ONLINE | NIS2 RH - Gestão de Recursos Humanos como Fator Crítico na Cibersegurança

DATAS
5, 12 e 19 de novembro de 2026 (quintas-feiras)

HORÁRIO
09:30 – 12:30

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

LOCAL
Online

DURAÇÃO
9 horas

ENQUADRAMENTO

NIS2 RH - Gestão de Recursos Humanos como Fator Crítico na Cibersegurança
Gestão segura de pessoas, funções, formação, acessos e ativos ao longo do ciclo de vida dos trabalhadores

A entidade tem as funções, as pessoas e as competências necessárias para executar as suas responsabilidades de cibersegurança — e consegue demonstrá-lo? Quando uma pessoa entra, muda de função, é suspensa ou sai, quem decide, quem executa, quem confirma e que evidência fica? A formação, os acessos, os ativos e a cobertura das funções acompanham efetivamente o ciclo de vida dos trabalhadores?

O curso foi concebido para capacitar profissionais que precisam de integrar a cibersegurança nos processos de Recursos Humanos, desde a definição e avaliação da função até à seleção, admissão, permanência, capacitação, mudança, sucessão, suspensão, saída e pós-saída.

O enquadramento considera o Regime Jurídico da Cibersegurança e o Regulamento n.º 756/2026, que aprova o QNRCS 2.0 e as medidas mínimas aplicáveis às Entidades Essenciais, Importantes e Públicas Relevantes.

O curso trabalha a integração da Cibersegurança nos processos de Recursos Humanos através de uma lógica simples:
atividade RH ? ação de segurança ? execução ? confirmação ? verificação ? evidência

São distinguidas ações de natureza predominantemente organizacional ou administrativa e técnica.

É disponibilizado o **Toolkit Essencial NIS2 — Recursos Humanos**, com sete artefactos editáveis:

- Questionário de Avaliação da Criticidade, Exposição e Requisitos de Segurança da Função;
- Matriz de Funções, Tarefas, Responsabilidades, Competências, Entregáveis, Titulares, Suplentes e Cobertura;
- Política de Segurança dos Recursos Humanos;
- Checklist de Admissão e Integração Segura;
- Plano de Capacitação em Cibersegurança por Públicos, Funções e Responsabilidades;
- Ficha de Mudança, Suspensão e Saída — Identidades, Acessos, Ativos, Responsabilidades e Obrigações Pós-Relação;
- Registo Integrado de Ações, Validações, Reconhecimentos, Formação, Verificações e Evidências de Recursos Humanos.

Consulte todos os cursos do percurso NIS2 aqui.

OBJETIVOS

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

1. relacionar os processos de Recursos Humanos com o Regime Jurídico da Cibersegurança, o Regulamento, o QNRCS e as medidas mínimas aplicáveis;
2. distinguir atividade de Recursos Humanos de ação de segurança associada;
3. traduzir requisitos de cibersegurança em tarefas, funções, responsabilidades, competências, entregáveis e evidências;
4. distinguir perfil de referência, função organizacional, posto de trabalho, papel num processo e pessoa que exerce a função;
5. avaliar a criticidade e exposição das funções com base em critérios estruturados e fundamentados;
6. relacionar a avaliação da função com requisitos proporcionais de competências, formação, acessos, ativos, verificações, cobertura e evidência;
7. utilizar o ECSF como referencial de apoio à descrição e combinação de funções, tarefas, competências e entregáveis;

8. identificar lacunas de capacidade e fundamentar decisões de desenvolvimento, aperfeiçoamento, requalificação, redistribuição, recrutamento ou recurso externo;
9. integrar requisitos de segurança nos processos de seleção, contratação, admissão, permanência, mudança, suspensão, saída e pós-saída;
10. articular o ciclo de vida das identidades, acessos e ativos com os acontecimentos registados por Recursos Humanos;
11. estruturar planos de capacitação em cibersegurança por públicos, funções, responsabilidades e exposição;
12. distinguir formação realizada de compreensão demonstrada, organizando mecanismos de avaliação, reforço e reavaliação;
13. organizar revisões planeadas e revisões desencadeadas por eventos relevantes;
14. identificar titulares, suplentes, dependências de pessoa-chave e necessidades de cobertura;
15. executar verificações cruzadas entre eventos de RH, acessos, ativos e evidências;
16. identificar ações incompletas, lacunas e pendências e preparar medidas de regularização;
17. reconhecer situações que devem ser escaladas para decisão ou supervisão do órgão de gestão;
18. organizar responsabilidades, ações, verificações e evidências através do Toolkit Essencial NIS2 — Recursos Humanos.

PROGRAMA

SESSÃO 1 — Classificar funções, definir responsabilidades e preparar uma entrada segura
Pergunta central: Que funções exigem que responsabilidades e medidas de segurança, e como justificamos essa decisão?

- Da função para as responsabilidades
- Avaliação da criticidade e exposição
- Da classificação para requisitos
- Obrigação, tarefa, competência e capacidade
- European Cybersecurity Skills Framework – ECSF
- Adequação da Pessoa
- Política de Segurança dos Recursos Humanos
- Entrada segura

Exercício principal: "A função é crítica. Mas com base em quê?" — análise de uma função cuja criticidade foi assumida sem critérios claros, com lacunas de competências, acessos, cobertura e evidência.
Outputs trabalhados: Questionário de Avaliação da Criticidade, Exposição e Requisitos de Segurança da Função; Matriz de Funções, Tarefas, Responsabilidades, Competências, Entregáveis, Titulares, Suplentes e Cobertura; Política de Segurança dos Recursos Humanos; Checklist de Admissão e Integração Segura.

SESSÃO 2 — Manter competências, capacitação, compreensão, acessos e cobertura
Pergunta central: Como demonstrar que as pessoas mantêm competências, compreensão, acessos e recursos adequados às funções que desempenham?

- Diferentes públicos, diferentes necessidades
- Plano de capacitação
- Articulação com as necessidades de capacitação dos trabalhadores e dos órgãos de gestão
- Formação específica e desenvolvimento da capacitação
- Da formação à compreensão
- Formação por gatilho
- Indicadores e cobertura
- Mudança de função
- Validação por área
- Verificação cruzada RH-TIC-Cibersegurança

Exercício principal: "A pessoa mudou. Os controlos e competências ficaram para trás." — análise de uma promoção em que persistem acessos antigos, faltam competências, formação e suplência e não existe confirmação de todas as alterações.
- Outputs trabalhados: Matriz de Funções, Tarefas, Responsabilidades, Competências, Entregáveis, Titulares, Suplentes e Cobertura; Plano de Capacitação em Cibersegurança por Públicos, Funções e Responsabilidades; Ficha de Mudança, Suspensão e Saída — componente de mudança.

SESSÃO 3 — Suspender, transferir, sair, suceder e fechar com evidência
Pergunta central: Como alterar ou terminar uma relação sem deixar acessos, ativos, responsabilidades, conhecimento, competências ou obrigações de segurança por tratar?
Obrigações que permanecem
Identidades e acessos
Ativos
Sucessão e transferência do conhecimento
Capacidade após saída
Pessoas externas
Pós-saída
Matérias para decisão e supervisão
Exercício final integrador: "A pessoa saiu, mas a função e as tarefas continuam." O caso evolui por vagas sucessivas e obriga os participantes a tratar acessos, ativos, sucessão, capacidade, dependências, escalamento e evidência antes de decidir se o processo pode ser encerrado.
Outputs trabalhados: Ficha de Mudança, Suspensão e Saída — Identidades, Acessos, Ativos, Responsabilidades e Obrigações Pós-Relação; Registo Integrado de Ações, Validações, Reconhecimentos, Formação, Verificações e Evidências de Recursos Humanos. São consolidados os restantes templates do Toolkit.

METODOLOGIA

A formação é prática, progressiva e orientada para profissionais de Recursos Humanos e funções de suporte, sem exigir conhecimentos técnicos avançados de cibersegurança.

Cada sessão parte de uma pergunta operacional, apresenta o enquadramento necessário, demonstra critérios de análise e evolui para um exercício principal baseado

num caso apresentado por vagas sucessivas de informação.

Os participantes trabalham a partir de factos confirmados, hipóteses, informação em falta, requisitos, responsabilidades, opções de decisão, ações, verificações e evidências. Os templates são utilizados como suporte à decisão e à organização da evidência, e não como objetivo autónomo de preenchimento.
A formação segue a assinatura pedagógica:
APRESENTAR ? DEMONSTRAR ? PRATICAR ? DISCUTIR ? VERIFICAR ? CONSOLIDAR.

Existem dois exercícios assíncronos facultativos, após as sessões 1 e 2.

O curso trabalha progressivamente o **Toolkit Essencial NIS2 — Recursos Humanos** e disponibiliza Documentação Pedagógica Complementar para apoio à aplicação posterior.

A avaliação é contínua e formativa.

FORMADOR

Henrique Necho

- Formador certificado
- Responsável de Cibersegurança, consultor e formador em NIS2
- Mais de 30 anos de experiência profissional nas áreas de redes e sistemas, cibersegurança, auditoria, privacidade, governação e regulação tecnológica
- Trabalho orientado para a tradução de requisitos legais e regulamentares em decisões, responsabilidades, medidas, processos, verificações e evidências aplicáveis às organizações
- Responsável pela conceção técnica e pedagógica do portefólio de formação NIS2 e dos respetivos casos, exercícios, Toolkits e Dossiers
- Certificações profissionais: CISM, CISA, ISO/IEC 27001 Lead Implementer, ISO/IEC 27005 Senior Risk Manager, CIPP/E, CIPM e CIPT
- Investigação e escrita do livro "NIS2 EXECUTA — Implementação Prática para Responsáveis de Cibersegurança (CISOs)"
- Responsável pela conceção do CYBERSECURE e pelo seu alinhamento com o RJC e o Regulamento n.º 756/2026

No NIS2 RH, Henrique Necho orienta os participantes na tradução dos requisitos aplicáveis em funções, responsabilidades, competências, processos de Recursos Humanos, articulação RH–TIC, capacitação, acessos, ativos, verificações e evidências, preservando a distinção entre decisão organizacional, execução técnica e validação pelas funções competentes.

DESTINATÁRIOS

A formação destina-se prioritariamente a:

- diretores, gestores e técnicos de Recursos Humanos;
- profissionais de recrutamento e seleção, formação e desenvolvimento, gestão de talento e competências;
- HR Business Partners e responsáveis por admissão, mobilidade, sucessão, suspensão e saída;
- responsáveis pela definição ou revisão de descrições de função;
- funções de suporte que desencadeiam ou acompanham alterações de acessos e gestão de ativos;
- responsáveis de instalações e segurança física.

Podem também participar:

- Responsáveis de Cibersegurança, CISOs e profissionais de governação da cibersegurança;
- profissionais de TIC, cibersegurança, identidade e gestão de acessos;
- profissionais de jurídico-laboral, compliance e proteção de dados;
- responsáveis pela gestão de ativos, segurança física, auditoria interna e chefias funcionais ou operacionais.

Não são exigidos conhecimentos técnicos avançados de cibersegurança. É recomendável experiência ou intervenção atual ou futura em Recursos Humanos, recrutamento, formação, gestão de competências, acessos, ativos, TIC, cibersegurança, compliance, jurídico-laboral, proteção de dados ou chefia de equipas.

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