

ONLINE | NIS2 - Conformidade Prática para Responsáveis de Cibersegurança



DATAS

18, 20, 25, 27 de novembro, 2, 4, 9 e 11 de dezembro de 2025

HORÁRIO

19:00 - 22:00

PREÇO

Associado AEP: 837€ Outros: 930€

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

Poderá ser reembolsado do valor pago, mediante a aprovação da sua candidatura em: <u>lefponline -</u> Cheque-Formação + Digital

LOCAL

Online

DURAÇÃO

40 horas
br /> 24h síncronas

+ 16h assíncronas

ENQUADRAMENTO

A Diretiva (UE) 2022/2555 (NIS2) estabelece um novo quadro europeu para a governação dos riscos de cibersegurança, impondo obrigações reforçadas de gestão de risco, reporte, supervisão e responsabilidade executiva às entidades públicas e privadas que prestam serviços essenciais ou críticos.

Em Portugal, a Lei n.º 59/2025 autoriza o Governo a transpor a Diretiva NIS2, dando origem ao futuro **Regime Jurídico da Cibersegurança (RJC)** - um marco legislativo que colocará **centenas de organizações sob supervisão da autoridade nacional e das autoridades setoriais competentes.**

Este regime representa uma mudança estrutural: a conformidade deixará de ser um tema técnico ou documental para se tornar um imperativo estratégico e legal, com responsabilidade solidária dos órgãos de gestão, direção e administração e coimas até 10 milhões de euros ou 2% do volume de negócios global.

Mais do que cumprir requisitos, as organizações terão de demonstrar governação ativa, resiliência operacional e capacidade de resposta a incidentes, provando - com evidências - que a cibersegurança é parte integrante da sua estratégia e cultura organizacional.

As entidades abrangidas deverão, entre outros requisitos:

âce Implementar um sistema de gestão de riscos de cibersegurança (SGRC), alinhado com as orientações da autoridade de cibersegurança competente (Art.ºs 26.º–29.º);

✠Aplicar medidas técnicas e organizativas mínimas em nove domínios, incluindo gestão de incidentes, continuidade, cadeia de fornecimento e ciber-higiene (Art.º 27.º);

âce Designar formalmente um Responsável de Cibersegurança (CISO) e um Ponto de Contacto Permanente (SPOC), comunicando-os à autoridade competente (Art.ºs 31.º e 32.º);

âce Notificar incidentes significativos no prazo de 24h, 72h e 30 dias (Art.ºs 40.º-44.º);

âce Elaborar relatórios anuais de governação da cibersegurança e manter evidências de conformidade contínua (Art.º 30.º);

âce Capacitar os órgãos de gestão, que passam a ter responsabilidade pessoal e solidária pelo cumprimento das obrigações legais (Art.º 25.º).

Este curso prepara profissionais e gestores para implementar na prática as exigências da NIS2, compreender os impactos do novo regime e estruturar um plano executivo de conformidade aplicável à sua organização.

MAIS VALIAS E FATORES DISTINTIVOS

O curso "NIS2 – Conformidade Prática para Responsáveis de Cibersegurança" é uma formação pioneira em Portugal.

Este curso, distingue-se por transformar a complexidade regulatória da NIS2 em metodologias práticas e operacionais de implementação real, aplicáveis a qualquer setor.

Desenvolvido e lecionado por Henrique Necho, engenheiro com 30 anos de experiência nas áreas das TIC e cibersegurança, o curso baseia-se em lições aprendidas em projetos reais de conformidade NIS2 - conduzidos em entidades da administração pública, no setor segurador e na indústria transformadora.

Esta experiência de terreno traduz-se numa abordagem executiva, pragmática e orientada a resultados, desenhada para profissionais que precisam de fazer acontecer a conformidade dentro das suas organizações.

O que torna este curso único:

1. Abordagem "hands-on", aplicada à realidade organizacional

Não se limita à teoria ou à análise jurídica. Ensina a operacionalizar a NIS2 - da avaliação de riscos à documentação de evidências - com ferramentas e práticas testadas no terreno.

2. Integração de frameworks e normas internacionais

Estruturado em alinhamento com o Quadro Nacional de Referência para a Cibersegurança (QNRCS), o Quadro de Avaliação de Capacidades (QACC) e normas ISO/IEC 27001, 27005 e 27035, promovendo uma visão integrada de governação, risco e compliance.

3. Ferramentas e templates operacionais exclusivos

Os participantes têm acesso a modelos práticos e reutilizáveis - matrizes de risco, guias de auditoria, playbooks e dashboards - que facilitam a execução e a comunicação com a gestão de topo.

4. Deliverable final com valor real para a organização

Cada participante conclui o curso com um **Plano Executivo de Conformidade NIS2**, um documento aplicável que consolida diagnóstico, roadmap e plano de ação. É o único curso nacional que gera um resultado tangível e apresentável à administração da sua entidade profissional.

5. Formador com experiência executiva e certificação internacional

Henrique Necho alia experiência técnica e estratégica a uma base académica sólida - Licenciatura em Engenharia Eletrotécnica e de Computadores (1994), MBA em Gestão de Empresas (2001) e Curso Doutoral em Engenharia de Políticas Públicas (2014), complementados por certificações CISM, CISA, ISO 27001 LI e ISO 27005 SRM, entre outras.

6. 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 lefponline - Cheque-Formação + Digital e/ou contacte-nos:

Tlm: 963 607 902

Email: formacao@aeportugal.pt

OBJETIVOS

O curso "NIS2 – Conformidade Prática para Responsáveis de Cibersegurança" prepara profissionais e gestores para interpretar, operacionalizar e evidenciar a conformidade com a Diretiva NIS2 e o Regime Jurídico da Cibersegurança (RJC) no contexto da sua organização.

Mais do que compreender a lei, os participantes aprendem a **implementá-la na prática**, desenvolvendo competências para gerir riscos, estruturar modelos de governação e responder às novas exigências de supervisão e reporte.

No final da formação, os participantes estarão aptos a:

âce Interpretar e aplicar o enquadramento legal da NIS2, do Regulamento (UE) 2024/2690 e do RJC, com foco na responsabilidade executiva e na supervisão; âce Desenhar e implementar um Sistema de Gestão de Riscos de Cibersegurança (SGRC) alinhado com as orientações da autoridade nacional e as normas ISO 27001 e 27005:

âce Definir medidas de conformidade e controlo interno, integrando segurança, privacidade, risco e continuidade operacional;

âce Estruturar um modelo de governação da cibersegurança, com papéis claros, reporting executivo e accountability dos órgãos de gestão;

âce Preparar a organização para auditorias e inspeções da autoridade de cibersegurança competente, garantindo evidências de conformidade contínua;

âce Elaborar o Plano Executivo de Conformidade NIS2, consolidando as aprendizagens do curso num documento aplicável e comunicável à gestão de topo.

Em suma:

Os formandos sairão deste curso com um quadro completo de competências práticas, capazes de traduzir a legislação em ação, reduzir riscos de incumprimento e fortalecer a maturidade digital e reputacional das suas organizações.

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 Legal e Responsabilidades Executivas

- Enquadramento normativo europeu e nacional: Diretiva NIS2, Regulamento (UE) 2024/2690 e RJC.
- Categorias de entidades e critérios de essencialidade.
- Setores abrangidos: importância crítica e outros setores críticos.
- Estrutura institucional: CNCS, CERT.PT e autoridades setoriais.

AEP Formação

Tlm: +351 924 128 842 | inscricoes.formacao@aeportugal.pt

- Responsabilidade solidária da gestão de topo (Art.º 25.º) e implicações práticas.
- Regime sancionatório e prazos de conformidade.
- Linha temporal da transposição e entrada em vigor em Portugal (DAR 9/XVII e publicação em DR).
- Prática Exercício 1: "Quem é Essencial?"

Componente Assíncrona (2h):

- Caracterização da Sua Organização. Esta atividade produz a Secção 2 do seu Plano Executivo Conformidade NIS2 final. Ao completá-la, terá 15-20% do trabalho final pronto.
- Template_S1_Caracterizacao_Organizacional.docx

Módulo 2 - Quadro Institucional, Obrigações Imediatas e Certificação

- Arquitetura Institucional Nacional:
 - o Competências do CNCS (Artigos 19.º e 20.º) e do CERT.PT.
 - Papel das autoridades setoriais e da Comissão Nacional de Avaliação da Cibersegurança (Art. 18.º).
 - o Coordenação entre entidades essenciais, importantes e prestadores de serviços digitais.
- Obrigações dos Órgãos de Gestão, Direção e Administração:
 - Responsabilidade solidária da administração e gestão (Art. 25.º).
 - o Obrigações imediatas: Art. 31.º (designação do CISO), Art. 32.º (ponto de contacto único) e Art. 8.º (qualificação e autoidentificação das entidades).
 - o Preparação e apresentação de relatórios à gestão de topo.
- Instrumentos e Certificação:
 - o QNRCS (Quadro Nacional de Referência em Cibersegurança) e QACC (Quadro de Avaliação da Conformidade e Capacidade).
 - o Esquemas de certificação: DNP TS 4577-1, EC QNRCS e ISO/IEC 27001 vantagens, limitações e complementaridade.
 - o Critérios de decisão: custo, reconhecimento internacional, auditoria Autoridade de Supervisão e contexto organizacional.
 - o Recomendações conservadoras: "DNP TS 4577-1 opção válida para conformidade nacional; ISO 27001 referência global ('gold standard')
- Prática Exercício 2: Decisão Executiva de Certificação.

Componente Assíncrona (2h):

- Gap Analysis 10 Medidas Mínimas. Auto-avaliar conformidade atual organização vs. 10 medidas mínimas Reg. 2024/2690. Produz base Secção 3.1 Plano Final (30% trabalho).
- Template_S2_Gap_Analysis_10Medidas.xlsx

Módulo 3 - Gestão do Risco da Cibersegurança (ISO 27005 + MONARC Hands-on)

- Enquadramento normativo: Sistema de gestão de riscos de cibersegurança (Art.º 26.º da PL 7). Conceitos-chave: ameaça, vulnerabilidade, impacto, probabilidade e risco residual.
- Metodologias internacionais de gestão de risco: ISO/IEC 27005:2022.
- Dimensão D do QNRCS correspondência e indicadores de maturidade.
- Aplicação prática da metodologia MONARC (Model for the Analysis of Risks).
- Integração da gestão de risco com governação e reporting executivo.
- Prática Exercício 3: Workshop MONARC hands-on. Componente Assíncrona (2h):
 - Análise Risco MONARC. Matriz risco formal ISO 27005 aplicada à sua organização. Produz Secção 3.2 + Anexo A do Plano Final (25% trabalho total).
 - Template_S3_Matriz_Riscos.docx + MONARC

Módulo 4 - Medidas Mínimas I: Incidentes e Continuidade de Atividades

- Enquadramento normativo:
 - o Art.º 27.º da NIS2 Medidas de cibersegurança obrigatórias.
 - o Art.º 8.º e 9.º do Regulamento (UE) 2024/2690 Gestão de incidentes e continuidade de atividades.
- Medida 1 Gestão de Incidentes:
 - o NIST SP 800-61r3: fases da resposta (preparação, deteção, contenção, erradicação e lições aprendidas).
 - o Estrutura e operação de um SOC, ferramentas (SIEM, EDR, SOAR).
 - o Tipologia de incidentes e cadeia de reporte (interno e externo).
 - Desenvolvimento de playbooks e testes de resposta.
- Medida 2 Notificação e Comunicação:
 - Obrigações de notificação (Art. 40.º 45.º) e coordenação com CNCS e CSIRT.
 - o Processo end-to-end de notificação ao CNCS: deteção, avaliação, reporte inicial, atualização e relatório final.
 - o Exemplo prático: caso nacional de ataque ransomware e análise de resposta.
 - o Comunicação de crise: referenciais CNCS e boas práticas de gestão reputacional.
- Medida 3 Continuidade de Atividades:
 - o Art.º 9.º do Regulamento 2024/2690 requisitos mínimos.
 - o Avaliação de impacto (BIA) e definição de RTO/RPO.
 - o Estratégias de backup e recuperação: modelo 3-2-1-1-0.
 - Planos de continuidade (BCP) e gestão de crises organizacionais.
- Prática Exercício 3: Tabletop Exercise Ransomware.

Componente Assíncrona (2h):

- Plano Resposta Incidentes. Procedimento notificação CNCS + Playbook ransomware. Produz Secção 6.2 + Anexos C/D do Plano Final (15% trabalho).
- Template_S4_Resposta_Incidentes.docx

Módulo 5 - Medidas Mínimas II: Cadeia de Abastecimento e Segurança RH

- Enquadramento normativo:
 - Art.º 27.º da NIS2 e Art.º 10.º-11.º do Regulamento (UE) 2024/2690.

- Medidas mínimas relacionadas com cadeia de abastecimento e segurança dos recursos humanos.
- o Responsabilidades do CISO e da gestão de topo no controlo de terceiros.
- Medida 4 Cadeia de Abastecimento:
 - o Avaliação de riscos da cadeia de fornecimento (técnicos, contratuais e geopolíticos).
 - o Integração com o QNRCS Dimensão E: Gestão de Fornecedores e Parceiros.
 - o Abordagem à NIST SP 1305.
 - o Vendor Risk Management e Supply Chain Mapping Cláusulas contratuais de segurança e mecanismos de auditoria a fornecedores.
- Medida 5 Segurança dos Recursos Humanos:
 - o O Ciclo de Vida do Funcionário.
 - o Procedimentos de recrutamento seguro, onboarding e offboarding com verificação de devolução de ativos e perfis.
 - o Segregação de funções e controlo de acessos baseado no princípio do menor privilégio.
 - o Programas de sensibilização contínua e cultura de segurança (Art.º 27.º, n.º 2, al. g).
 - o Gestão de incidentes internos e conduta ética.
- · Prática:
 - o Exercício 5-A: Avaliação do Risco da Cadeia de Abastecimento
 - Exercício 5-B: Simulação de Cessação Segura de Funções de funcionário

Componente Assíncrona (2h):

- Gestão Cadeia de Abastecimento. Mapeamento fornecedores críticos + due diligence. Produz Secção 5.3 + Anexo E do Plano Final (10% trabalho).
- Template_S5_Supply_Chain.xlsx + Template_S5_Secao_5.3.docx

Módulo 6 - Medidas Mínimas III e Governação

- Enquadramento normativo e medidas associadas:
 - o Medida 5 Eficácia das Medidas:
 - Monitorização contínua, auditorias internas, métricas de controlo técnico e dashboards executivos.
 - Ciclo PDCA aplicado à cibersegurança: planeamento, execução, verificação e melhoria.
 - o Medida 6 Segurança TIC e Autenticação Multifator (MFA):
 - Conceitos e métodos (TOTP, Push, FIDO2, biometria).
 - Estratégias de implementação: roadmap 3 meses, políticas de MFA adaptativas e gestão de exceções.
 - o Medida 7 Entidades Públicas Relevantes:
 - Cooperação interinstitucional e reporte centralizado ao CNCS.
 - Integração com plataformas nacionais de gestão de incidentes e partilha de informação.
- · Governança e Accountability:
 - o Art.º 30.º Relatório anual de governação da cibersegurança.
 - o Art.º 35.º-37.º Deveres de registo, gestão de nomes de domínio e acesso controlado.
 - o Responsabilidade solidária da gestão de topo (órgãos de gestão, direção e administração da Entidade).
 - o Modelos de reporte à da gestão de topo (formato e frequência).
 - o KPIs/KRIs de maturidade: tempo de resposta, percentagem de sistemas com MFA, eficácia de controlos, taxa de sensibilização.
 - o Cultura de segurança e gestão da mudança organizacional.
- Integração com o QNRCS:
 - o Correspondência entre as Dimensões G (Governança) e H (Avaliação e Melhoria).
 - o Utilização dos indicadores CNCS para avaliação contínua.
- Prática:
 - o Exercício 6-A: Elaboração de Dashboard de Maturidade NIS
 - o Exercício 6-B: Apresentação de Dashboard ao Board

Componente Assíncrona (2h):

- Governança e KPIs. Estrutura governação cibersegurança + dashboard KPIs. Produz Secção 4.3 do Plano Final (10% trabalho).
- Template_S6_Governance_Dashboard.xlsx + Template_S6_Secao_4.3.docx

Sessão 7 - Supervisão, Sanções e Mock Audit de Supervisor

- Enquadramento normativo e institucional:
 - o Art.º 30.º Relatório anual e dever de reporting ao CNCS.
 - ∘ Art.º 54.º a 57.º Medidas de supervisão, execução e bloqueio
 - Art.º 61.º a 68.º Regime sancionatório (contraordenações leves, graves e muito graves).
 - Art.º 66.º Critérios de determinação da medida da coima.
 - o Art.º 79.º Violação de dados pessoais e responsabilidade cumulativa (RGPD).
 - Estrutura e poder de supervisão do CNCS e das autoridades competentes.
- Processo de Supervisão e Auditoria da Autoridade de Supervisão:
 - Tipologia de auditorias: iniciais, de manutenção e de follow-up.
 - o Anatomia de uma auditoria típica da Autoridade de Supervisão:
 - Fases: planeamento, execução, entrevistas, recolha e validação de evidências, relatório final.
 - Requisitos documentais e formato de evidências (políticas, registos, logs, atas).
 - Gestão do ciclo de evidência: criação, controlo de versões, acesso e confidencialidade.
 - o Evidence Repository Blueprint: estrutura recomendada de pastas (estilo ISO 27001), naming conventions, controlo de acesso e versionamento.
- Gestão Pós-Certificação e Melhoria Contínua:
 - Manutenção de conformidade e auditorias internas.
 - Elaboração e execução de planos de ação corretiva.
 Costão do receptificação (opuel ou bianal) e de comunicación.
 - $\circ\,$ Gestão da recertificação (anual ou bienal) e da comunicação contínua com o CNCS.
 - o Integração com o QNRCS Dimensão H (Avaliação e Melhoria Contínua).
- Prática:
 - o Exercício 7-A: Mock Audit de autoridade de supervisão simulado (Role-Play)
 - o Exercício 7-B: Hot Wash Debrief em Plenário

Componente Assíncrona (2h):

- Gap Analysis Atualizada + Checklist Evidências. Refinar gap analysis com aprendizagens mock audit + preparar checklist evidências auditoria real. Atualiza Secção 3.1 do Plano Final (5% trabalho) + cria ferramenta gestão ongoing (Checklist).
- Template_S7_Gap_Analysis_Revista.docx + Template_S7_Checklist_Evidencias.xlsx.

Sessão 8 - Roadmap, Casos Setoriais e Encerramento

- Planeamento e Execução da Conformidade:
 - o Estruturação do Roadmap NIS2 a 24 meses fases 0 ? 4 (diagnóstico, planeamento, implementação, monitorização e melhoria).
 - o Definição de prioridades e quick wins (curto, médio e longo prazo).
 - Orçamentação realista: faixa de referência 25.000 40.000 € no 1.º ano (entidades médias), com variação conforme maturidade e contexto.
 - Gestão de dependências, recursos e monitorização.
- Comunicação Executiva:
 - o Estrutura de apresentação à gestão e topo: narrativa de risco, impacto e investimento.
 - o Construção de Executive Deck de 20 slides com mensagem orientada a decisão.
- Casos Práticos Setoriais:
 - o Trabalho em grupos temáticos:
 - Saúde, Financeiro, Telecomunicações, Indústria/Logística, Administração Pública e Energia/Utilities (focus OT/SCADA).
 - o Aplicação prática dos requisitos NIS2 e Regulamento 2024/2690 a cada setor.
 - o Análise comparativa de riscos, dependências e medidas prioritárias.
- Encerramento e Próximos Passos:
 - o Síntese das aprendizagens-chave e reforço do plano individual de conformidade.
 - o Continuidade de desenvolvimento: community of practice, webinars e office hours.
 - Avaliação final e orientações finais
- Prática:
 - o Exercício 8-A: Roadmap & Orçamentação
 - o Exercício 8-B: Consolidação do Plano Executivo Final

Componente Assíncrona (2h):

- CONSOLIDAÇÃO PLANO EXECUTIVO FINAL. Integrar todos os deliverables S1-S7 num documento profissional coeso de 20-30 páginas.
- Template S8 Plano Executivo COMPLETO.docx.
- · Feedback individualizado do plano.

METODOLOGIA

Formação executiva, aplicada e orientada a resultados reais.

O curso "NIS2 - Conformidade Prática para Responsáveis de Cibersegurança" foi concebido segundo um modelo pedagógico "learning by doing", que combina rigor normativo com aplicação prática e contextualizada à realidade das organizações.

Cada sessão transforma as exigências legais em decisões operacionais concretas, com ferramentas, exercícios e exemplos reais de implementação.

Mais do que assistir a aulas, os participantes constroem progressivamente o seu próprio plano de conformidade, aplicando os conceitos ao contexto da sua organização.

O modelo pedagógico combina:

- Sessões síncronas (online ao vivo) debates, simulações, estudos de caso e exercícios práticos orientados à realidade profissional.
- Atividades assíncronas guiadas exercícios aplicados com templates, checklists e guiões de execução progressiva.
- Feedback individualizado acompanhamento contínuo pelo formador, assegurando ligação direta entre teoria e prática.
- Deliverable final elaboração de um Plano Executivo de Conformidade NIS2, consolidado ao longo do curso, pronto a ser apresentado à gestão de topo ou à autoridade de supervisão.

Em síntese:

Uma metodologia imersiva, centrada na execução e no valor real, que transforma a aprendizagem em competência aplicável e comprovável - a diferença entre saber a lei e saber cumpri-la.

São considerados três momentos de avaliação principais:

- 1. Participação e envolvimento nas sessões síncronas (20%)
 - Participação ativa nos debates e simulações (tabletop, role-play);
 - Contributos em grupo e capacidade de reflexão crítica;
 - Assiduidade mínima de 80% obrigatória para certificação.

2. Realização de exercícios e atividades práticas (40%)

- Entrega de exercícios assíncronos (ex.: matriz de risco MONARC, checklist de auditoria de Autoridade de Supervisão, relatório de incidente);
- Cumprimento de prazos no Moodle e qualidade das evidências apresentadas.

3. Trabalho Final Individual (40%)

- Elaboração de Plano Executivo de Conformidade NIS2 (10-15 páginas) ou Relatório Técnico Setorial (caso prático OT/SCADA);
- Avaliação segundo grelha de critérios: coerência, aplicabilidade e relevância.
- Entrega até 5 dias após a última sessão, com feedback individual.

O feedback é assegurado ao longo do curso através de:

- Interação em tempo real durante as sessões síncronas;
- · Revisão e debriefing após cada módulo principal.

FORMADOR

Henrique Necho

Responsável de Cibersegurança (CISO) e Encarregado de Proteção de Dados (DPO) certificado. CISM, CISA (ISACA) | ISO 27001 Lead Implementer | ISO 27005 Senior Risk Manager | CIPP/E, CIPM, CIPT (IAPP)

Engenheiro com 30 anos de experiência profissional nas áreas das Tecnologias de Informação, Cibersegurança e Governação Digital, Henrique Necho é fundador e CEO da NECHO TECHLAW, empresa especializada em conformidade tecnológica, risco e segurança da informação.

Atualmente exerce funções como **Responsável de Cibersegurança (CISO)** de uma entidade pública de grande dimensão e atua como **consultor sénior** em projetos nacionais de conformidade NIS2 nos setores público, segurador e industrial.

Com uma sólida formação académica - Licenciatura em Engenharia, MBA em Gestão de Empresas e Curso de Doutoramento em Engenharia de Políticas Públicas - alia visão técnica e estratégica à capacidade de transformar legislação complexa em planos operacionais de execução.

É também membro do Comité Técnico Português de Inteligência Artificial (IPQ CT223) e convenor do ISO/IEC 42001 AIMS Handbook for PMEs, contribuindo ativamente para a normalização e regulação internacional da cibersegurança e da inteligência artificial.

Leciona formação executiva certificada (DGERT/AEP) desde 2020, com mais de 500 horas de ensino profissional e académico em cibersegurança, privacidade e governação tecnológica.

Henrique Necho traz para as sessões de formação a experiência real de quem implementa a NIS2 no terreno - traduzindo teoria em prática e partilhando lessons learned diretamente aplicáveis ao contexto de cada participante.

DESTINATÁRIOS

O curso "NIS2 – Conformidade Prática para Responsáveis de Cibersegurança" destina-se a profissionais com responsabilidades de decisão, coordenação ou supervisão da conformidade NIS2 - em organizações públicas ou privadas abrangidas pelo futuro Regime Jurídico da Cibersegurança (RJC).

Mais do que conhecer a lei, estes profissionais precisam de **transformar obrigações legais em ações concretas**, garantindo resiliência, segurança e responsabilidade organizacional.

Público-alvo principal

- Responsáveis de Cibersegurança (CISO) nomeados ou a nomear ao abrigo do Art.º 31.º do RJC, com funções de liderança técnica e estratégica.
- Diretores de Tecnologia e Sistemas de Informação (CIOs, CTOs) responsáveis pela execução das medidas técnicas e organizativas previstas na NIS2.
- Compliance Officers, DPOs e Gestores de Risco profissionais que asseguram conformidade regulatória, auditoria e governação de risco digital.
- Administradores, Diretores e Gestores Executivos titulares de responsabilidade solidária pelos deveres de governação e supervisão da cibersegurança (Art.º 25.º).
- Consultores e Auditores de Cibersegurança Regulatória prestadores de serviços que apoiam entidades abrangidas pelo RJC em processos de conformidade, auditoria e certificação.

Perfil ideal

Profissionais com experiência prévia em gestão, governação tecnológica ou compliance, capazes de integrar perspetivas técnicas, organizacionais e legais.

O curso **não é técnico-operacional** (não aborda configuração de sistemas ou ferramentas de segurança), mas sim **estratégico e executivo - centrado na implementação e governação da conformidade NIS2.**

Em suma:

Este curso é para quem precisa de **liderar a conformidade**, não apenas de a executar.

Para quem quer passar da leitura da diretiva à prática da conformidade - com segurança, evidência e credibilidade.

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