matéria da cibersegurança, que saem reforçados com instrumentos como os recentes compromissos plasmados no Pacto do Futuro e, em especial, no "Pacto Digital Global".

As a side note, on 8 November, the European Council published the Budapest Declaration on the New European Competitiveness Deal, much inspired by Enrico Letta and Mario Draghi's previous reports, in order to reinforce the importance of rightly strengthening competition, sovereignty, security, resilience, and the EU's global influence in these areas.

The search for an ideal balance now seems to be in the sights of our legislators. But it is not easy and, above all, it makes the process (even more) time-consuming. 17 October arrived and, for one reason or another, Portugal failed to meet the transposition deadline. But so did 22 other Member States, which might reveal that the process was, at least from the outset, more complex than anticipated.

The centrality of the issue and the urgency for a solid, multi-sectoral legislative framework that is uniform across Europe, and generates trust and legal certainty for citizens and organisations will be unavoidable in this legislative process. Do not think, however, that we are sailing in a legal vacuum or that the new Cybersecurity Legal Framework is the iconic La Jument lighthouse.

At the right time, we have already had the opportunity to take a look at many laws on cybersecurity, which have been strengthened by instruments such as the recent commitments set out in the Pact for the Future and, in particular, the "Global Digital Compact".

Foto: willian

Esta iniciativa central das Nações Unidas, votada no passado dia 22 de setembro, pauta aquilo que são os princípios orientadores para um futuro digital aberto, livre, seguro, acessível, sustentável e centrado no ser humano, endereçando questões como a conectividade, a fragmentação da Internet, os dados, as tecnologias emergentes em geral, mas também a matéria da segurança que sendo um tema global e sem fronteiras deve ser tratado também de formal holística e concertada entre Estados.

Plano internacional

No plano internacional, e a título meramente ilustrativo, destacam-se ainda a primeira Convenção das Nações Unidas contra o Cibercrime, aprovada após três anos de negociações formais, e a Convenção de Budapeste que, embora adotada em 2001, conta já com dois

This central United Nations initiative, voted on 22 September, sets out the guiding principles for an open, free, secure, accessible, sustainable, and human-centred digital future, addressing issues such as connectivity, fragmentation of the Internet, data, emerging technologies in general, but also security, which, as a global issue without borders, must also be dealt with in a holistic and concerted manner between States.

International level

At international level, and by way of illustration, the first United Nations Convention against Cybercrime was approved after three years of formal negotiations, and the Budapest Convention which, although adopted in 2001, already has two additional protocols reflecting the commitment of the signatory countries

Protocolos adicionais que refletem o compromisso dos países signatários em fortalecer a cooperação internacional e aprimorar as ferramentas legais disponíveis para o combate ao cibercrime.

No passado dia 7 de novembro, a ENISA iniciou uma consulta pública com as diretrizes para implementar os requisitos técnicos e metodológicos de gestão de riscos da Diretiva NIS 2. Este documento, embora não vinculativo, e antecipando a própria transposição da Diretiva, é já lido como um guia fundamental de apoio à implementação futura de obrigações que se antecipam pesadas para organizações como os registos de nomes de domínios de topo, onde se inclui o .PT.

Dentro fronteiras, a recém-publicada Estratégia Digital Nacional, identifica a segurança como um dos princípios orientadores basilares à transformação digital do país e identifica a cibersegurança como uma prioridade nacional. Esta priorização será concretizada, nomeadamente, com o incremento de plataformas existentes para a identificação, monitorização e resposta a incidentes de cibersegurança, assegurando uma intervenção ágil em situações de crise.

Toda esta atuação implicará, a nosso ver, um necessário fortalecimento de iniciativas assentes na colaboração entre diferentes atores representativos dos diferentes setores, chamando cada um a agir e cooperar dentro daquilo que são as respetivas competências.

to strengthen international cooperation and improve the legal tools available to fight cybercrime.

On 7 November 2024, ENISA launched a public consultation on the guide-lines for implementing the technical and methodological risk management requirements of the NIS 2 Directive. This document, although non-binding and in anticipation of the transposition of the Directive itself, is already being read as a key guide to support the future implementation of obligations - that are expected to be heavy for organisations such as top-level domain name registries, including .PT.

Within borders, the recently published National Digital Strategy identifies security as one of the basic guiding principles for the country's digital transformation and identifies cybersecurity as a national priority. This prioritisation will be achieved by increasing existing platforms for identifying, monitoring, and responding to cybersecurity incidents, ensuring agile intervention in situations of crisis.

In our understanding, all this action will involve the necessary strengthening of initiatives based on collaboration between different stakeholders representing different sectors, calling on each to act and co-operate within their respective competences.

We are looking forward to the final wording on the new Cybersecurity Legal Framework; we see it as an opportunity to strengthen the

Aguardamos com expectativa a letra final do novo Regime Jurídico da Cibersegurança, e vemos nele uma oportunidade para fortalecer a resiliência cibernética do país e promover um ambiente digital mais seguro e de confiança para todos e todas, que é, refira-se, parte da missão do .PT. A jornada é complexa, mas os benefícios de uma implementação eficaz são inegáveis.

Para o .PT, enquanto entidade essencial, gestor de um Centro de Operações de Segurança (PTSOC) e responsável pela base de dados nacional relativa ao registo de nomes de domínio .pt, a implementação do Regime Jurídico que transponha para a ordem jurídica nacional a Diretiva NIS2 é tão relevante como desafiante.

Desde logo, e nomeadamente, no que respeita às novas obrigações de validação e verificação dos dados de registo de domínios, à segurança da cadeia de abastecimento, e à avaliação da aplicabilidade da vastidão de requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança identificados também no Regulamento de Execução 2024/2690 da Comissão, de 17 de outubro de 2024. Contamos com uma lei forte e capaz de gerar mais confiança aos cidadãos e a todos os operadores a quem se vai aplicar diretamente. Mas contamos também com um enforcement eficaz.

No final das contas, o Princípio Goldilocks pode até merecer o nosso aplauso.

country's cyber resilience and promote a safer and more trustworthy digital environment for everyone, which is, it should be noted, part of .PT's mission. The journey is complex, but the benefits of effective implementation are undeniable.

For .PT, as an essential entity, manager of a Security Operations Centre (PTSOC) and responsible for the national database for the registration of .pt domain names, the implementation of the Legal Framework transposing the NIS2 Directive into national law is as relevant as it is challenging.

First and foremost, regarding the new obligations to validate and verify domain registration data, the security of the supply chain, and assessment of the applicability of the vast array of technical and methodological requirements for cybersecurity risk management measures also identified in the Commission's Implementing Regulation 2024/2690, of 17 October 2024. We are counting on a strong law capable of generating more confidence among citizens and all the operators to whom it will apply directly. But we are also counting on effective enforcement.

In the end, the Goldilocks Principle may even deserve our applause.

NIS2: a quem se aplica e o que se segue para as empresas abrangidas
NIS2: Whom does it applies to and what's next for the companies covered

João de Araújo Ferraz | Senior Associate, VdA

Face ao antigo regime (resultante da transposição da Diretiva NIS 1), o novo Regime Jurídico da Cibersegurança implicará alterações significativas (apesar de a versão final do diploma ainda não ser conhecida), destacando-se:

- Um âmbito de aplicação mais alargado (incluindo novos setores);
- Uma aplicação automática às entidades (que devem autoidentificar-se, ao invés de serem designadas, sem prejuízo de o CNCS elaborar listas de entidades essenciais, importantes e públicas relevantes);
- Um conjunto mais exigente de obrigações;
- Uma responsabilização direta dos órgãos de administração das entidades; e
- Um regime sancionatório consideravelmente mais pesado.

1. A quem se aplica?

À semelhança da Diretiva NIS 2, a proposta de Regime Jurídico da Cibersegurança aplica-se a entidades que sejam consideradas essenciais ou importantes, aplicando-se ainda a entidades públicas relevantes, distinguindo, o que constitui uma novidade, entidades públicas relevantes do Grupo A e entidades públicas relevantes do Grupo B.

Compared to the old framework (resulting from the transposition of the NIS 1 Directive), the new Cybersecurity Legal Framework will entail significant changes (although the final version of the law is not yet known), the following standing out:

- A wider scope of application (including new sectors);
- Automatic application to entities (which must self-identify rather than be designated, without prejudice to the CNCS drawing up lists of essential, important, and relevant public entities);
- A more demanding set of obligations;
- Direct accountability of the entities' management bodies; and
- A considerably heavier sanctioning regime.

1. Whom does it applies to?

Like the NIS 2 Directive, the proposed Cybersecurity Legal Framework applies to entities that are considered essential or important; it also applies to relevant public entities, distinguishing, which is a novelty, between relevant public entities in Group A, and relevant public entities in Group B.

ENTIDADES ESSENCIAIS

- Entidades de um dos tipos referidos no Anexo I da diretiva, que excedam os limiares previstos para as médias empresas [1].
- Prestadores de serviços de confiança qualificados e registo de nomes de domínio de topo e prestadores de serviços de sistemas de nomes de domínio independentemente da sua dimensão.
- Empresas que oferecem redes públicas de comunicações eletrónicas ou serviços de comunicações eletrónicas acessíveis ao público que sejam consideradas médias empresas.
- Entidades da Administração Pública que tenham como atribuições a prestação de serviços nas áreas do desenvolvimento, manutenção e gestão de infraestruturas de tecnologias de informação e comunicação ou aquelas que apresentem um grau particularmente elevado de integração digital na prestação dos seus serviços.
- Entidades identificadas como críticas [2].
- Qualquer outra entidade de um dos tipos constantes dos anexos I ou II, que seja qualificada como entidade essencial com base no respetivo grau de exposição da entidade aos riscos, na dimensão da entidade e na probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico.

ENTIDADES IMPORTANTES

- Entidades dos tipos referidos nos anexos I e II que não sejam consideradas entidades essenciais.
- Outras entidades de um dos tipos constantes nos anexos I ou II que sejam identificadas como entidades importantes.

[1] A categoria das micro, pequenas e médias empresas (PME) é constituída por empresas que empregam menos de 250 pessoas ou cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros.

[2] Nos termos da Diretiva (UE) 2022/2557 do Parlamento Europeu e o Conselho, de 14 de dezembro.

ESSENTIAL ENTITIES

- Entities of one of the types referred to in the directive's Annex I, which exceed the thresholds laid down for medium-sized enterprises[1].
- Qualified trust and top-level domain name registrars and domain name system service providers regardless of their size.
- Companies providing public electronic communications networks or publicly available electronic communications services that are considered medium-sized enterprises.
- Public Administration Entities who provide services in the areas of development, maintenance, and management of information and communication technology infrastructures, or those that have a particularly high degree of digital integration in the provision of their services.
- Entities identified as critical[2].
- Any other entity of one of the types listed in Annex I or II, qualified as an essential entity on the basis of the respective degree of exposure of the entity to risks, the size of the entity, and the likelihood of incidents occurring and their severity, including their social and economic impact.

IMPORTANT ENTITIES

- Entities of the types referred to in Annexes I and II not considered essential entities.
- Other entities of one of the types listed in Annexes I or II identified as important entities.

[1] The category of micro, small and medium-sized enterprises (SMEs) is made up of companies that employ fewer than 250 people, or whose annual turnover does not exceed 50 million euros, or whose annual balance sheet total does not exceed 43 million euros.

[2] In accordance with Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December.

A qualificação das entidades tem por base os setores identificados nos Anexos I e II da Proposta de Regime Jurídico da Cibersegurança, que são os seguintes:

ANEXO I – Setores de importância crítica

- Banca
- Saúde
- Energia
- Gestão de serviços TIC
- Infraestruturas Digitais
- Água Potável
- Águas Residuais
- Mercados Financeiros
- Transportes
- Espaço

ANEXO II – Outros setores críticos

- Produtos Químicos
- Bens Alimentares
- Serviços Postais
- Indústria Transformadora
- Investigação
- Serviços Digitais
- Gestão de Resíduos

2. Como devem as entidades proceder quando considerem estar abrangidas pela Proposta?

As entidades devem proceder à sua **auto-identificação** como entidade essencial, importante ou pública relevante, numa plataforma eletrónica disponibilizada pelo CNCS[3].

[3] Cujo funcionamento será definido através de Regulamento.

The classification of entities is based on the sectors identified in Annexes I and II of the Proposal for Cybersecurity Legal Framework, which are as follows:

ANNEX I - Sectors of critical importance

- Banking
- Health
- Energy
- ICT Service Management
- Digital Infrastructures
- Drinking Water
- Waste Water
- Financial Markets
- Transport
- Space

ANNEX II - Other critical sectors

- Chemical Products
- Foodstuffs
- Postal Services
- Manufacturing Industry
- Research
- Digital Services
- Waste Management

2. How should entities proceed when they consider to be covered by the Proposal?

Entities must **self-identify** on an electronic platform made available by the CNCS as either an essential, important, or relevant public entity[3].

[3] The functioning of which will be defined by Regulation.

Essa autoidentificação deve ocorrer no prazo de 1 mês após o início da atividade ou, quando já estejam a operar, no **prazo de 60 dias após a disponibilização da plataforma**[4]. A plataforma deverá também ser utilizada para o registo de informação de identificação das entidades. Sem prejuízo deste ponto, o CNCS irá propor, pelo menos de 2 em 2 anos, uma lista de entidades, dendo que a primeira lista deve, de acordo com a Proposta, entrar em vigor até ao dia 17 de março de 2025.

A Proposta define o prazo de 17 de fevereiro de 2025 para a realização da autoidentificação e do registo de informação, apesar de não ser claro se, nessa altura, estará já disponível a plataforma eletrónica destinada à sua realização.

3. Que obrigações / deveres se aplicam no âmbito da gestão da cibersegurança e da segurança da informação?

Obrigações dos órgãos de gestão, direção e administração

Estabelece-se a responsabilidade dos órgãos de gestão, direção e administração de entidades essenciais e importantes em aprovar as medidas de gestão de risco de cibersegurança, supervisionar a aplicação de medidas e assegurar a frequência anual em ações de formação em cibersegurança, podendo os seus titulares responder por ação ou omissão, com dolo ou culpa grave, pelas infrações previstas no regime.

[4] Os prestadores de serviços de registos de nomes de domínio devem identificar-se no prazo de um mês após o início da sua atividade.

This self-identification must take place within 1 month of the start of activity or, should they already be in operation, within 60 days of the platform becoming available [4]. The platform must also be used to register information identifying the entities. Without prejudice to this point, the CNCS will propose a list of entities at least every 2 years. The first list must, according to the Proposal, come into force by 17 March 2025.

The Proposal sets a deadline of 17 February 2025 for self-identification and registration of information, although it is not clear whether the electronic platform for this will be available by then.

3. What obligations / duties apply within the scope of cybersecurity and information security management?

Obligations of management, board of directors, and administrative bodies

Management, board of directors, and administration bodies of essential and important entities are responsible for approving cybersecurity risk management measures, supervising the implementation of measures and for ensuring annual attendance at cybersecurity training courses; their holders may be held liable for action or omission, with intent or serious fault, for offences provided for in the framework.

[4] Domain name registration service providers must identify themselves within one month of starting their activity.

Sistema de gestão de riscos de cibersegurança

As entidades essenciais e importantes devem adotar, seguindo uma abordagem sistémica, as medidas técnicas, operacionais e organizativas adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação, bem como para impedir ou minimizar o impacto de incidentes. As medidas devem ser adequadas ao risco em causa e proporcionais ao grau de exposição da entidade.

Medidas de cibersegurança*

As entidades essenciais e importantes, tendo em consideração a matriz de risco definida, devem adotar medidas que cubram um conjunto de áreas, tais como:

- tratamento de incidentes;
- continuidade de atividades;
- segurança da cadeia de abastecimento;
- segurança na aquisição, desenvolvimento e manutenção dos sistemas
- políticas e procedimentos para avaliar a eficácia das medidas de gestão de risco;
- práticas básicas de ciber-higiene e formação em cibersegurança;
- políticas e procedimentos relativos à utilização de criptografia e de cifragem;
- segurança dos recursos humanos; e
- utilização de autenticação multifator.

* As entidades públicas relevantes devem cumprir as medidas de cibersegurança que sejam aprovadas pelo CNCS através de regulamento.

Cybersecurity risk management system

Following a systemic approach, essential and important entities must adopt the appropriate technical, operational, and organisational measures to manage the risks posed to the security of networks and information systems, as well as to prevent or minimise the impact of incidents. The measures must be appropriate to the risk in question and proportionate to the entity's level of exposure.

Cybersecurity measures*

Taking into account the defined risk matrix, essential and important entities must adopt measures covering a range of areas, such as:

- incident handling;
- business continuity;
- supply chain security;
- security in the acquisition, development, and maintenance of systems;
- policies and procedures for evaluating the effectiveness of risk management measures;
- basic cyber-hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography and encryption;
- security of human resources; and
- use of multi-factor authentication.

* Relevant public entities must comply with the cybersecurity measures approved by the CNCS by means of a regulation.

Segurança da cadeia de abastecimento*

As medidas a adotar devem considerar as vulnerabilidades de cada fornecedor direto e de cada prestador de serviços, a qualidade global dos produtos na componente de cibersegurança, práticas de cibersegurança dos fornecedores e prestadores e as avaliações coordenadas de risco, bem como as decisões relativas a aplicações de restrições.

Gestão de risco residual*

As entidades essenciais e importantes devem realizar (e documentar) uma análise de gestão de riscos, por referência a cada ativo das redes e sistemas de informação que usam, em moldes a definir pelo CNCS. Com base em tal avaliação, devem ser adotadas medidas adequadas e proporcionais de forma a gerir os riscos, incluindo os riscos residuais.

Responsável de cibersegurança e ponto de contacto permanente

As entidades essenciais e importantes devem designar (e comunicar ao CNCS, no prazo de 20 dias úteis) um responsável de cibersegurança para a gestão da cibersegurança e da segurança da informação, que seja titular de órgão de gestão ou lhes responda organicamente e de forma direta, bem como a função de ponto de contacto permanente, com uma disponibilidade contínua de 24 horas por dia.

As obrigações assinaladas com * produzem efeitos 18 meses após a entrada em vigor do Regime Jurídico da Cibersegurança.

Supply chain security*

The measures to be adopted must take into account the vulnerabilities of each direct supplier and each service provider, the overall quality of the products in the cybersecurity component, the cybersecurity practices of the suppliers and providers, and the coordinated risk assessments, as well as the decisions regarding the application of restrictions.

Residual risk management*

Essential and important entities must carry out (and document) a risk management analysis, with reference to each asset of the networks and information systems they use, in a manner to be defined by the CNCS. On the basis of this assessment, appropriate and proportionate measures must be taken to manage risks, including residual risks.

Cybersecurity officer and permanent point of contact

Essential and important entities must appoint (and notify the CNCS within 20 business days) a cybersecurity officer to manage cybersecurity and information security, who is a management body or reports to them organically and directly, as well as the role of permanent point of contact, with continuous availability 24 hours a day.

Obligations marked with an * take effect 18 months after the Cybersecurity Legal Framework comes into force.

Certificação da cibersegurança

O CNCS pode exigir às entidades (i) a obtenção de certificação em cibersegurança e (ii) a utilização de produtos, serviços e processos, todos de TIC, desenvolvidos pela entidade ou fornecidos por terceiros, certificados no âmbito de sistemas nacionais e europeus de certificação da cibersegurança.

Há ainda vários aspetos que carecem de clarificação, e o CNCS irá aprovar, ao longo do tempo, um conjunto de documentos muito relevantes (desde logo o Quadro Nacional de Referência), que conterão um conjunto de medidas mais concretas que as entidades terão de implementar.

É, por isso, muito importante estar atento ao que vai sendo aprovado.

Cybersecurity certification

The CNCS may require entities (i) to obtain cybersecurity certification and (ii) to use products, services, and processes, all ICT, developed by the entity or third-party provided, certified under national and European cybersecurity certification systems.

There are still several issues that need clarification, and the CNCS will be approving a number of very important documents over time (starting with the National Reference Framework), which will contain a set of more concrete measures for entities to implement.

It is therefore very important to keep an eye on what is approved.

3

Gonçalo Silva

Head of Cyber Threat Intelligence, CERT.PT

1. O que é a Rede Nacional de CSIRTs?

A Rede Nacional de CSIRT (RNCSIRT) é um fórum técnico de partilha de informação de Incidentes de Segurança Informática cujo objetivo é criar laços de confiança entre os membros, criar um ambiente de assistência mútua no tratamento de incidentes, partilhar boas práticas de segurança e contribuir para a promoção de uma cultura de cibersegurança em Portugal. Neste momento, a RNCSIRT conta com 63 membros (39 de origem privada e 24 de origem pública).

A história da RNCSIRT começou em 2007, quando foi realizada a primeira reunião pelos membros fundadores, com o objetivo de começar a criar uma comunidade de Segurança Informática em Portugal. Ao longo destes 17 anos, a RNCSIRT tem crescido de uma forma sustentada com os mesmos princípios desde a sua origem, onde a partilha de informação assume o principal destaque.

A fácil adoção de uma Taxonomia Comum de Incidentes, permite que todas equipas de Resposta a Incidentes da RNCSIRT utilizem a mesma linguagem ao comunicarem entre si, fazendo com que o

1. What is the National Network of CSIRTs?

The National Network of CSIRTs (RNCSIRT) is a technical forum for sharing information on Computer Security Incidents. It aims to create bonds of trust between members, to create an environment of mutual assistance in dealing with incidents, to share good security practices, and to contribute to the promotion of a cybersecurity culture in Portugal. As of now, the RNCSIRT has 63 members (39 private and 24 public).

RNCSIRT's history begins in 2007, when the first meeting was held by the founding members, with the aim of starting to create an Computer Security community in Portugal. Over these 17 years, the RNCSIRT has grown in a sustained way with the same principles since its inception, with the sharing of information taking centre stage.

The easy adoption of a Common Incident Taxonomy allows all RNCSIRT Incident Response teams to use the same language when communicating with each other; this means that all incident types (e.g. Fraud - Phishing) are classified the same way. The Taxonomy adopted by the RNCSIRT is the same as that adopted by ENISA and the various teams.

2. How does one join the RNCSIRT?

In order to join the RNCSIRT, the applying entity must meet a number of requirements (for example, have a community of users defined, have an Incident Response Team, handle incidents pursuant to the RNCSIRT Taxonomy, etc.).

mesmo conceito de tipo de incidente (ex: Fraude – Phishing) seja igual. A Taxonomia adotada pela RNCSIRT é a mesma adotada pela ENISA e pelas diversas equipas.

2. Como aderir à RNCSIRT?

Para aderir à RNCSIRT, a entidade proponente terá de reunir um conjunto de requisitos (por exemplo, ter definido uma comunidade de utilizadores concerta, ter uma equipa de resposta a Incidentes, realizar tratamento de incidentes conforme os definidos na Taxonomia da RNCSIRT, etc.)

Importa também indicar, que após as entidades aderirem à RNCSIRT, existe um conjunto de obrigações (presença assídua nas reuniões, atualizações de contatos, atualização do RFC 2350, etc.), às quais os membros estão vinculados, permitindo que a RNCSIRT consiga manter uma interatividade, comunicação e cooperação entre equipas de resposta a Incidentes.

Por fim, não nos podemos esquecer, que nenhuma equipa de Resposta a Incidentes consegue resolver um Incidente sozinho – é através da conjunção das diversas partes interessadas que faz com o objetivo de mitigar ou recuperar de um Incidente seja efetuado de uma forma segura, rápida e eficaz, minimizando impactos e futuros incidentes.

3. Quais as vantagens/serviços da Rede Nacional de CSIRTs?

Os membros da RNCSIRT têm acesso a um conjunto de serviços que inclui uma Base de Dados

It is also important to point out that once entities have joined the RNCSIRT, there is a set of obligations (regularly attend meetings, update contacts, update the RFC 2350, etc.) to which members are bound, allowing the RNCSIRT to maintain interactivity, communication, and cooperation between Incident Response teams.

Finally, we must not forget that no Incident Response Team can resolve an Incident on its own - it is through the join work of the various stakeholders that the goal of mitigating or recovering from an Incident is achieved safely, quickly and effectively, minimising impacts and future incidents.

3. What are the advantages/services of the National Network of CSIRTs?

RNCSIRT members have access to a range of services including a Contact Database, Security Alerts, a Chat Service, a Platform for sharing Indicators of Compromise (MISP), a Document management platform, Workshops and the sharing of technical information, threat intelligence and specific cases of (national and international) incidents through quarterly meetings.

Members can use the services, for example, to share Indicators of Compromise (IoCs) of Phishing campaigns, Malicious Code, etc. between RNCSIRT teams and for them to be able to place these IoCs in perimeter systems, preventing Incidents or compromises.

de Contactos, Alertas de Segurança, um Serviço de Chat, uma Plataforma de partilha de Indicadores de Comprometimento (MISP), uma Plataforma de gestão documental, Workshops e a partilha de informação técnica, threat intel e casos concretos de incidentes (nacionais e internacionais) através das reuniões trimestrais.

A utilização dos serviços pelos membros permite, por exemplo, que a partilha de Indicadores de Comprometimento (IoCs) de campanhas de Phishing, Código Malicioso, etc. entre equipas da RNCSIRT e que estas consigam colocar estes IoCs nos sistemas de perímetro, prevenindo Incidentes ou comprometimentos.

No momento de transposição da NIS 2, as vantagens de pertencer à Rede Nacional de CSIRTs são ainda mais evidentes. Uma vez que a RNCSIRT promove a partilha de conhecimento e experiência entre os seus membros, tal permite que as entidades agora abrangidas pela NIS 2 possam retirar aprendizagens a partir da experiência de outros membros que já eram abrangidos pela NIS.

Adicionalmente, o esforço individual para cumprir com a NIS 2 será menor devido a este ambiente de partilha, permitindo focar nos temas essenciais e dar prioridade às iniciativas internas mais relevantes. A RNCSIRT promove frequentemente apresentações técnicas nas suas reuniões, ajudando a que todos os membros tenham acesso a perceções relevantes que os poderão auxiliar no cumprimento da NIS 2.

When it comes to transposing NIS 2, the advantages of belonging to the National Network of CSIRTs are even more notorious. Since the RNCSIRT promotes the sharing of knowledge and experience between its members, this allows the entities now covered by NIS 2 to learn from the experience of other members already covered by NIS.

In addition, the individual effort to comply with NIS 2 will be less due to this sharing environment, allowing the entities to focus on key issues and prioritise the most relevant internal initiatives. The RNCSIRT frequently promotes technical presentations at its meetings, helping all members to access relevant insights that can help them meet NIS 2.

Carlos Friaças

Head of RCTS CERT da FCCN

CSIRT in a Box: Capacitação Inicial de Equipas de Resposta a Incidentes

A cibersegurança está cada vez mais presente no dia-a-dia dos cidadãos. Contudo, os incidentes de segurança informática ocorrem diariamente, e cada vez com mais impacto nas nossas infraestruturas digitais. Consequentemente, e juntamente com a importância da digitalização na sociedade atual, surgiram as equipas de resposta a incidentes.

Em Portugal foi criada a Rede Nacional CSIRT em 2008, com as equipas existentes à data que não eram mais que os dedos de uma mão. Passados 16 anos, essa Rede conta com mais de 60 equipas, e digno de nota, com presença de diversos setores, como a energia, as telecomunicações, a banca, os seguros, a saúde e o ensino superior, entre outros.

Neste contexto de expansão, e apesar de existirem ofertas formativas na área da resposta a incidentes, identificámos que faltava um conteúdo em língua portuguesa. Assim, o RCTS CERT, a equipa que lidero na FCCN Serviços Digitais FCT decidiu criar um curso que tem como objetivo abordar o processo de criação das equipas de resposta a incidentes.

CSIRT in a Box: Initial Training for Incident Response Teams

Cybersecurity is increasingly present in people's daily lives. However, computer security incidents occur on a daily basis, increasingly impacting our digital infrastructures. Consequently, and together with the importance of digitalisation in today's society, incident response teams have been created.

In Portugal, the National CSIRT Network was created in 2008, with no more than a handful of teams. 16 years later, the Network has more than 60 teams. It is worth mentioning that they come from different sectors, such as energy, telecommunications, banking, insurance, health, and higher education, among others.

In this context of expansion, and despite the existence of training offers in the area of incident response, we identified there was a lack of content in Portuguese. So, the RCTS CERT, the team I lead at FCCN Digital Services FCT, decided to create a course that aims to address the process of setting up incident response teams.

Foto: Curso_CSIRT in a box

Pretende-se com este recurso, influenciar a criação de novas equipas CSIRT, especialmente em Portugal, e em países de língua oficial portuguesa, fornecendo uma visão geral dos conhecimentos básicos e essenciais ao exercício de futuros membros de uma equipa de resposta a incidentes.

A escolha do formato (MOOC – Massive Open Online Course) teve por pressuposto base alcançar o maior número possível de pessoas com potencial interesse nesta temática, e logicamente que a escolha da plataforma NAU (outro serviço da FCCN Serviços Digitais FCT) para albergar o curso foi também a opção óbvia, dada a facilidade e gratuitidade em termos de acesso.

The aim of this resource is to influence the creation of new CSIRT teams, especially in Portugal and in Portuguese-speaking countries, by providing an overview of the basic knowledge essential for future incident response team members.

The MOOC (Massive Open Online Course) format was chosen assuming it would reach as many people as possible with a potential interest in this subject; logically, the choice of the NAU platform (another FCCN Digital Services FCT service) to host the course was also obvious, given its free, easy access.

As for the course itself, its structure comprises six modules. The initial module

Sobre o curso propriamente dito, a sua estrutura compreende seis módulos. O módulo inicial centra-se no incentivo à criação de novas equipas de resposta a incidentes, o segundo é sobre o workflow padrão do processo de resposta a incidentes, e o terceiro versa sobre diversos aspetos de coordenação e colaboração que são necessários para que exista uma resposta efetiva.

A segunda metade deste curso inclui módulos sobre ferramentas geralmente usadas pelas equipas de resposta a incidentes, sobre treino, e por fim sobre auditoria e análise forense, sem, contudo, abordar estes temas em demasiada profundidade.

O resultado final do conteúdo construído envolverá uma interação com o mesmo de cerca de apenas duas horas, pelo que é importante deixar claro que o seu carácter é eminentemente introdutório.

À data desta edição, mais de 1400 pessoas realizaram a inscrição neste curso, sendo que mais de 300 já o concluíram e obtiveram o seu certificado.

Esperamos com este trabalho incentivar à criação de mais equipas de resposta a incidentes, capacitando cada vez mais organizações neste nicho da cibersegurança. Dentro desta linha, perspetivamos também a criação de um segundo curso, com conteúdos um pouco mais avançados e mais específicos em 2025.

focuses on encouraging the creation of new incident response teams, the second is about the standard workflow of the incident response process, and the third deals with various aspects of coordination and collaboration that are necessary for an effective response.

The second half of this course includes modules on the tools generally used by incident response teams, on training, and finally on auditing and forensic analysis, without, however, delving too deep into these topics.

The end result of the constructed content will involve an interaction with it of around two hours only, so it is important to make it clear that its character is eminently introductory.

At the time of writing, more than 1 500 people have registered for this course, and more than 300 have already completed it and obtained their certificate.

With this work, we hope to encourage the creation of more incident response teams, empowering more and more organisations in this cybersecurity niche. Along these lines, we also envisage the creation of a second course, with slightly more advanced and more specific content, for 2025.

2024 Report on the State of the Cybersecurity in the Union

Este relatório, publicado em dezembro, elenca seis recomendações a seguir pelos estados-membros da União Europeia, no contexto do quadro legislativo definido pela diretiva NIS 2, nomeadamente:

• Reforçar o apoio técnico e financeiro prestado às instituições, organismos e agências da UE e às autoridades nacionais competentes, bem como às entidades abrangidas pelo âmbito de aplicação da Diretiva NIS 2, a fim de garantir uma aplicação harmonizada, abrangente, atempada e coerente do quadro político evolutivo da UE em matéria de cibersegurança;

• Rever o plano de ação da UE para uma resposta coordenada a incidentes de cibersegurança em grande escala, tendo em conta os mais recentes desenvolvimentos da política de cibersegurança da UE;

• Reforçar os meios humanos da UE no domínio da cibersegurança, implementando a Academia de Competências em Cibersegurança ("Cybersecurity Skills Academy") e, em especial, estabelecendo uma abordagem comum da UE em matéria de formação em cibersegurança;

• Abordar a segurança da cadeia de abastecimento na UE, intensificando as avaliações de risco coordenadas e o desenvolvimento de um quadro político horizontal para

This report, published in December, lists six recommendations to be followed by the member states of the European Union, in the context of the legislative framework defined by the NIS 2 directive, namely to:

• Strengthening the technical and financial support given to EUIBAs and national competent authorities and to entities falling within the scope of the NIS2 Directive to ensure a harmonised, comprehensive, timely and coherent implementation of the evolving EU cybersecurity policy framework;

• Revising the EU blueprint for a coordinated response to large-scale cyber incidents, while taking into account all the latest EU cybersecurity policy developments;

• Strengthening the EU cyber workforce by implementing the Cybersecurity Skills Academy and in particular by establishing a common EU approach to cybersecurity training;

• Addressing supply chain security in the EU by stepping up coordinated risk assessments and the development of a horizontal policy framework for supply chain security aimed at addressing the cybersecurity challenges both by the public and the private sectors;

• Enhancing the understanding of sectorial specificities and needs, improving the level

a segurança da cadeia de abastecimento destinado a enfrentar os desafios de cibersegurança com que se deparam os setores público e privado;

• Reforçar a compreensão das especificidades e necessidades setoriais, melhorar o nível de maturidade da cibersegurança dos setores abrangidos pela Diretiva NIS 2 e utilizar o futuro Mecanismo de Emergência em matéria de Cibersegurança ("Cybersecurity Emergency Mechanism"), a criar no âmbito do CSoA, para a preparação e a resiliência setoriais;

• Promover uma abordagem unificada com base nas iniciativas políticas existentes e harmonizando os esforços nacionais para alcançar um nível elevado comum de sensibilização para a cibersegurança e a ciber-higiene entre os profissionais e os cidadãos, independentemente das caraterísticas demográficas.

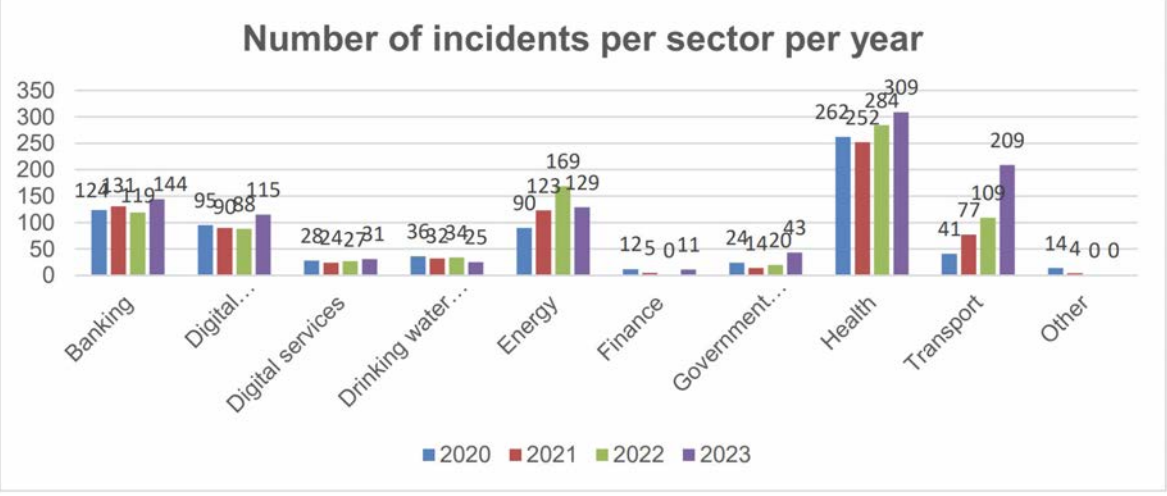
Uma versão condensada deste relatório pode ser obtida aqui

of cybersecurity maturity of sectors covered by the NIS 2 Directive and using the future Cybersecurity Emergency Mechanism to be established under the CSoA for sectorial preparedness and resilience;

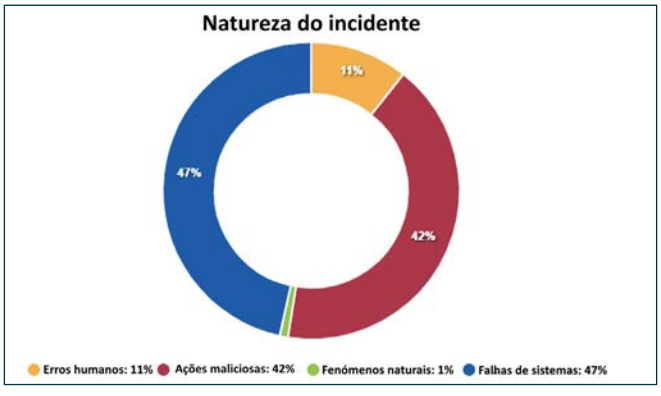
• Promote a unified approach by building on existing policy initiatives and harmonising national efforts to achieve a common high-level of cybersecurity awareness and cyber hygiene among professionals and citizens, irrespective of demographic characteristics.

A condensed version of this report can be found here

Annual report NIS Directive incidents



De acordo com o Annual report NIS Directive incidents 2023, publicado em outubro passado, o número de incidentes de cibersegurança reportados a nível europeu nos setores críticos (de acordo com a diretiva NIS ainda em vigor) aumentou e o setor da Saúde é o que regista um maior número de incidentes – algo que acontece de forma consistente desde 2020.



Em termos da natureza dos incidentes, o maior contributo é dado pelas falhas de sistemas, seguido por ações maliciosas, erros humanos e, de forma residual, fenómenos naturais.

According to the Annual Report NIS Directive Incidents 2023, published last October, the number of cybersecurity incidents reported at European level in critical sectors (according to the NIS directive still in force) has increased, the Health sector being the one with the highest number of incidents - something that has happened consistently since 2020.

In terms of the nature of incidents, the biggest contribution comes from systems failures, followed by malicious actions, human errors and, to a lesser extent, natural phenomena.

ENISA Threat Landscape 2024

De acordo com o último ENISA Threat Landscape, publicado em setembro passado, foram sete as principais ameaças às empresas e organizações identificadas em 2024: ransomware, malware, engenharia social, ameaças contra dados, ameaças contra disponibilidade (tipo DoS) e manipulação da informação.

According to the latest ENISA Threat Landscape, published last September, there were seven main threats to companies and organisations identified in 2024: ransomware, malware, social engineering, threats against data, threats against availability (DoS type), and information manipulation.

ENISA Threat Landscape 2024 - Prime threats

Diretora | Director
Inês Esteves

Editor | Editor
António Eduardo Marques

Design Gráfico | Graphic Design
Sara Dias
Maria Cristóvão

Tradução | Translation
Sara Pereira

Fotografia | Photography
Capa/Cover: : ImageKing, Adobe Stock
Índice/Table of contents: ImageKing, Adobe Stock

Publicação trimestral | Quarterly publication
Janeiro 2025 | January 2025