ONLINE | NIS2 DECIDE - Responsabilidade, Risco e Decisão para Órgãos de Gestão, Direção e Administração

DATAS
9, 16, 23 e 30* de outubro de 2026 (6ª feira)

HORÁRIO
14:30 - 17:30
*16:00 - 19:00

PREÇO
Associado AEP: **1.125€**
Outros: **1.250€**

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

Consulte todos os cursos NIS2 **aqui**
Quer inscrever-se em mais do que um curso NIS2? Ou inscrever diferentes trabalhadores nos diferentes cursos NIS2?
Diga **aqui** o que pretende, saiba como beneficiar até 20% desconto.

LOCAL
Online

DURAÇÃO
12h30:
 12h síncronas + 30min. mentoria por entidade inscrita

ENQUADRAMENTO

NIS2 DECIDE - Responsabilidade, Risco e Decisão para Órgãos de Gestão, Direção e Administração
Compreender o impacto. Decidir. Supervisionar. Exigir evidência.

O Decreto-Lei n.º 125/2025, de 4 de dezembro, aprovou o Regime Jurídico da Cibersegurança e transpôs a Diretiva (UE) 2022/2555.

O Regulamento n.º 756/2026, em vigor desde 23 de junho de 2026, concretizou matérias essenciais da execução do regime, incluindo a plataforma MyCiber, a qualificação das entidades, o QNRCS 2.0, a Matriz de Risco, os níveis de conformidade, as medidas mínimas, o risco residual, o relatório anual, as comunicações e as notificações.

Para os órgãos de gestão, direção e administração, a cibersegurança não é apenas uma matéria técnica. A abrangência pelo Regime Jurídico da Cibersegurança tem impacto na governação, nos recursos, na supervisão, na continuidade, na cadeia de abastecimento, na resposta a incidentes e na capacidade de demonstrar decisões e acompanhamento.

O NIS2 DECIDE foi concebido para responder às perguntas que mais preocupam os decisores:
- Qual é o impacto de a nossa entidade estar abrangida?
- Que decisões pertencem ao órgão de gestão?
- Que informação e evidência devemos exigir?
- De que fornecedores e serviços críticos dependemos?
- Quem pode aceitar o risco residual?
- Conseguimos demonstrar o que decidimos, exigimos e acompanhámos?

Toolkit Executivo NIS2
A formação privilegia a decisão executiva. Em vez de exigir trabalhos assíncronos extensos, disponibiliza um Toolkit Executivo NIS2 com **fichas orientadoras parcialmente preenchidas, prontas a distribuir** a**o CISO, IT, jurídico, compras, continuidade, auditoria interna e responsáveis de negócio.**

Tabletop Executivo
O programa termina com um tabletop executivo que **combina um incidente num fornecedor crítico, impacto operacional e uma simulação pedagógica de pedido de informação da autoridade competente.**

Mentoria - 30 minutos por entidade
O programa inclui 30 minutos de mentoria por entidade inscrita, a agendar, a realizar após a última sessão. A mentoria tem natureza pedagógica e prática e não constitui parecer jurídico, auditoria, certificação ou validação formal de conformidade. Agenda recomendada:
1. Impacto provável ou confirmado da abrangência.
2. Principal lacuna de governação.
3. Dependência ou fornecedor crítico mais sensível.
4. Risco residual ou evidência mais frágil.
5. Três prioridades para os 30 dias seguintes.

Este não é um curso técnico para implementação de controlos, é um programa executivo para compreender impacto, tomar decisões, atribuir

responsabilidades, disponibilizar recursos, exigir evidência e supervisionar a execução.

Consulte todos os cursos do percurso NIS2 aqui

OBJETIVOS

A formação permite aos participantes:

- compreender o impacto organizacional, executivo e operacional de a entidade estar abrangida pelo RJC;
- distinguir autoidentificação, qualificação, nível de conformidade comunicado pelo CNCS no processo de validação da inscrição de EE e EI e grupo aplicável às EPR;
- compreender as consequências da qualificação e do nível ou grupo comunicado;
- identificar as decisões que pertencem ao órgão de gestão;
- distinguir responsabilidade executiva de execução técnica;
- definir informação, métricas e evidências que devem ser apresentadas ao órgão de gestão;
- interpretar o risco cibernético como risco financeiro, operacional, jurídico, reputacional, contratual e regulatório;
- definir critérios de escalamento, aceitação temporária, tratamento e revisão do risco residual;
- identificar serviços, fornecedores e dependências críticas;
- compreender riscos de concentração, subcontratação, acessos privilegiados e ausência de alternativas;
- decidir sobre manutenção condicionada, regularização, medidas compensatórias, substituição ou aceitação de risco de terceiros;
- distinguir política, implementação, verificação, eficácia e evidência;
- preparar decisões executivas em contexto de incidente, continuidade e comunicação;
- responder de forma estruturada a pedidos de informação, auditoria ou supervisão;
- definir prioridades e um plano executivo de 30, 60 e 90 dias.

PROGRAMA

SESSÃO 1 - O IMPACTO DE ESTAR ABRANGIDO
Pergunta central: Estamos abrangidos e o que muda para a entidade e para o órgão de gestão?

Conteúdos principais
• RJC e Regulamento n.º 756/2026: vigência e consequências práticas;
• EE, EI e EPR;
• enquadramento, autoidentificação e qualificação;
• MyCiber: dados, comunicações, validação e atualização;
• nível de conformidade comunicado pelo CNCS no processo de qualificação e validação da inscrição de EE e EI;
• Grupo A ou B aplicável às EPR;
• impacto na governação;
• impacto nos recursos;
• impacto nas responsabilidades;
• impacto no reporte;
• impacto na gestão de incidentes;
• impacto na supervisão;
• Responsável de Cibersegurança;
• ponto de contacto permanente;
• primeiras decisões do órgão de gestão;
• prioridades dos primeiros 30 dias.

Exercício principal
A entidade foi qualificada. O que tem de decidir o órgão de gestão nos próximos 30 dias?

Fichas executivas entregues
• Ficha Executiva de Impacto da Abrangência;
• Mapa das Decisões Imediatas;
• Perguntas ao CISO;
• Checklist de informação e evidência a apresentar à gestão.

SESSÃO 2 - GOVERNAÇÃO, RISCO RESIDUAL E SUPERVISÃO
Pergunta central: Que riscos, recursos, exceções e medidas têm de subir ao órgão de gestão?

Conteúdos principais
• responsabilidade executiva versus execução técnica;
• governação;
• autoridade;
• reporting;
• escalamento;
• medidas mínimas;
• critérios de verificação;
• evidência;
• diferença entre documento, implementação, teste e eficácia;
• risco inerente;
• controlos existentes;
• risco tratado;
• risco residual;
• critérios de escalamento;

• aceitação temporária de risco;
• condições e prazo da aceitação;
• revisão da decisão;
• prioridades de investimento;
• decisões sobre exceções;
• KPI;
• KRI;
• tolerâncias;
• decisões associadas ao painel executivo.

Exercício principal
O CISO apresenta um risco residual acima da sua autoridade. Que decisão deve o órgão de gestão tomar?

Fichas executivas entregues
• Ficha de Escalamento e Decisão de Risco Residual;
• Modelo de Deliberação Executiva;
• Painel Executivo NIS2;
• Registo de Acompanhamento e Revisão.

SESSÃO 3 - CADEIA DE ABASTECIMENTO CRÍTICA
Pergunta central: De quem depende o nosso serviço e o que acontece se esse fornecedor falhar?

Conteúdos principais
• serviços críticos externos;
• dependências essenciais;
• identificação de fornecedores críticos;
• criticidade;
• concentração;
• substituibilidade;
• acessos privilegiados;
• dados tratados pelo fornecedor;
• subcontratação;
• localização do serviço;
• risco contratual;
• risco técnico;
• risco operacional;
• risco de continuidade;
• evidência do fornecedor;
• limites das certificações;
• requisitos relativos a incidentes;
• direito de auditoria;
• acesso a logs;
• continuidade;
• planos de saída;
• medidas compensatórias;
• regularização;
• decisão de manter;
• manutenção condicionada;
• substituição;
• aceitação de risco.

Exercício principal
O fornecedor é indispensável, mas o contrato e a evidência são insuficientes.

Fichas executivas entregues
• Mapa Executivo de Dependências Críticas;
• Ficha de Fornecedor Indispensável;
• Decisão de Manutenção Condicionada;
• Plano de Regularização e Medidas Compensatórias.

SESSÃO 4 - INCIDENTE, AUTORIDADE E DEFENSABILIDADE
Pergunta central: Num incidente ou perante o CNCS, conseguimos decidir, demonstrar e corrigir?

Conteúdos principais
• evento;
• incidente;
• incidente significativo;
• crise;
• decisão sob informação incompleta;
• informação mínima que deve chegar ao órgão de gestão;
• continuidade;
• recuperação;
• comunicação;
• preservação de evidência;
• notificações;
• articulação com outras obrigações;

• poderes de supervisão;
• pedidos de informação;
• auditoria;
• resposta factual;
• resposta transparente;
• resposta proporcional;
• identificação de lacunas;
• regularização;
• risco residual;
• plano corretivo;
• Dossier Executivo NIS2;
• plano de 30, 60 e 90 dias.

Exercício principal
Tabletop executivo: incidente num fornecedor crítico, impacto no serviço e pedido de informação da autoridade competente. A simulação é exclusivamente pedagógica e não reproduz um procedimento ou guião oficial do CNCS.

Fichas executivas entregues
• Checklist Executiva de Decisão em Incidente;
• Resposta Inicial à Supervisão;
• Plano Corretivo de 30, 60 e 90 dias;
• Índice do Dossier Executivo NIS2

METODOLOGIA

A formação adota uma metodologia executiva, aplicada e orientada à decisão.

Cada sessão combina:
- exposição estruturada;
- análise do RJC e do Regulamento n.º 756/2026;
- discussão de casos;
- decisão guiada;
- análise de fichas executivas;
- aplicação a cenários realistas;
- plenário orientado;
- demonstração de instrumentos de apoio.

Cada sessão:
- responde a uma pergunta executiva;
- trabalha um caso;
- conduz a uma decisão;
- disponibiliza fichas orientadoras prontas a utilizar internamente.

Em cada sessão são entregues fichas orientadoras parcialmente preenchidas, destinadas a ser:
- distribuídas pelas áreas responsáveis;
- completadas internamente;
- validadas pelos responsáveis competentes;
- devolvidas ao órgão de gestão;
- usadas para decisão, aprovação, supervisão ou acompanhamento.

O programa **inclui demonstrações selecionadas do CYBERSECURE.AI**:
- estruturação de informação;
- acompanhamento de decisões;
- identificação de lacunas;
- organização de fornecedores e dependências;
- registo de risco residual;
- preparação de evidência;
- construção de planos de ação.

A última sessão inclui um tabletop executivo com incidente num fornecedor crítico e simulação pedagógica de pedido de informação da autoridade competente.

A avaliação é contínua, formativa e centrada na participação, são considerados:
- assiduidade;
- participação nas discussões;
- qualidade das intervenções;
- capacidade para distinguir decisão executiva de execução técnica;
- capacidade para identificar riscos e dependências críticas;
- capacidade para formular decisões proporcionais;
- participação nos casos e exercícios;
- participação no tabletop final.

FORMADORES

O curso é assegurado por uma dupla sénior técnico-jurídica com experiência real em governação executiva, implementação de sistemas de

cibersegurança e análise de regimes sancionatórios.

Henrique Necho
Formador certificado com vasta experiência profissional em cibersegurança, auditoria, privacidade, governação e regulação tecnológica.
Certificações profissionais relevantes, incluindo CISM, CISA e CIPP/E.
Investigação e escrita do livro “NIS2 — Implementação Prática para Responsáveis de Cibersegurança (CISOs)”.
Responsável pela conceção do CYBERSECURE.AI e pelo seu alinhamento com o RJC e o Regulamento n.º 756/2026.

Maria José Lima
Formadora certificada
Jurista especializada em Ciências Jurídico-Económicas
25 anos de experiência
Esperiência em procedimentos contraordenacionais e regimes sancionatórios
Auditora Interna de Qualidade ISO 9001

DESTINATÁRIOS

Esta formação destina-se prioritariamente a:
- membros de órgãos de gestão, direção e administração;
- administradores executivos e não executivos;
- diretores-gerais;
- dirigentes superiores;
- CEOs;
- managing directors;
- responsáveis máximos de unidades de negócio.

Como público complementar, poderão participar:
- CIOs;
- CISOs;
- Responsáveis de Cibersegurança;
- responsáveis de risco;
- responsáveis de compliance;
- juristas internos;
- responsáveis de auditoria interna;

desde que participem para apoiar ou assessorar diretamente o órgão de gestão.

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