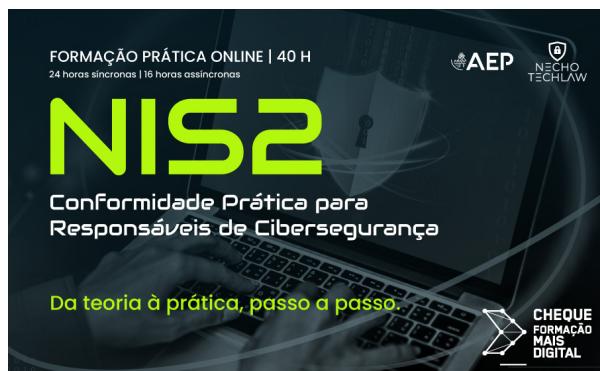


ONLINE | NIS2 - Conformidade Prática para Responsáveis de Cibersegurança



DATAS
2, 6, 9, 13, 16, 20, 23 e 27 de março de 2026

LOCAL
Online

HORÁRIO
2^a feira: 09:30 - 12:30
6^a feira: 14:30 - 17:30

DURAÇÃO
40 horas: 24h síncronas + 16h assíncronas

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:
[lefonline - Cheque-Formação + Digital](#)

ENQUADRAMENTO

A entrada em vigor do **Decreto-Lei n.º 125/2025** (transposição da **Diretiva NIS2**) representa um novo patamar de exigência para as organizações públicas e privadas em matéria de cibersegurança. Este novo enquadramento legal reforça significativamente as obrigações das entidades abrangidas e introduz, de forma clara, a responsabilização direta dos órgãos de direção, exigindo uma abordagem estruturada, contínua e documentada à gestão do risco de cibersegurança.

Num contexto de crescente exposição a ciberameaças, incidentes com impacto operacional e escrutínio regulatório reforçado, a conformidade com a NIS2 deixou de ser uma opção técnica para se tornar uma **prioridade estratégica e de governação**. O incumprimento pode traduzir-se em **coimas elevadas, medidas de supervisão e execução por parte das autoridades competentes**, bem como impactos reputacionais e operacionais relevantes.

O curso **"NIS2 – Conformidade Prática para Responsáveis de Cibersegurança"** foi desenvolvido para apoiar dirigentes, responsáveis de cibersegurança e profissionais de compliance na interpretação e aplicação prática dos novos requisitos legais, de forma clara, estruturada e orientada aos desafios reais das organizações.

Ao longo de 8 sessões, os participantes são conduzidos por um percurso formativo que transforma a legislação em **decisões concretas de governação**, abordando temas como a definição de responsabilidades, a gestão de riscos de cibersegurança, as medidas de cibersegurança, a gestão da cadeia de fornecimento, a segurança dos recursos humanos, a gestão de crises e a articulação com a gestão de topo, a notificação de incidentes, a supervisão e a integração com outros referenciais, como o RGPD e a ISO/IEC 27001.

O grande valor acrescentado desta formação reside na sua forte componente prática. **Cada participante desenvolve progressivamente um Plano Executivo NIS2, adaptado à sua própria organização**, que consolida o enquadramento regulatório, a estrutura de governação, as políticas e os mecanismos de controlo exigidos pela lei.

Com este curso formandos ficam capacitados para:

- âœ apoiar a gestão de topo na tomada de decisões informadas em matéria de cibersegurança,
- âœ responder com confiança a processos de supervisão e auditoria,
- âœ liderar a implementação efetiva da NIS2 nas suas organizações.

Uma formação orientada à ação:

- âœ Foco prático e aplicável à realidade das organizações
- âœ Enquadramento claro do DL 125/2025 e da Diretiva NIS2
- âœ Desenvolvimento de um Plano Executivo NIS2 pronto a utilizar
- âœ Alinhamento entre gestão, cibersegurança e conformidade
- âœ Formação ministrada por especialista com experiência prática

MAIS VALIAS E FATORES DISTINTIVOS

Esta formação distingue-se pela sua abordagem **prática, aplicada e orientada à realidade das organizações**, permitindo aos participantes transformar o enquadramento legal da NIS2 em decisões concretas de governação e ação.

âœ **Abordagem prática e orientada à implementação**

Ao contrário de formações meramente teóricas, este curso foca-se na aplicação efetiva do DL 125/2025 (NIS2), com exemplos reais, exercícios orientados e

desenvolvimento progressivo de um Plano Executivo NIS2, adaptado à organização de cada participante.

âœ Foco na gestão e na responsabilização executiva

A formação responde diretamente às novas exigências de responsabilização dos órgãos de gestão, apoiando a preparação de decisores para supervisionar, aprovar e acompanhar a gestão dos riscos de cibersegurança, conforme exigido pelo DL 125/2025 (NIS2).

âœ Alinhamento com boas práticas internacionais

Os conteúdos estão estruturados em coerência com referenciais amplamente reconhecidos, como a ISO/IEC 27001, assegurando uma abordagem integrada entre requisitos legais, governação, políticas de segurança e gestão do risco.

âœ Integração NIS2 – RGPD – Compliance Organizacional

O curso promove uma visão integrada da conformidade, ajudando os participantes a articular a NIS2 e o RGPD, evitando redundâncias e reforçando a eficácia dos modelos de compliance e de controlo interno.

âœ Desenvolvimento de um Plano Executivo NIS2

Ao longo da formação, cada participante constrói um Plano Executivo NIS2, que constitui um entregável prático e reutilizável, fundamental para auditorias, processos de supervisão e comunicação com a gestão de topo.

âœ Orientação para supervisão e auditoria

A formação prepara os participantes para responder com segurança a processos de supervisão, pedidos de informação e auditorias, incluindo organização de evidências, reporting e documentação exigida pelas autoridades competentes.

âœ Formação pensada para o contexto empresarial e institucional

Desenhada para entidades privadas e entidades públicas, esta ação formativa tem em conta diferentes realidades organizacionais, níveis de maturidade e setores de atividade, assegurando relevância prática para PME, grandes organizações e entidades públicas relevantes.

âœ Elegibilidade para 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 mais informação sobre esta medida em [lefonline - Cheque-Formação + Digital](#) e/ou contacte-nos:

Tlm: 963 607 902

Email: formacao@aeportugal.pt

OBJETIVOS

Este curso desenvolve competências operacionais que faltam entre "saber o que a lei exige" e "fazer acontecer a conformidade".

No final da formação, os participantes estarão aptos a:

âœ Interpretar e aplicar o DL 125/2025 com foco em responsabilidades executivas e obrigações de supervisão

âœ Implementar um Sistema de Gestão de Riscos de Cibersegurança (ISO 27005) alinhado com o QNRCs

âœ Estruturar a governação da cibersegurança: papéis, responsabilidades do órgão de gestão, reporting e accountability

âœ Aplicar as 10 medidas mínimas obrigatórias (Art.º 27.º) com critérios de eficácia

âœ Preparar evidências documentais para auditorias do CNCS e demonstrar conformidade contínua

âœ Elaborar o Plano Executivo NIS2 completo - roadmap, medidas, cronograma e orçamento

Conclui o curso com capacidade real de liderar a implementação NIS2 na sua organização.

PROGRAMA

Com uma duração total de **40 horas (24h síncronas + 16h assíncronas)**, o curso desenvolve-se em **8 módulos progressivos**, que combinam fundamentos legais, gestão de risco e aplicação prática de medidas de conformidade.

Cada sessão é estruturada para traduzir a Diretiva NIS2 em **processos, instrumentos e evidências aplicáveis**, conduzindo o participante da interpretação jurídica à execução operacional - passo a passo.

MÓDULO 1 | ENQUADRAMENTO REGULATÓRIO E GOVERNANCE

âœ Sessão Síncrona: 3h | âœ Exercício Assíncrono: 2h

- Diretiva NIS2 e DL 125/2025: contexto, objetivos, âmbito e complementaridade
- Quadro institucional: CNCS, CERT.PT, autoridades setoriais e supervisão
- Classificação de entidades e setores abrangidos (Anexos I e II)
- Obrigações dos órgãos de gestão: responsabilidade solidária (Art.º 25.º), CISO (Art.º 31.º), ponto de contacto (Art.º 32.º), autoidentificação (Art.º 8.º)
- Governança e accountability: relatório anual (Art.º 30.º), deveres de

- registo (Arts. 35.º-37.º), KPIs/KRIs, reporting à gestão
- Regime de supervisão (Arts. 54.º-57.º) e sancionatório (Arts. 61.º-68.º, 79.º)
- Evidence Repository: estrutura documental e controlo de acesso
- Prática: "Quem é Essencial?"

EXERCÍCIO ASSÍNCRONO: Enquadramento da Entidade (2h)

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

MÓDULO 2 | RESPONSÁVEL DE CIBERSEGURANÇA E POLÍTICAS

Sessão Síncrona: 3h | Exercício Assíncrono: 2h

- Papel e responsabilidades do CISO (Art.º 31.º): perfil, competências, funções executivas e reporte à gestão de topo
- Papel e responsabilidades do SPOC (Art.º 32.º): perfil, competências e interface com CNCS
- Relatório anual de cibersegurança (Art.º 30.º): estrutura, conteúdos obrigatórios e periodicidade
- Framework de políticas de segurança (ISO/IEC 27001): hierarquia documental, políticas vs procedimentos vs guias
- Interface GDPR-NIS2: compliance integrada e complementaridades
- Prática: "Governança da Cibersegurança e Políticas de Segurança"

EXERCÍCIO ASSÍNCRONO: Designação de Responsáveis e Framework de Governance (2h)

Desenvolve a Secção 2 do Plano Executivo NIS2 (3-5 páginas): designação formal do CISO e SPOC, perfis de responsabilidades, estrutura de governança e arquitetura de políticas. Template fornecido.

MÓDULO 3 | INVENTÁRIO DE ATIVOS E AVALIAÇÃO DOS RISCOS

Sessão Síncrona: 3h | Exercício Assíncrono: 2h

- Inventário de ativos críticos e diagramas de rede (observabilidade)
- Metodologias internacionais de gestão de risco: ISO/IEC 27005:2022
- Gestão do risco e do risco residual (Arts. 26.º e 29.º do DL 125/2025)
- QNRCs / NIST CSF 2.0 - Dimensão "Identificar": governança, vulnerabilidades, avaliação de riscos, gestão de riscos e logs
- Guia para Gestão dos Riscos do CNCS: tabelas de avaliação e critérios
- Prática: Hands-on de análise de riscos com ferramenta "Gestão dos Riscos de Cibersegurança" da NECHO TECHLAW®

EXERCÍCIO ASSÍNCRONO: Executive Risk Assessment (2h)

Desenvolve a Secção 3 do Plano Executivo NIS2 (3-5 páginas): executive summary, heat map de riscos, top 3 riscos críticos detalhados, dashboard de KRIs e recomendações de investimento, apresentável ao órgão de gestão. Template fornecido.

MÓDULO 4 | MEDIDAS DE GESTÃO DOS RISCOS

Sessão Síncrona: 3h | Exercício Assíncrono: 2h

- As 10 medidas mínimas de cibersegurança (Art.º 27.º)
- Quadro Nacional de Referência da Cibersegurança - QNRCs (Art.º 14.º)
- Mapeamento ENISA NIS2 Technical Guidance, ISO 27002:2022 e NIST CSF 2.0
- Medidas aplicáveis a entidades públicas relevantes (Art.º 33.º)
- Plano de tratamento dos riscos identificados no Módulo 3
- Roadmap de implementação faseado e avaliação da eficácia das medidas
- Prática: "Medidas em Ação"

EXERCÍCIO ASSÍNCRONO: Plano de Medidas e Tratamento de Riscos (2h)

Desenvolve a Secção 4 do Plano Executivo NIS2 (3-5 páginas): inventário das 10 medidas mínimas aplicáveis, plano de tratamento de riscos prioritários, roadmap faseado e mecanismos de avaliação de eficácia. Template fornecido.

MÓDULO 5 | GESTÃO RISCOS CADEIA ABASTECIMENTO

Sessão Síncrona: 3h | Exercício Assíncrono: 2h

- Medidas mínimas relacionadas com cadeia de abastecimento (Art.º 27.º, n.º 1, al. c) e Art.º 28.º)
- Responsabilidades do CISO e da gestão de topo no controlo de terceiros
- Due diligence e avaliação de risco de fornecedores TIC
- QNRCs Dimensão E: Gestão de Fornecedores e Parceiros
- NIST SP 1305: Cybersecurity Supply Chain Risk Management
- Avaliação de criticidade de funções e fornecedores TIC críticos
- Cláusulas contratuais de cibersegurança e plano de conformidade da cadeia
- Prática: "Gerir ou Aceitar o Risco da Cadeia de Abastecimento?"

EXERCÍCIO ASSÍNCRONO: Framework de Gestão da Cadeia de Abastecimento (2h)

Desenvolve a Secção 5 do Plano Executivo NIS2 (3-5 páginas): mapeamento de fornecedores críticos, framework de due diligence, cláusulas contratuais, matriz de decisão de risco (gerir/aceitar/transferir) e plano de conformidade. Template fornecido.

MÓDULO 6 | GESTÃO INCIDENTES, NOTIFICAÇÃO E CONTINUIDADE

Sessão Síncrona: 3h | Exercício Assíncrono: 2h

- O que é um incidente de cibersegurança? (Confidencialidade, Integridade, Disponibilidade e Autenticidade)
- ISO/IEC 27035: Information security incident management
- NIST SP 800-61r3: Incident Response and Cybersecurity Risk Management

- Ciclo de vida do incidente: detetar, avaliar, responder, recuperar e lições aprendidas. Taxonomia e tipologia de incidentes
- Classificação e obrigações de notificação ao CNCS (Arts. 24.º-27.º)
- Comunicação de crise: referencial CNCS e gestão reputacional
- Continuidade de atividades: Avaliação de impacto (BIA) e Planos de Continuidade (BCP)
- Prática: "Gestão de incidente: Notificar ou não notificar?"

EXERCÍCIO ASSÍNCRONO: Procedimento de Gestão de Ciberincidentes (2h)

Desenvolve a Secção 6 do Plano Executivo NIS2 (3-5 páginas): procedimento com ciclo de vida completo, matriz de classificação e critérios de notificação ao CNCS, e playbook de comunicação de crise. Template fornecido.

MÓDULO 7 | PESSOAS, CULTURA E TECNOLOGIAS SEGURANÇA

sessão Síncrona: 3h | exercício Assíncrono: 2h

- Segurança dos recursos humanos e cultura organizacional (Art.º 27.º, n.º 1, al. h): ciclo de vida do colaborador, funções críticas/sensíveis, segregação de funções, menor privilégio e conduta ética
- Formação e sensibilização em cibersegurança (Arts. 25.º e 27.º, n.º 1, al. f)
- Criptografia e autenticação multifator - MFA (Art.º 27.º, n.º 1, als. g) e i))
- Gestão de vulnerabilidades e patch management (Art.º 27.º, n.º 1, al. d)
- Coordinated disclosure e testes de segurança
- Prática: "O Elo Mais Fraco: Tecnologia ou Pessoas?"

EXERCÍCIO ASSÍNCRONO: Política de Segurança dos Recursos Humanos (2h)

Desenvolve a Secção 7 do Plano Executivo NIS2 (3-5 páginas): política de segurança RH com ciclo de vida do colaborador, programa de sensibilização e formação, matriz de medidas para funções importantes/críticas, código de conduta e roadmap de implementação. Template fornecido.

MÓDULO 8 | CONSOLIDAÇÃO FINAL E MELHORIA CONTÍNUA (CAPSTONE)

sessão Síncrona: 3h | exercício Assíncrono: 2h

- Monitorização e melhoria contínua: KPIs, métricas de cibersegurança e avaliação da eficácia das medidas
- Gestão de evidências: requisitos documentais, formato e ciclo de vida (políticas, registos, logs, atas)
- Auditoria e testes: vulnerability assessment, penetration testing, red team e cyber tabletop exercises
- Comunicação executiva à gestão de topo: narrativa de risco/impacto/investimento e dashboard de maturidade
- Gap analysis final face ao DL 125/2025 e roadmap de implementação (24 meses): fases, quick wins, prioridades e orçamentação
- Consolidação do Plano Executivo NIS2 completo (secções 1-7 + gap analysis + roadmap + orçamento)
- Prática: "NIS2 Quiz Battle" (60 min) - Quiz competitivo em equipa
- Encerramento: síntese, community of practice, webinars e office hours

EXERCÍCIO ASSÍNCRONO: Plano Executivo de Conformidade NIS2 Completo (2h)

Consolida o Plano Executivo NIS2 (20-30 páginas): integração das secções 1-7, gap analysis com avaliação de maturidade, roadmap de 24 meses com cronograma e prioridades, orçamento e business case, executive summary e anexos. Template fornecido.

METODOLOGIA

Formação executiva baseada em "learning by doing" - cada sessão transforma requisitos legais em decisões operacionais concretas.

Cada formando constrói progressivamente o seu Plano Executivo NIS2, aplicando ferramentas e metodologias reais ao contexto da tua organização.

O curso combina:

SESSÕES SÍNCRONAS (online ao vivo)

Debates, simulações e exercícios práticos com casos reais

TRABALHOS ASSÍNCRONOS GUIADOS

Templates, checklists e frameworks de implementação progressiva

FEEDBACK INDIVIDUALIZADO

Acompanhamento direto pelo formador em cada entregável

DELIVERABLE FINAL

Plano Executivo de Conformidade NIS2 completo, pronto a apresentar à gestão de topo e ao CNCS

Avaliação contínua e progressiva, centrada na construção do seu Plano Executivo NIS2.

1. PARTICIPAÇÃO ATIVA (20%)

Envolvimento em debates, simulações e exercícios práticos. Contributos em grupo e reflexão crítica. Assiduidade mínima: 80%.

2. DESENVOLVIMENTO PROGRESSIVO (40%)

Entrega de 8 secções do Plano ao longo do curso (trabalhos assíncronos).

Cada módulo desenvolve um componente: enquadramento, risco, medidas, incidentes, governação, etc. Feedback individualizado em cada entregável.

3. CONSOLIDAÇÃO FINAL (40%)

Integração das 8 secções num Plano Executivo NIS2 coerente e completo, com gap analysis, roadmap e orçamento. Avaliação: coerência, viabilidade e maturidade de

implementação.

? O formador acompanha a evolução do seu Plano desde a primeira sessão, assegurando aplicabilidade direta à sua organização.

FORMADORES

Henrique Necho

CISO | DPO | Consultor Séniior NIS2

Especialista em **cibersegurança, privacidade, inteligência artificial e conformidade regulatória**, com uma abordagem fortemente orientada à implementação prática e à tomada de decisão executiva.

Fundador e CEO da NECHO TECHLAW, consultora especializada em NIS2, RGPD e AI Act, atua como CISO de uma entidade pública de grande dimensão e participa ativamente em projetos reais de conformidade com o DL 125/2025, nos setores público, segurador e industrial.

Com **mais de 30 anos de experiência profissional**, combina uma visão estratégica de governação com conhecimento técnico profundo, apoiando organizações na tradução dos requisitos legais em modelos de decisão, políticas, processos e evidência de conformidade.

Certificações profissionais

CISM, CISA (ISACA) • ISO/IEC 27001 Lead Implementer • ISO/IEC 27005 Senior Risk Manager • CIPP/E, CIPM, CIPT (IAPP)

Formação académica

Licenciatura em Engenharia • MBA em Gestão de Empresas • Curso de Doutoramento em Engenharia de Políticas Públicas

Contributo institucional

Membro do Comité Técnico Português de Inteligência Artificial (IPQ CT223) • Project Editor do ISO/IEC 42001 – AIMS Handbook for SMEs

Experiência docente

Formador certificado DGERT/AEP, com mais de 500 horas de formação executiva nas áreas da cibersegurança, privacidade, governação digital e compliance regulatório.

Henrique Necho **ensina aquilo que implementa**: partilha experiência prática de projetos NIS2 reais, metodologias testadas no terreno e soluções aplicáveis ao contexto concreto de cada organização, preparando os participantes para responder com confiança a desafios de governação, supervisão e auditoria.

DESTINATÁRIOS

Esta formação é adequada a organizações públicas e privadas, incluindo PME, grandes empresas e entidades públicas relevantes, abrangidas ou potencialmente abrangidas pelo regime NIS2.

Destina-se a **profissionais e decisores com responsabilidades na governação da cibersegurança e na conformidade regulatória**, que necessitam de compreender e aplicar, de forma prática, os requisitos do Decreto-Lei n.º 125/2025 (NIS 2).

É especialmente indicada para:

- Administradores, gestores e membros de órgãos de direção, com responsabilidades na supervisão da cibersegurança e na tomada de decisão estratégica;
- Responsáveis de Cibersegurança (CISO), ou profissionais designados ou em vias de designação para esta função;
- Responsáveis de Compliance, Risco e Auditoria, envolvidos na implementação e monitorização de requisitos regulatórios;
- Encarregados de Proteção de Dados (DPO), no contexto da articulação entre NIS2 e RGPD;
- Diretores e responsáveis de Sistemas de Informação, Tecnologia e Segurança, com funções de coordenação ou supervisão;
- Consultores e profissionais sénior, que apoiam organizações públicas ou privadas em projetos de conformidade, governação e gestão do risco de cibersegurança.

Perfil dos participantes

- Funções de decisão, supervisão ou coordenação
- Envolvimento direto na conformidade NIS2
- Responsabilidade na definição de políticas, processos e evidência
- Interacção com autoridades, auditorias e gestão de topo

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://aeporugal.pt/pt/condicoes-gerais-de-participacao>