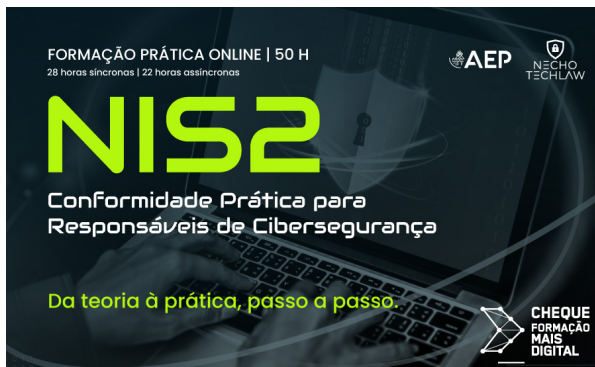


## ONLINE | NIS2 - Conformidade Prática para Responsáveis de Cibersegurança

**DATAS**

4, 8, 11, 15, 18, 22, 25 e 29 de maio de 2026

**HORÁRIO**

2ª feira e 6ª feira: 09:30 - 13:00

**PREÇO**

Associado AEP: **837€**

Outros: **930€**

**10% desconto grupo a partir de 3 inscrições**  
não acumula com outros descontos

Poderá ser reembolsado 750€ do valor pago,  
mediante a aprovação da sua candidatura em  
[lefp online - Cheque-Formação + Digital](#)

Para consultar a edição em **horário pós laboral**  
clique [aqui](#)

**LOCAL**

Online

**DURAÇÃO**

50 horas: <br /> 28h  
s&iacutecronas + 22h  
ass&iacutecron

### ENQUADRAMENTO

O Decreto-Lei n.º 125/2025 (4 de dezembro) estabelece um novo regime vinculativo de cibersegurança para entidades essenciais, importantes e públicas relevantes.

A NIS2 já não é apenas um requisito técnico.  
É uma responsabilidade direta dos órgãos de gestão.

**IMPACTO REAL PARA A ORGANIZAÇÃO:**

- Responsabilidade solidária da administração (Art. 25.º)
- Nomeação formal de Responsável de Cibersegurança (Art. 31.º) e do Ponto de Contacto Permanente (art. 32.º)
- Supervisão ativa pelo CNCS (auditorias e inspeções)
- Coimas até 10 milhões de euros ou 2% do volume de negócios
- Notificação obrigatória de incidentes em 24h–72h
- Obrigação de relatório anual e evidência documental permanente

**Este programa executivo transforma o enquadramento legal num plano concreto de ação.**

Ao longo de 8 módulos progressivos, irá desenvolver o seu:  
«**Dossier Técnico de Implementação NIS2 Completo (20–30 páginas)**»  
**Documento profissional pronto a apresentar ao órgão de gestão e a demonstrar perante o CNCS.**

O curso culmina com:

- Cyber Tabletop evolutivo com incidente realista
- Simulação Board + Incidente Crítico Integrado
- Defesa executiva do seu Plano

### MAIS VALIAS E FATORES DISTINTIVOS

**â€ Metodologia Executiva e Prática**

Não é um curso teórico.

É um programa hands-on baseado em projetos reais de conformidade NIS2 nos setores público, segurador e industrial.  
Trabalhará com cenários reais. Tomará decisões reais. Defenderá o seu plano.

**â€ Ferramentas Imediatamente Aplicáveis**

Receberá templates profissionais prontos a implementar:

- Metodologia e Matriz de gestão do risco ISO 27005
- Modelo de critério de aceitação de risco
- Framework documental NIS2
- Adendas às cláusulas contratuais para fornecedores
- Playbook de gestão e notificação de incidentes
- Dashboard executivo de maturidade

#### âœ Deliverable com valor Tangível

**Dossier Técnico de Implementação NIS2** completo (20–30 páginas).

Documento estruturado, profissional e imediatamente utilizável na tua organização.

Programa único em Portugal com este output estruturado.

#### âœ Formador com Experiência Executiva

Henrique Necho

CISO com 30 anos de experiência em redes, sistemas e cibersegurança.

Especialista no DL 125/2025 e em projetos ativos de conformidade NIS2.

Certificações internacionais:

CISM | CISA | ISO 27001 Lead Implementer | ISO 27005 Senior Risk Manager

#### âœ Apoio Financeiro IEFP

**O curso é elegível para o Cheque Formação + Digital**, permitindo um **apoio até 750€**- reduzindo o custo final de inscrição para apenas 180€.

#### Podem candidatar-se a esta medida:

- Trabalhadores por Conta de Outrem;
- Trabalhadores Independentes com rendimentos empresariais ou profissionais;
- Empresários em Nome Individual;
- Sócios de Sociedades Unipessoais por Quotas;
- Trabalhadores em Funções Públicas.

Consulte toda a informação sobre esta medida em [Iefponline - Cheque-Formação + Digital](#) e/ou contacte-nos:

Tlm: 963 607 902

Email: [formacao@aeportugal.pt](mailto:formacao@aeportugal.pt)

## OBJETIVOS

Este curso desenvolve competências executivas e operacionais que fazem a ponte entre:

“Saber o que a lei exige” e “liderar a conformidade na prática”.

No final da ação, os formandos deverão ser capazes de:

- Interpretar e aplicar o DL 125/2025 com foco na responsabilidade solidária da gestão, deveres de registo e supervisão ativa pelo CNCS
- Estruturar formalmente a governação da cibersegurança: Responsável de Cibersegurança, Ponto de Contacto Permanente, reporting ao órgão de Direção e modelo de accountability
- Implementar um Sistema de Gestão de Riscos de Cibersegurança (ISO 27005) alinhado com o QNRCS e com critérios formais de aceitação e gestão do risco residual
- Aplicar as 10 medidas mínimas obrigatórias (Art.º 27.º) com métricas de eficácia e evidência auditável
- Gerir risco da cadeia de abastecimento (Art.º 28.º) e integrar adendas com cláusulas contratuais NIS2
- Classificar incidentes segundo critérios legais e decidir sobre notificação obrigatória ao CNCS (24h–72h)
- Preparar evidência documental robusta para auditorias, inspeções e pedidos de esclarecimento regulatório
- **Elaborar e defender um Dossier Técnico de Implementação NIS2, com roadmap, cronograma, orçamento e narrativa executiva para o Board**

Conclui o curso com capacidade real de:

- Liderar a implementação NIS2 na sua organização
- Defender decisões técnicas perante a gestão de topo
- Responder com confiança a uma auditoria do CNCS
- Gerir um incidente crítico sob pressão

Não sai apenas com conhecimento. Sai com um plano pronto a executar.

## PROGRAMA

### MÓDULO 1 | ENQUADRAMENTO REGULATÓRIO E GOVERNANCE

ðŸ“ Sessão Síncrona: 3h30 | ðŸ“ Exercício Assíncrono: 2h30

Objeto, definições e âmbito (Arts. 1.º–10.º DL 125/2025)

- Entidades essenciais, importantes e públicas relevantes
- Centro Nacional de Cibersegurança e CERT.PT (Arts. 19.º–22.º)
- Instrumentos estruturantes da Segurança do Ciberespaço (Art. 11.º)
- Responsabilidade solidária dos órgãos de gestão (Art. 25.º)

- Regime de supervisão e sancionatório (Arts. 54.º–68.º e 79.º)
- Dever de registo (Art. 35.º)
- Produção de efeitos e entrada em vigor

ðŸ“‹ EXERCÍCIO PRÁTICO: “QUEM É ESSENCIAL?” – CLASSIFICAÇÃO E RESPONSABILIDADE DA GESTÃO

APRENDE A:

- Classificar juridicamente a tua entidade
- Identificar obrigações imediatas e prazos críticos
- Compreender o alcance da responsabilidade da gestão
- Estruturar o modelo de governance exigido pela NIS2

ðŸ“‹ EXERCÍCIO ASSÍNCRONO (2h30): ENQUADRAMENTO JURÍDICO DA ENTIDADE

Desenvolve a Secção 1 do Plano Executivo NIS2 (3–5 páginas): classificação legal, obrigações imediatas, prazos críticos e estrutura de governança aplicável à tua organização. Template fornecido.

## MÓDULO 2 | RESPONSÁVEL DE CIBERSEGURANÇA, PONTO DE CAONTATO PERMANENTE E POLÍTICAS DE SEGURANÇA

ðŸ“‹ Sessão Síncrona: 3h30 | ðŸ“‹ Exercício Assíncrono: 2h30

- Responsável de Cibersegurança (Art. 31.º)
- Ponto de Contacto Permanente (Art. 32.º)
- Relatório Anual (Art. 30.º)
- Estrutura documental (políticas, procedimentos, registos)
- Integração NIS2 + RGPD
- Evidence Repository e controlo documental

ðŸ“‹ EXERCÍCIO PRÁTICO: “GOVERNANÇA SOB ESCRUTÍNIO” – DESENHO DA ESTRUTURA FORMAL NIS2

APRENDE A:

- Definir formalmente o papel do CISO e do SPOC
- Estruturar um sistema documental alinhado com ISO 27001
- Implementar reporting regular à gestão de topo
- Integrar NIS2 com requisitos RGPD

ðŸ“‹ EXERCÍCIO ASSÍNCRONO (2h30): DESIGNAÇÃO FORMAL E FRAMEWORK DOCUMENTAL

Desenvolve a Secção 2 do Plano Executivo NIS2 (3–5 páginas): designação formal do CISO e SPOC, arquitetura documental e modelo de reporting à gestão. Template fornecido.

## MÓDULO 3 | GESTÃO DO RISCO DA CIBERSEGURANÇA

ðŸ“‹ Sessão Síncrona: 3h30 | ðŸ“‹ Exercício Assíncrono: 2h30

- Inventário e classificação de ativos (CIA+A)
- ISO 27005:2022
- Guia de Gestão do Risco CNCS – multi-critérios na significância do impacto
- Sistema de gestão de riscos (Art. 26.º)
- Gestão do risco residual (Art. 29.º)
- Matriz de risco e critério de aceitação
- QNRCS + NIST CSF 2.0 (Dimensão Identify)

ðŸ“‹ EXERCÍCIO PRÁTICO: “RISK LAB” – CONSTRUÇÃO DE CENÁRIOS E MATRIZ DE RISCO

APRENDE A:

- Construir cenários de risco baseados em ameaças credíveis e vulnerabilidades conhecidas
- Aplicar impacto multi-critério segundo o Guia CNCS
- Definir critério formal de aceitação de risco
- Traduzir risco técnico em linguagem executiva

ðŸ“‹ EXERCÍCIO ASSÍNCRONO (3h00): EXECUTIVE RISK ASSESSMENT

Desenvolve a Secção 3 do Plano Executivo NIS2 (3–5 páginas): heatmap de riscos, top 3 riscos críticos, KRIs e recomendações de investimento. Template fornecido.

## MÓDULO 4 | MEDIDAS DE GESTÃO DOS RISCOS

ðŸ“‹ Sessão Síncrona: 3h30 | ðŸ“‹ Exercício Assíncrono: 2h30

- As 10 medidas mínimas de cibersegurança (Art.º 27.º)
- Medidas para entidades públicas relevantes (Art. 33.º)
- Quadro Nacional de Referência da Cibersegurança - QNRCS (Art.º 14.º)
- Mapeamento ENISA NIS2 Technical Guidance e ISO 27002
- Plano de tratamento (mitigar, aceitar, transferir, eliminar)
- Avaliação da eficácia das medidas

ðŸ“‹ EXERCÍCIO PRÁTICO: “MEDIDAS EM AÇÃO” – MAPEAMENTO LEGAL-TÉCNICO

#### APRENDE A:

- Mapear requisitos legais para controlos técnicos
- Estruturar plano de tratamento com prioridades
- Definir roadmap faseado de implementação
- Avaliar a eficácia das medidas adotadas

ðŸ“ EXERCÍCIO ASSÍNCRONO (3h00): Desenvolve a Secção 4 do Plano Executivo NIS2 (3–5 páginas): plano de tratamento, roadmap faseado e indicadores de eficácia. Template fornecido.

### MÓDULO 5 | GESTÃO DO RISCO NA CADEIA ABASTECIMENTO E CONTRATOS DE SERVIÇO

ðŸ“ Sessão Síncrona: 3h30 | ðŸ“ Exercício Assíncrono: 2h30

- Art. 28.º – Gestão do risco na cadeia de abastecimento
- Due diligence de fornecedores TIC
- Classificação de funções TIC críticas/importantes
- Cláusulas contratuais NIS2
- Monitorização contínua e score de risco fornecedor

ðŸ“ EXERCÍCIO PRÁTICO: “GERIR OU ACEITAR O RISCO DO FORNECEDOR?”

#### APRENDE A:

- Identificar fornecedores críticos
- Avaliar maturidade de terceiros
- Integrar adendas com cláusulas contratuais NIS2
- Gerir risco da cadeia de abastecimento de forma estruturada

ðŸ“ EXERCÍCIO ASSÍNCRONO (2h30): FRAMEWORK SUPPLY CHAIN NIS2

Desenvolve a Secção 5 do Plano Executivo NIS2 (3–5 páginas): mapeamento de fornecedores críticos, critérios de avaliação e plano de monitorização. Template fornecido.

### MÓDULO 6 | GESTÃO DE INCIDENTES, NOTIFICAÇÃO CONTINUIDADE DE ATIVIDADES + CYBER TABLETOP EVOLUTIVO

ðŸ“ Sessão Síncrona: 3h30 | ðŸ“ Exercício Assíncrono: 2h30

- Conceito de incidente (CIA+A)
- ISO 27035 / NIST 800-61r3
- Notificação obrigatória (Arts. 40.º–45.º)
- Critérios de significância (DL 125/2025)
- BIA, BCP e DRP
- Comunicação de crise

ðŸ“ EXERCÍCIO PRÁTICO: CYBER TABLETOP EVOLUTIVO – INCIDENTE COM ESCALADA REGULATÓRIA E MEDIÁTICA

#### APRENDE A:

- Classificar incidentes segundo critérios legais
- Decidir sobre notificação obrigatória
- Integrar gestão de crise e continuidade
- Defender tecnicamente decisões sob pressão

ðŸ“ EXERCÍCIO ASSÍNCRONO (2h30): PROCEDIMENTO DE GESTÃO DE INCIDENTES

Desenvolve a Secção 6 do Plano Executivo NIS2 (3–5 páginas): ciclo de vida do incidente, critérios de significância, notificação e playbook de crise. Template fornecido.

### MÓDULO 7 | PESSOAS, CULTURA E TECNOLOGIAS DE SEGURANÇA

ðŸ“ Sessão Síncrona: 3h30 | ðŸ“ Exercício Assíncrono: 2h30

- Segurança de RH e funções críticas
- Formação e ciber-higiene (Arts. 25.º e 27.º)
- MFA e autenticação contínua
- Criptografia
- Gestão de vulnerabilidades
- Art. 8.º-A – atos não puníveis

ðŸ“ EXERCÍCIO PRÁTICO: “O ELO MAIS FRACO?” – PESSOAS VS TECNOLOGIA

#### APRENDE A:

- Estruturar segurança no ciclo de vida do colaborador
- Implementar programas de formação eficazes
- Definir políticas de MFA e criptografia
- Gerir vulnerabilidades de forma sistemática

ðŸ“ EXERCÍCIO ASSÍNCRONO: POLÍTICA DE SEGURANÇA DE RECURSOS HUMANOS

Desenvolve a Secção 7 do Plano Executivo NIS2 (3–5 páginas): ciclo de vida do colaborador, formação, controlo de acessos e roadmap de implementação. Template

fornecido.

## MÓDULO 8 | CONSOLIDAÇÃO FINAL - SIMULAÇÃO BOARD + INCIDENTE CRÍTICO INTEGRADO

“Sessão Síncrona: 3h30 | “Exercício Assíncrono: 2h30

- Consolidação do **Dossier Técnico de Implementação NIS2** (20–30 páginas)
- Apresentação executiva à gestão
- Defesa do critério de aceitação de risco
- Justificação de investimento
- Incidente crítico integrado
- Gap analysis final e roadmap 24 meses
- Encerramento: síntese, community of practice, webinars e office hours

“EXERCÍCIO PRÁTICO: “TEMOS UM PLANO ROBUSTO... MAS ESTAMOS PREPARADOS PARA DEFENDÊ-LO?”

APRENDE A:

- Defender tecnicamente o Dossier Técnico de Implementação NIS2 perante o Board
- Traduzir risco técnico em decisão estratégica
- Justificar orçamento e prioridades
- Avaliar maturidade organizacional sob pressão

**Resultado final: Entrega do DOSSIER TÉCNICO DE IMPLEMENTAÇÃO NIS2, pronto a apresentar ao órgão de gestão.**

## METODOLOGIA

Programa executivo estruturado com base em metodologias ativas e aprendizagem experiencial (“learning by doing”).

Cada módulo transforma requisitos legais do DL 125/2025 em decisões operacionais concretas, aplicadas ao contexto real da organização do formando.

**Ao longo do curso, irá construir progressivamente o seu Dossier Técnico de Implementação NIS2 - um documento estruturado, profissional e defensável perante o Órgão de Direção da sua Entidade e o CNCS.**

O CURSO COMBINA:

### SESSÕES SÍNCRONAS (ONLINE AO VIVO – 3h30 CADA)

- Exposição estruturada com enquadramento jurídico e técnico
- Exercícios práticos em grupo (trabalho colaborativo 3–4 participantes)
- Discussão em plenário e consolidação executiva
- Gamificação com quizzes interativos
- Cyber Tabletop evolutivo com escalada regulatória e mediática
- Simulação final “Board + Incidente Crítico Integrado”

### TRABALHOS ASSÍNCRONOS GUIADOS

- Desenvolvimento progressivo das 7 secções do Dossier Técnico de Implementação NIS2
- Templates exclusivos fornecidos pela NECHO TECHLAW
- Aplicação prática de ISO 27005, QNRCS e ENISA TIG
- Construção de evidência documental auditável

### FEEDBACK INDIVIDUALIZADO

- Revisão dos entregáveis intermédios
- Orientação técnica e executiva
- Ajuste do Plano ao contexto real da organização

### RESULTADO PEDAGÓGICO:

Não termina com conhecimento teórico.

Termina com capacidade comprovada de liderar a implementação NIS2.

? A diferença entre conhecer a lei e conseguir sustentá-la sob escrutínio executivo e regulatório.

### AVALIAÇÃO

Sem testes teóricos.

Sem perguntas de escolha múltipla.

#### 20% - ENVOLVIMENTO EXECUTIVO

Participação ativa nos debates, exercícios práticos e Cyber Tabletop.

Avalia-se pensamento crítico e tomada de decisão sob pressão.

#### 80% - CONSTRUÇÃO DO DOSSIER TÉCNICO DE IMPLEMENTAÇÃO NIS2

Desenvolvimento progressivo do seu Dossier Técnico de Implementação NIS2 com feedback direto do formador.

Coerência jurídica. Solidez técnica. Aplicabilidade real.

## FORMADORES

Henrique Necho (Engenheiro IT)

Perfil: CEO NECHO TECHLAW, 30 anos experiência cibersegurança  
Certificações: CISM, CISA, CIPP/E  
Qualificação: PhD Engineering and Public Policy  
Especialização: NIS 2, GDPR, AI Act, participante em comités europeus normalização  
Certificado de Competências Pedagógicas (CAP/CCP)

M<sup>a</sup> José Lima (Jurista)

Perfil: Jurista especializada em Direito Digital  
Especialização: Procedimentos contraordenacionais e regimes sancionatórios  
Certificado de Competências Pedagógicas (CAP/CCP)  
Formadora do Módulo: 1

## DESTINATÁRIOS

Programa executivo dirigido a profissionais que assumem – ou vão assumir – a liderança da conformidade NIS2 na sua organização.

Destina-se a quem tem responsabilidade direta na implementação, coordenação e evidência da conformidade com o DL 125/2025.

O curso prepara quem transforma obrigações legais em:

- Estrutura de governação formal
- Sistema de gestão de risco documentado
- Plano Executivo apresentável à gestão
- Evidência auditável perante o CNCS

### PERFIS RECOMENDADOS:

- Responsáveis de Cibersegurança (CISO) – nomeados ou a nomear (Art.º 31.º)
- Diretores de Tecnologia (CIO / CTO) – responsáveis pela implementação das medidas técnicas e organizativas
- Responsáveis de Risco, Compliance e Segurança da Informação – que asseguram a integração regulatória
- DPOs e profissionais de privacidade – que necessitam integrar RGPD e NIS2
- Consultores e Auditores de Cibersegurança – que apoiam entidades abrangidas pelo DL 125/2025

### PERFIL IDEAL DO FORMANDO:

- Experiência técnica prévia em IT ou cibersegurança
- Responsabilidade atual ou futura na coordenação da conformidade
- Necessidade de estruturar governance e reporting executivo

ãš ĩ• **NOTA IMPORTANTE:**

Este é um curso estratégico e executivo.

Está centrado na governação, gestão de risco, implementação estruturada e accountability regulatória.

Não é um curso de configuração técnica de firewalls, SIEM ou ferramentas de segurança.

## CONDIÇÕES DE PARTICIPAÇÃO

As **CONDIÇÕES GERAIS DE PARTICIPAÇÃO** são aplicáveis às modalidades de formação presencial e online. A inscrição pressupõe o conhecimento e aceitação das **Condições Gerais de Participação**, disponíveis em:

<https://aeportugal.pt/pt/condicoes-gerais-de-participacao>