deti universidade de aveiro
departamento de eletrónica, telecomunicações e informática

Se você conhece o inimigo e a si mesmo, não precisa temer o resultado de cem batalhas

Neste trabalho pretende-se refletir sobre uma área na qual pretendo vir a especializar-me, o que é que fiz ou planeio fazer para alcançar esse *expertise* na matéria em questão, qual a metodologia que penso usar para lá chegar e provas/evidências que mostrem o progresso feito nesse tema.

A área em que me pretendo especializar é na Network and Information Security Directive 2 (NIS2), que surge como um dos pilares fundamentais da estratégia europeia de cibersegurança, impondo novos requisitos legais, técnicos e organizacionais às entidades públicas e privadas e que muito recentemente, no dia quatro de dezembro, foi transposta para a legislação nacional através do Decreto-Lei nº125/2025. Assim, através da especialização na NIS2, desenvolverei também muito conhecimento numa das grandes áreas de Ciberseguranças que é Governance, Risk and Compliance (GRC), ao combinar conhecimento técnico, enquadramento legal e responsabilidade organizacional.

A Diretiva NIS2: breve contextualização histórica e evolução

A Diretiva NIS2 resulta da revisão da primeira Diretiva NIS, adotada em 2016, que constituiu o primeiro esforço legislativo europeu para estabelecer um nível comum de segurança das redes e sistemas de informação. Contudo, a rápida evolução das ameaças, o aumento da digitalização e a experiência adquirida com incidentes de grande impacto demonstraram que o regime anterior era insuficiente, tanto em termos de âmbito como de exigência.

Como resposta, a União Europeia atualizou a Diretiva para NIS2, com o objetivo de reforçar a resiliência cibernética, harmonizar requisitos entre Estados-Membros e assegurar uma maior responsabilização das organizações e das suas estruturas de gestão.

O que é a NIS2 e o que exige

A NIS2 estabelece um quadro legal abrangente para a cibersegurança, com foco em três grandes pilares:

- **Gestão de Risco:** As entidades abrangidas devem adotar medidas técnicas e organizacionais adequadas e proporcionais aos riscos identificados, incluindo políticas de segurança, controlo de acessos, gestão de vulnerabilidades, continuidade de negócio, backups, encriptação e formação dos colaboradores. Estas entidades abrangidas incluem setores como energia, transportes, saúde, água, serviços digitais mas também administração pública e unidades de investigação, afetando assim a Universidade de Aveiro.
- **Notificação de Incidentes:** A diretiva impõe obrigações rigorosas de notificação de incidentes significativos, introduzindo um modelo faseado de reporte que inclui um aviso inicial até 24h após a deteção do incidente, uma notificação mais detalhada até um máximo de 72h e depois um relatório final onde consta uma análise de impacto e lições aprendidas.
- **Governação e Responsabilidade:** Um dos aspetos mais relevantes da NIS2 é a responsabilização da gestão de topo. A administração das organizações passa a ter um papel ativo na supervisão da cibersegurança, podendo ser responsabilizada pessoalmente em caso de incumprimento. Há também um agravar das coimas, em caso de incumprimento.

Desta forma, ao conhecer mais a fundo a NIS2 e o que é que ela pede, desenvolvo conhecimento da área de GRC que se vai manter mesmo depois do prazo de implementação para o disposto no Decreto-Lei ter terminado, que são 2 anos.

De seguida, enuncio alguns tópicos que eu tenho aprendido e outros que tenho de conhecer mais a fundo para alcançar este objetivo:

- Compliance com uma certificação, seja ela de âmbito mais nacional e direcionado para PMEs, como é o caso do Selo de Maturidade Digital e a certificação de serviços de cibersegurança lançado pelo CNCS [4] ou de âmbito internacional, como é o caso da ISO27001 para a segurança da informação, a ISO20000 relativa a boas práticas nos serviços TI ou a ISO9001 para a qualidade dos processos
- Aprender a interpretar e a tirar valor de *frameworks* na área de Gestão de Risco de cibersegurança, como é o caso do CSF2.0 [3], proposta pela NIST e que dá uma abordagem holística da aplicação da cibersegurança a toda a empresa
- Regulamento Geral de Proteção de Dados (RGPD), aprendido na Unidade Curricular de Direito e Organização da Segurança [5], que faz parte do plano curricular do Mestrado em Cibersegurança
- Cursos na NAU, como são os exemplos das figuras 2 e 4

Para além do acima mencionado, o conhecimento mais prático tem saído da aplicação na prática destes temas em conjunto com todo o tipo de entidades, sejam elas da administração pública, como escolas ou Câmaras Municipais ou PMEs dos vários setores de atividade, trabalho desenvolvido no Centro de Competências em Cibersegurança [6] (website na figura 3).

Evidências

Figura 1: Certificado de participação na formação sobre NIS2 realizada pela empresa *StrongStep*

Figura 2: Certificado de formação sobre funcionamento de um CSIRT

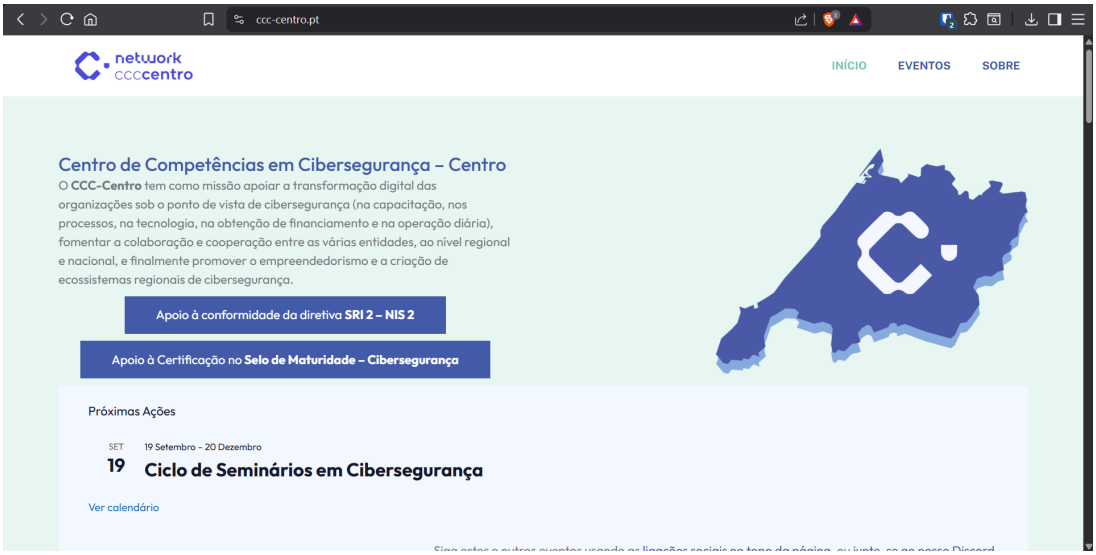

Figura 3: Website do Centro de Competências em Cibersegurança da Região Centro (CCC-Centro)

Figura 4: Certificado de formação sobre a Segurança da Informação Classificada

Referências

[1] União Europeia, *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 (NIS2)*, Jornal Oficial da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555

[2] Presidência do Conselho de Ministros, *Decreto-Lei n.º 125/2025, de 4 de dezembro — Regime Jurídico da Cibersegurança*, Diário da República, 1.ª série, n.º 234, 2025. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

[3] The NIST Cybersecurity Framework (CSF) 2.0. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[4] Certificação Serviços de Cibersegurança Disponível em: https://www.cncs.gov.pt/pt/certificacao-servicos-de-ciberseguranca/

[5] Direito e Organização da Segurança Disponível em: https://www.ua.pt/pt/uc/14826

[6] Centro de Competências em Cibersegurança Disponível em: https://www.ccc-centro.pt/