ONLINE | NIS2 PROTEGE - Gestão da Cadeia de Abastecimento e Planos de Saída

DATAS
2, 9 e 16 de novembro de 2026

HORÁRIO
09:30 - 12:30

PREÇO
Associado AEP: **495€**
Outros: **550€**

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
9 horas

ENQUADRAMENTO

NIS2 PROTEGE - Gestão da Cadeia de Abastecimento e Planos de Saída
Fornecedores críticos, risco residual, restrição e saída segura

Está a receber questionários NIS2 dos seus grandes Clientes? Quer saber como responder, organizar as evidências e cumprir com os requisitos destes Clientes?

A segurança da cadeia de abastecimento exige que as entidades conheçam os fornecedores, produtos e serviços dos quais dependem, avaliem o risco de cada relação, definam requisitos proporcionais, acompanhem a respetiva execução e preparem alternativas quando o risco deixe de ser aceitável.

Uma certificação, um questionário ou uma cláusula contratual não eliminam a responsabilidade da entidade. É necessário compreender que serviços, processos e ativos dependem de terceiros, que impacto pode resultar da indisponibilidade ou comprometimento do fornecedor, que controlos estão efetivamente implementados, que evidência existe e que risco permanece.

O curso transforma estas exigências num ciclo prático:
selecionar ? avaliar ? contratar ? monitorizar ? regularizar ? restringir ? substituir ? encerrar.

São trabalhados fornecedores críticos, produtos e serviços TIC, cloud, MSP e MSSP, acessos privilegiados, vulnerabilidades, desenvolvimento seguro, risco de concentração, dependência tecnológica, risco residual, continuidade, transição e planos de saída.

Em três sessões síncronas, os participantes analisam um caso integrado, tomam decisões e utilizam templates editáveis. A terceira sessão inclui um exercício de simulação sobre a restrição e substituição de um fornecedor crítico.

O programa utiliza como referenciais o Regime Jurídico da Cibersegurança, o Regulamento n.º 756/2026, o QNRCS 2.0, o Roteiro NIS2 do CNCS e o ENISA Technical Implementation Guidance — Supply Chain Security, de acordo com a respetiva natureza e força.

O **ENISA TIG é utilizado como orientação técnica complementar** e não vinculativa, **nomeadamente para aprofundar critérios de seleção, requisitos contratuais, monitorização do ciclo de vida, dependência tecnológica, componentes de software livre e de código aberto, revisão extraordinária e encerramento seguro.**

É disponibilizado o **Toolkit Essencial NIS2 - Protege com os templates editáveis, e reutilizáveis, a utilizar nos exercícios:**
- Ficha Integrada de Avaliação do Fornecedor e do Produto;
- Ficha de Análise e Aceitação do Risco Residual;
- Matriz de Responsabilidades e Requisitos Contratuais;
- Plano de Monitorização, Regularização e Verificação de Eficácia;
- Plano de Restrição, Saída e Substituição;
- Checklist e Termo de Encerramento Seguro.

Consulte todos os cursos do percurso NIS2 aqui

OBJETIVOS

No final da formação, os participantes deverão ser capazes de:

1. Identificar fornecedores, produtos, serviços e dependências críticas.
2. Avaliar criticidade, concentração, exposição, substituibilidade e impacto.
3. Distinguir risco do fornecedor, risco do produto e risco da relação.
4. Executar uma due diligence proporcional antes da contratação ou renovação.
5. Definir requisitos contratuais e operacionais verificáveis.
6. Avaliar risco inerente, controlos, eficácia e risco residual.
7. Preparar decisões de manutenção, regularização, restrição ou substituição.
8. Monitorizar o fornecedor ao longo do ciclo de vida e desencadear reavaliações.
9. Estruturar planos de saída, transição e encerramento seguro.
10. Organizar decisões, evidências e aprovações para o Dossier NIS2.

PROGRAMA

SESSÃO 1 - Avaliar Antes de Contratar
Pergunta central: Temos informação suficiente para selecionar o fornecedor, o produto e o modelo de relação?

• política de segurança da cadeia de abastecimento;
• papel da entidade na cadeia;
• serviços, processos, ativos e dependências críticas;
• diretório de fornecedores, produtos, serviços e contactos;
• critérios de classificação e criticidade;
• práticas de cibersegurança do fornecedor;
• desenvolvimento seguro e gestão de vulnerabilidades;
• qualidade e resiliência do produto ou serviço;
• jurisdição e localização;
• estrutura de propriedade;
• capacidade de fornecimento;
• dependência de subfornecedores;
• acessos, dados e níveis de privilégio;
• cloud, MSP, MSSP e serviços geridos;
• interoperabilidade, portabilidade e formatos abertos;
• dependência ou aprisionamento tecnológico;
• alternativas e diversificação;
• componentes de software livre e de código aberto;
• risco inerente, controlos existentes, eficácia, risco atual e risco residual;
• devida diligência antes da adjudicação, assinatura, renovação ou expansão.

Exercício principal: Fornecedor dominante, produto com componentes de software livre e de código aberto, dependência elevada, risco de aprisionamento tecnológico e evidência incompleta.

Outputs trabalhados:
• Ficha Integrada de Avaliação do Fornecedor e do Produto;
• Ficha de Análise e Aceitação do Risco Residual.

Materiais de apoio
• Diretório Mestre de Fornecedores e Serviços;
• Mapa de Dependências, Acessos e Alternativas.

SESSÃO 2 - Contratar, Coordenar e Monitorizar
Pergunta central: O contrato e a monitorização permitem gerir o risco ao longo da relação?

• papéis e responsabilidades internas e externas;
• articulação entre CISO, compras, jurídico, IT, continuidade, dono do serviço e órgão de gestão;
• requisitos contratuais de cibersegurança;
• competências e formação do pessoal do fornecedor;
• antecedentes, quando aplicável;
• gestão de incidentes;
• tratamento de vulnerabilidades;
• auditoria e acesso a relatórios;
• subcontratação;
• continuidade e recuperação;
• níveis de serviço;
• disponibilidade, integridade, autenticidade e confidencialidade;
• localização dos serviços e dos dados;
• obrigação de comunicar alterações materiais;
• contactos e linhas de reporte;
• cooperação com autoridades;
• assistência durante incidentes;
• custos e condições da assistência;
• direitos de cessação;
• transição e obrigações de saída;
• contratos padrão e desequilíbrio negocial;
• compromissos públicos, certificações e evidência alternativa;
• monitorização de SLA;

• incidentes associados ao fornecedor;
• vulnerabilidades e alterações relevantes;
• notas de versão;
• configuração e fim de suporte;
• revisões extraordinárias;
• medidas corretivas;
• medidas compensatórias;
• verificação da eficácia e reteste;
• desvios, supervisão e risco residual.

Exercício principal: O fornecedor recusa alterar o contrato padrão. O caso evolui por vagas:
1 - falha de SLA;
3 - alteração de localização ou subcontratante;
3 - nova vulnerabilidade ou versão com impacto de segurança;
4 - necessidade de rever o risco e a decisão.

Outputs trabalhados:
• Matriz de Responsabilidades e Requisitos Contratuais;
• Plano de Monitorização, Regularização e Verificação de Eficácia.

Materiais de apoio
• Registo de Revisão Extraordinária;
• Quadro de Supervisão de Fornecedores Críticos..

SESSÃO 3 - Testar, Sair e Encerrar com Segurança
Pergunta central: Conseguimos restringir ou substituir o fornecedor sem comprometer o serviço e sem deixar risco para trás?

• participação dos fornecedores em testes de resposta, recuperação e gestão de crise;
• critérios de restrição, suspensão, cessação, exclusão e substituição;
• continuidade durante a transição;
• reversibilidade;
• período de transição;
• alternativas e capacidade de substituição;
• migração de dados;
• transferência de configurações;
• transferência de chaves e credenciais;
• transferência de documentação;
• transferência de conhecimento;
• propriedade intelectual;
• entrega de logs históricos;
• assistência do fornecedor durante a saída;
• revogação de acessos;
• desativação de contas;
• rotação de credenciais;
• término de fluxos de dados;
• devolução de ativos;
• eliminação segura de dados;
• risco durante a migração;
• risco após substituição;
• obrigações que sobrevivem ao contrato;
• risco pós-cessação;
• evidência de implementação;
• decisão formal de fecho;
• contributos para o Dossier NIS2 e para o relatório anual.

Exercício de simulação final
Restrição da utilização de um fornecedor crítico, com:
• incidente em curso;
• contacto principal indisponível;
• falha de cooperação;
• dependência tecnológica elevada;
• ausência de alternativa pronta;
• necessidade de manter a continuidade;
• decisão entre manutenção temporária, restrição, cessação ou substituição.

Resultado esperado
O grupo deve apresentar:
• decisão;
• autoridade competente;
• fundamento;
• condições;
• prazo;
• medidas compensatórias;
• plano de transição;
• risco residual;
• critérios de fecho;

• evidência a conservar.

Outputs trabalhados
• Plano de Restrição, Saída e Substituição;
• Checklist e Termo de Encerramento Seguro.

Materiais de apoio
• Plano de Exercício Conjunto com Fornecedor Crítico;
• Mapa de Evidências e Aprovações.

METODOLOGIA

Estrutura geral: 3 sessões online de 3 horas.
Ciclo pedagógico: seleção ? contratação ? monitorização ? teste ? saída ? fecho.

A formação adota uma metodologia aplicada e orientada à decisão.

Cada sessão combina:
- enquadramento jurídico-operacional;
- análise de casos;
- exercício em grupo;
- discussão em plenário;
- utilização de templates editáveis;
- consolidação de decisões e evidências.

O curso segue uma cadeia comum: serviço e dependência ? fornecedor e produto ? risco ? requisitos ? decisão ? monitorização ? saída ? evidência.

A cadeia de governação é trabalhada da seguinte forma: responsável de cibersegurança propõe ? áreas internas instruem ? órgão competente decide ? responsáveis executam ? órgão de gestão supervisiona.

Os exercícios são apresentados através de vagas sucessivas de informação. Os participantes atualizam o risco, os requisitos, a decisão, as medidas, o plano de saída e a evidência à medida que surgem novos factos.

Não existe trabalho assíncrono obrigatório.

O Toolkit é utilizado nos exercícios e disponibilizado para aplicação posterior. Os materiais complementares não são preenchidos integralmente durante a formação.

A avaliação é contínua e formativa, considerando a participação, a qualidade da análise, a capacidade de identificar dependências e riscos, e a fundamentação das decisões tomadas nos exercícios.

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

- CISOs e responsáveis de cibersegurança;
- CIOs, diretores de IT e responsáveis de segurança da informação;
- Responsáveis de compras, contratação e gestão de fornecedores;
- Juristas internos, DPOs e responsáveis de compliance;
- Responsáveis de gestão do risco, continuidade de negócio e auditoria interna;
- Gestores de contratos e de serviços externalizados;
- Responsáveis por serviços cloud, MSP, MSSP e fornecedores tecnológicos críticos;
- Consultores e auditores que apoiem entidades essenciais, importantes ou públicas relevantes.

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