ONLINE | NIS2 EXECUTA - Implementação Prática para Responsáveis de Cibersegurança

DATAS
6, 9, 13, 16, 20, 23, 27 e 30 de outubro de 2026 (3ªF e 6ªF)

HORÁRIO
09:30 - 12:30

PREÇO
Associado AEP: **765€**
Outros: **850€**

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
38 horas: 24h síncronas + 14h assíncronas

ENQUADRAMENTO

NIS2 EXECUTA - Implementação Prática para Responsáveis de Cibersegurança
Da obrigação à execução. Da execução à evidência.

O Decreto-Lei n.º 125/2025, de 4 de dezembro, aprovou o Regime Jurídico da Cibersegurança e transpôs para a ordem jurídica nacional a Diretiva (UE) 2022/2555. O Regulamento n.º 756/2026, **em vigor desde 23 de junho, concretizou matérias essenciais à execução do regime, incluindo o funcionamento da MyCiber, o QNRCS 2.0, a Matriz de Risco, os níveis de conformidade, as medidas mínimas, a gestão do risco residual, o relatório anual e as comunicações com as autoridades competentes.**

Para os Responsáveis de Cibersegurança, a questão deixou de ser apenas compreender a NIS2. É necessário transformar o enquadramento legal e regulamentar em decisões, responsabilidades, controlos, testes, evidências, escalamentos e planos de melhoria que possam ser acompanhados pela gestão e demonstrados em contexto de supervisão.

O programa de formação NIS2 EXECUTA foi concebido para Responsáveis de Cibersegurança/CISOs e profissionais que coordenam a implementação do regime em Entidades Essenciais, Entidades Importantes e Entidades Públicas Relevantes. O programa combina enquadramento jurídico-operacional, exercícios de grupo, casos continuados, atividades assíncronas, templates editáveis e funcionalidades selecionadas do **CYBERSECURE.AI**, sempre sujeitas a validação humana.

Os trabalhos desenvolvidos ao longo do curso alimentam uma estrutura inicial de **Dossier Técnico de Implementação NIS2**. O Dossier não substitui a implementação, o teste, a aprovação ou a evidência da entidade. Organiza a cadeia entre obrigação, decisão, execução, verificação, evidência, risco residual, reporte e defesa.

Alguns elementos disponibilizados:
- Manual digital do formando, atualizado ao RJC e ao Regulamento n.º 756/2026.
- Guiões dos exercícios síncronos e dossiers de caso.
- Templates editáveis DT-01 a DT-07.
- Matriz de medidas, testes e evidências.
- Modelos de registo de risco, avaliação de fornecedores e incidentes.
- Playbook do cyber tabletop final.
- Acesso ao CYBERSECURE.AI durante o curso + 30 dias para apoio à realização da componente prática do curso.

Consulte todos os cursos do percurso NIS2 aqui

OBJETIVOS

No final do programa, os participantes estarão aptos a:

- Analisar e documentar o enquadramento da entidade no RJC, distinguindo factos, pressupostos e informação em falta.

- Preparar a autoidentificação e acompanhar o processo de qualificação na MyCiber.
- Interpretar a qualificação, o nível de conformidade atribuído pelo CNCS ou o grupo aplicável às EPR, e traduzir essa decisão em consequências operacionais.
- Estruturar um modelo de governação que defina autoridade, responsabilidades, suplência, reporte e escalamento.
- Relacionar medidas mínimas, implementação concreta, critérios de verificação, testes e evidências.
- Organizar a gestão dos riscos, o tratamento e o escalamento do risco residual.
- Avaliar fornecedores críticos, dependências, lacunas contratuais e medidas compensatórias.
- Qualificar incidentes, registar decisões, preparar notificações e articular resposta, continuidade e recuperação.
- Construir e manter uma estrutura inicial de Dossier Técnico de Implementação NIS2.
- Preparar respostas factuais e defensáveis a pedidos de informação, auditorias, inspeções ou processos de regularização.

PROGRAMA

Módulo 1 - Aplicabilidade, Autoidentificação e MyCiber
Pergunta dominante: A entidade está abrangida e que ações deve iniciar?
Sessão síncrona: 3 horas | Atividade assíncrona: 2 horas

• Arquitetura do RJC e do Regulamento n.º 756/2026.
• Hierarquia entre obrigação legal, regulamentação, orientação oficial e boa prática.
• Entidades Essenciais, Entidades Importantes e Entidades Públicas Relevantes.
• Setores, subsetores, dimensão e relações entre empresas.
• Autoidentificação, registo provisório, qualificação e atualização de dados na MyCiber.
• Decisão documentada de abrangência ou não abrangência.

Exercício síncrono: EX01 — "Estamos abrangidos? A administração quer uma resposta até amanhã." Caso Pedro Ferreira / Sabores do Vale. O grupo distingue factos, pressupostos e lacunas e prepara uma nota preliminar de abrangência.

Atividade assíncrona: AA01 — Nota de enquadramento da entidade: setor, atividade, dimensão, relações relevantes, possível qualificação, factos a confirmar, decisão recomendada e evidência.
Output / Dossier: DT-01 — Enquadramento, abrangência e qualificação.
CYBERSECURE.AI: Assistente de enquadramento e recolha estruturada de factos.

Módulo 2 - Governação, Responsável de Cibersegurança e Ponto de Contacto Permanente
Pergunta dominante: Quem decide, quem executa, quem verifica e quem responde?
Sessão síncrona: 3 horas | Atividade assíncrona: 2 horas

• Deveres dos órgãos de gestão, direção e administração.
• Funções, autoridade e limites do Responsável de Cibersegurança.
• Ponto de contacto permanente, titulares, suplentes e disponibilidade.
• Modelo de reporte, escalamento e tomada de decisão.
• Matriz de responsabilidades e segregação de funções.
• Relação entre Dossier Técnico e Dossier Executivo.

Exercício síncrono: EX02 — "Responsável sem autoridade." Caso Teresa Lima / Hidromira. O grupo corrige um modelo de governação insuficiente e define autoridade, reporte, escalamento e evidências.

Atividade assíncrona: AA02 — Modelo de governação: papéis, autoridade, suplência, decisões reservadas, reporting, reuniões e evidências.
Output / Dossier: DT-02 — Modelo de governação e responsabilidades.
CYBERSECURE.AI: Matriz assistida de responsabilidades e fluxos de escalamento.

Módulo 3 - Qualificação, Nível de Conformidade ou Grupo e Consequências Operacionais
Pergunta dominante: Como interpretar e operacionalizar a decisão recebida na MyCiber?
Sessão síncrona: 3 horas | Atividade assíncrona: 2 horas

• Distinção entre autoidentificação, qualificação e validação do registo.
• Informação utilizada no processo oficial e obrigação de atualização.
• Nível Básico, Substancial ou Elevado para EE e EI, atribuído pelo CNCS no processo de validação.
• Grupo A ou Grupo B para EPR e medidas correspondentes.
• Caráter cumulativo das medidas dos níveis ou grupos aplicáveis.
• Validação dos dados, correção, esclarecimento e reação fundamentada.
• Distinção entre nível regulamentar, maturidade e análise interna de riscos.

Exercício síncrono: EX03 — "A MyCiber notificou a decisão. Os dados estão certos?" Caso Hidromira. O grupo valida os dados, interpreta a decisão, identifica impactos e recomenda aceitar, corrigir, esclarecer ou reagir.

Atividade assíncrona: AA03 — Ficha de qualificação e requisitos aplicáveis. Quando a decisão ainda não exista, o participante regista expressamente que o nível não foi atribuído pelo CNCS e trabalha apenas com cenários provisórios de planeamento.
Output / Dossier: DT-03 — Qualificação, nível ou grupo e requisitos aplicáveis.
CYBERSECURE.AI: Registo e validação da decisão MyCiber, sem atribuição autónoma de nível.

Módulo 4 - Medidas Mínimas, Implementação, Verificação e Evidência
Pergunta dominante: A medida está implementada, testada e evidenciada?
Sessão síncrona: 3 horas | Atividade assíncrona: 2 horas

• QNRCS 2.0: Gerir, Identificar, Proteger, Detetar, Responder e Recuperar.
• Anexo III — medidas mínimas para EE e EI.
• Anexo IV — medidas mínimas para EPR.
• Relação entre controlo, medida e critério de verificação.

• Estados de implementação e critérios de evidência.
• Teste, output, atualidade, origem, integridade e rastreabilidade.
• Lacunas, ações corretivas e risco residual.

Exercício síncrono: EX04 — “Documento não é controlo.” Caso Nuno Monteiro / Câmara de Vilamonte. O grupo avalia três pacotes de evidência e decide se existe documentação, implementação, verificação ou eficácia.

Atividade assíncrona: AA04 — Matriz de implementação e evidência aplicada a cinco a oito medidas prioritárias da entidade.
Output / Dossier: DT-04 — Matriz de medidas, verificação e evidência.
CYBERSECURE.AI: Gestor de medidas, testes, evidências e ações corretivas.

Módulo 5 - Gestão dos Riscos e Risco Residual
Pergunta dominante: Que risco permanece, como deve ser tratado e quem decide?
Sessão síncrona: 3 horas | Atividade assíncrona: 2 horas

• Contexto, serviços críticos, ativos e dependências.
• Cenários de risco: ameaça, vulnerabilidade e consequência.
• Risco inerente, controlos existentes e risco residual.
• Tratamento: evitar, reduzir, transferir ou aceitar.
• Critérios de tolerância, autoridade e escalamento.
• Plano de tratamento, prazos, triggers e monitorização.
• Relação entre medidas mínimas e medidas adicionais.

Exercício síncrono: EX05 — “O controlo existe. O risco continua.” Caso Hidromira. O grupo compara opções de tratamento e prepara uma nota de escalamento para risco residual que excede a autoridade do CISO.

Atividade assíncrona: AA05 — Registo prioritário de três riscos reais e respetivo plano de tratamento.
Output / Dossier: DT-05 — Registo de riscos e plano de tratamento.
CYBERSECURE.AI: Assistente de cenários, opções de tratamento e escalamento.

Módulo 6 - Cadeia de Abastecimento e Fornecedores Críticos
Pergunta dominante: O fornecedor pode continuar e em que condições?
Sessão síncrona: 3 horas | Atividade assíncrona: 2 horas

• Serviços externos críticos, dependência e substituibilidade.
• Critérios de criticidade e due diligence.
• Acessos privilegiados, dados, subcontratação e concentração.
• Requisitos contratuais e prazos de comunicação de incidentes.
• Monitorização, evidências e direito de auditoria.
• Medidas compensatórias e plano de regularização.
• Saída, substituição, continuidade e risco residual.

Exercício síncrono: EX06 — “Fornecedor indispensável, contrato insuficiente.” Caso Hospital CuidarNorte. O grupo decide manter, manter condicionalmente, suspender ou substituir o fornecedor e define medidas compensatórias.

Atividade assíncrona: AA06 — Registo de três fornecedores críticos, gaps, medidas e plano de regularização.
Output / Dossier: DT-06 — Cadeia de abastecimento e terceiros.
CYBERSECURE.AI: Avaliação assistida de fornecedores, contratos, gaps e ações.

Módulo 7 - Incidentes, Notificação, Continuidade e Recuperação
Pergunta dominante: Quando existe fundamento para notificar e como agir sob incerteza?
Sessão síncrona: 3 horas | Atividade assíncrona: 2 horas

• Deteção, triagem, categorização e escalamento.
• Incidente significativo e critérios regulamentares de impacto.
• Registo do momento em que a entidade conclui que existe ou pode existir impacto significativo.
• Notificação inicial, atualização, fim do impacto e relatório final.
• Comunicação aos destinatários e articulação com RGPD e outras autoridades.
• Continuidade, recuperação e preservação de evidência.
• Análise de causa-raiz, encerramento e lições aprendidas.

Exercício síncrono: EX07 — “Notificar ou continuar a investigar?” Caso Hospital CuidarNorte, com informação entregue em vagas. O grupo mantém a timeline, separa factos de hipóteses e define o momento da decisão.

Atividade assíncrona: AA07 — Procedimento de qualificação, escalamento, notificação, continuidade e preservação de evidência.
Output / Dossier: DT-07 — Gestão, notificação e evidência de incidentes.
CYBERSECURE.AI: Assistente de incidentes, cronologia, checklist de impacto e estrutura de notificação.

Módulo 8 - Cyber tabletop final, Dossier Técnico, Supervisão e Defesa
Pergunta dominante: Como demonstrar e defender o que foi decidido, executado, verificado e corrigido?
Sessão síncrona: 3 horas

• Estrutura e manutenção do Dossier Técnico.
• Ligação entre obrigação, decisão, controlo, teste, evidência e risco.
• Pedidos de informação, auditorias, inspeções e regularização.
• Resposta factual, limitações, lacunas e plano corretivo.
• Visão técnica e síntese executiva.
• Controlo de versões, origem, data e integridade da evidência.

• Atualização do risco e lições aprendidas.

Exercício síncrono: EX08 — Cyber tabletop final “72 horas depois: incidente significativo e auditoria do CNCS”. A Hidromira responde a um incidente originado num fornecedor e, depois, a um pedido simulado de informação e evidência da autoridade.

Atividade assíncrona: Não existe atividade assíncrona obrigatória. O módulo consolida os sete outputs anteriores e orienta a conclusão do Dossier.
Output / Dossier: Resposta inicial à supervisão, índice do Dossier, mapa de evidências, plano corretivo 30/60/90 dias e nota ao órgão de gestão.
CYBERSECURE.AI: Audit Readiness e Dossier Review: cruzamento de pedidos, documentos, evidências, lacunas e ações.

METODOLOGIA

A metodologia assenta em **learning by doing** e na aplicação progressiva do método do curso. **Cada módulo combina exposição estruturada, decisão em grupo, discussão em plenário, consolidação interativa e trabalho aplicado à entidade do participante.**

Os exercícios síncronos trabalham uma tensão e uma decisão dominante. O trabalho assíncrono aplica o mesmo método à realidade da entidade do participante e produz uma peça do Dossier Técnico.

Utilização do CYBERSECURE.AI
O CYBERSECURE.AI é uma ferramenta de apoio à conformidade com o RJC (DL 125/2025) e o Regulamento n.º 756/2026. O curso privilegia o uso de algumas funcionalidades da aplicação, no apoio direto aos exercícios.

A avaliação é contínua, orientada à aplicação e compatível com a natureza profissional do programa.
- Participação e contributo nas sessões síncronas e exercícios de grupo
- Realização das atividades assíncronas e qualidade das peças do Dossier
- Participação no cyber tabletop final e capacidade de decisão, evidência e escalamento

A avaliação considera clareza da decisão, fundamento, adequação da autoridade, implementação proposta, método de verificação, qualidade da evidência, identificação de lacunas e tratamento do risco residual.

FORMADORES

Henrique Necho

- Formador certificado
- 30 anos de experiência profissional em cibersegurança, auditoria, governação e regulação tecnológica.
- Responsável de Cibersegurança (CISO) de entidade pública relevante
- Consultor principal em projetos de conformidade NIS1 e NIS2
- Certificações profissionais relevantes, incluindo CISM, CISA e ISO/IEC 27001.
- Investigação e escrita do livro “NIS2 EXECUTA - 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.

DESTINATÁRIOS

O curso destina-se prioritariamente a:

- Responsáveis de Cibersegurança e CISOs.
- Profissionais designados ou em processo de designação para a função.
- Responsáveis de segurança da informação e de coordenação da implementação NIS2.
- CIOs, CTOs e responsáveis de IT com funções relevantes de cibersegurança.
- Gestores de risco tecnológico, continuidade e resposta a incidentes.
- Profissionais de compliance, auditoria interna e jurídico que apoiem o CISO.
- Consultores e auditores que apoiem EE, EI ou EPR.

É particularmente relevante para profissionais de Entidades Essenciais, Entidades Importantes e Entidades Públicas Relevantes, bem como para organizações que integrem cadeias de abastecimento críticas de entidades abrangidas.

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