ONLINE | NIS2 RESPONDE - Gestão e Notificação de Incidentes

DATAS
2, 9 e 16 de novembro de 2026

HORÁRIO
14:30 - 17:30

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 RESPONDE - Gestão e Notificação de Incidentes
Qualificar, escalar, notificar, recuperar, fechar e provar

O curso foi concebido para capacitar profissionais que precisam de transformar um alerta técnico num processo organizacional disciplinado: qualificar o incidente, escalar, decidir, notificar, comunicar, recuperar, fechar e provar.

O programa assenta no RJC, no Regulamento n.º 756/2026, em vigor desde 23 de junho, e no QNRCS 2.0 como apoio técnico não vinculativo, no ENISA Technical Implementation Guidance — Incident Handling.

A formação não pretende cobrir em profundidade arquitetura de SIEM, EDR/XDR, threat intelligence, análise forense ou desenho técnico de logging. Estes temas são tratados apenas enquanto condições de preparação e fontes de evidência. **O foco das nove horas está na decisão e na execução do ciclo do incidente.**

O artigo 30.º é integrado no fecho do curso: os participantes aprendem a consolidar números absolutos, percentagens, tendências e indicadores trimestrais e anuais, sem confundir métricas de gestão com requisitos legais autónomos.

É disponibilizado o **Toolkit Essencial NIS2 - Responde** com os templates editáveis, e reutilizáveis, a utilizar nos exercícios:
- Ficha de Triagem e Qualificação.
- Timeline e Registo de Decisões.
- Matriz de Escalamento e Autoridade.
- Registo de Factos, Hipóteses e Desconhecidos.
- Mapa dos Atos de Notificação.
- Matriz de Comunicações e Obrigações Paralelas.
- Checklist de Submissão e Evidência.
- Ficha de Autorização para Recuperação.
- Checklist de Resolução e Fecho.
- Mapa Trimestral e Anual de Incidentes.

Consulte todos os cursos do percurso NIS2 aqui

OBJETIVOS

No final do programa, os participantes estarão aptos a:

- Distinguir evento, incidente, incidente significativo e crise.
- Separar factos, hipóteses, desconhecidos e decisões.
- Aplicar critérios de categorização, severidade, impacto e escalamento.
- Estruturar a articulação entre equipa técnica, CISO, ponto de contacto permanente e órgão de gestão.
- Preparar, validar, autorizar, submeter e evidenciar os atos de notificação.
- Identificar obrigações paralelas de comunicação ou participação.
- Preservar cronologia, versões, recibos, logs e evidência relevante.
- Tomar decisões sobre contenção, continuidade, recuperação e resolução.

- Atualizar risco residual e plano corretivo.
- Consolidar estatística trimestral e anual com números absolutos, percentagens e tendências.
- Preparar contributos para o relatório anual previsto no artigo 30.º.
- Organizar um Dossier de Incidente defensável.

PROGRAMA

SESSÃO 1 - Qualificar e Escalar
Pergunta central: Temos informação suficiente para declarar e escalar o incidente?

- Evento, incidente, incidente significativo e crise.
- Factos confirmados, hipóteses, desconhecidos e fontes.
- Critérios de categorização, severidade, impacto e prioridade.
- Reclassificação quando surge nova informação.
- Timeline e momento da conclusão.
- Papéis: equipa técnica, CISO, ponto de contacto, jurídico/DPO, continuidade e órgão de gestão.
- Critérios para escalamento técnico, organizacional e executivo.
- Preparação técnica essencial: plano, contactos, monitorização e logging enquanto fontes de evidência.

Exercício principal: O alerta chegou. Já temos de declarar e escalar?

Outputs trabalhados:
- Ficha de Triagem e Qualificação.
- Timeline e Registo de Decisões.
- Matriz de Escalamento e Autoridade.
- Registo de Factos, Hipóteses e Desconhecidos.

SESSÃO 2 - Notificar e Comunicar
Pergunta central: Notificar agora, atualizar ou continuar a investigar?

- Visão executiva: notificação inicial, fim do impacto significativo e relatório final.
- Sequência operacional completa, incluindo atualizações e relatórios intercalares quando aplicáveis.
- Plataforma eletrónica: preparação, validação, autorização, submissão e recibos.
- Responsabilidades de quem prepara, valida, autoriza e submete.
- Obrigações paralelas: proteção de dados, participação criminal, requisitos setoriais e contratuais.
- Comunicação interna, externa e com fornecedores.
- Preservação de versões, timestamps e evidência da submissão.
- Diferença entre ausência de responsabilidade adicional pela mera notificação e inexistência de responsabilidade.

Exercício principal: A informação ainda é incompleta. O que submetemos, a quem e com que evidência?

Outputs trabalhados:
- Mapa dos Atos de Notificação.
- Matriz de Comunicações e Obrigações Paralelas.
- Checklist de Submissão na Plataforma.
- Registo de Versões, Recibos e Timestamps.

SESSÃO 3 - Recuperar, Fechar e Provar
Pergunta central: Quando podemos recuperar, declarar resolvido e consolidar o incidente?

- Contenção, continuidade, recuperação e preservação de evidência.
- Critérios para iniciar a recuperação.
- Diferença entre recuperação técnica, fim do impacto significativo, resolução e fecho.
- Risco residual, plano corretivo e ações pendentes.
- Revisão pós-incidente e lições aprendidas.
- Registo Mestre de Incidentes e consolidação trimestral.
- Relatório anual: números, tipos, impacto, problemas, medidas e recomendações.
- Percentagens como métricas de gestão: por tipo, significância, origem em terceiros, deteção interna, causa-raiz e ações concluídas.
- Leitura conjunta de percentagens e números absolutos.
- Diferenças entre EE, EI e EPR quanto ao relatório anual.
- Artigo 30.º e Indicadores

Exercício principal: Cyber tabletop: ransomware num fornecedor crítico, impacto operacional, dados pessoais, decisão de recuperação, fim do impacto, risco residual e contributo para o relatório anual.

Outputs trabalhados:
- Ficha de Autorização para Recuperação.
- Checklist de Resolução e Fecho.
- Plano Corretivo e Risco Residual.
- Mapa Trimestral e Anual de Incidentes.

METODOLOGIA

Cada sessão responde a uma pergunta operacional, integra um exercício principal e produz um conjunto limitado de artefactos.

Os exercícios são apresentados em vagas sucessivas de informação. Os participantes atualizam a timeline, reclassificam o incidente, registam decisões e justificam notificações, recuperação e fecho.
Não existe trabalho assíncrono obrigatório. O **Toolkit Essencial NIS2 - Responde** é trabalhado durante as sessões de formação. A Biblioteca Complementar é entregue como referência, sem explicação exaustiva.

A avaliação é contínua e formativa, considerando a participação, a qualidade da análise, a capacidade de distinguir facto de inferência, a fundamentação das decisões, a coerência dos registos e a participação no tabletop final.

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.
- Equipas SOC, CSIRT e resposta a incidentes.
- Responsáveis de continuidade, recuperação e gestão de crise.
- Juristas internos, DPOs e responsáveis de compliance.
- Auditores internos, gestores de risco e responsáveis por fornecedores críticos.
- Consultores e prestadores que apoiem EE, EI ou EPR.

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