Curso CSNI200 - NIS2 | Implementação para o responsável de cibersegurança

Duração: 14h

Introdução

Este curso prepara o responsável de cibersegurança para pôr em prática a NIS2 em Portugal, nos termos do Decreto-Lei n.º 125/2025 (Regime Jurídico da Cibersegurança) e do Regulamento n.º 756/2026 do CNCS: registo e comunicações na plataforma do CNCS, análise e gestão dos riscos, medidas mínimas do Quadro Nacional de Referência para a Cibersegurança, notificação de incidentes e relatório anual.

A partir dos textos oficiais e de casos práticos, cada medida é traduzida no que é preciso fazer e na evidência que o CNCS pede para a verificar. O curso relaciona as medidas com as normas que o próprio regulamento usa como referência, como a ISO/IEC 27001 e o NIST Cybersecurity Framework 2.0.

Público-alvo

Este curso destina-se a responsáveis de cibersegurança e de segurança da informação, pontos de contacto permanentes, responsáveis de sistemas de informação, de risco, de auditoria e de conformidade, e a consultores que acompanham entidades essenciais e importantes na adaptação ao regime.

No final do curso

Após a conclusão deste curso, os formandos deverão ser capazes de:
• Determinar se a entidade é abrangida, a sua qualificação e o nível de conformidade que lhe corresponde.
• Tratar do registo e das comunicações na plataforma eletrónica do CNCS.
• Conduzir a análise e a gestão dos riscos, incluindo o risco residual e a cadeia de abastecimento.
• Interpretar as medidas mínimas do Quadro Nacional de Referência para a Cibersegurança e preparar a evidência de cada uma.
• Organizar a notificação de incidentes ao CNCS, da notificação inicial ao relatório final.
• Elaborar o relatório anual e informar os órgãos de gestão, direção e administração.
• Definir o plano de sensibilização e formação da organização.

Pré-requisitos

Conhecimentos gerais de sistemas de informação e de gestão do risco. A experiência com a ISO/IEC 27001 ajuda, mas não é obrigatória.

Exames de certificação

(não existem exames)

Conteúdo programático em detalhe

O regime e a sua aplicação
• Da Diretiva NIS2 ao Decreto-Lei n.º 125/2025 e ao Regulamento n.º 756/2026
• Entidades essenciais, importantes e públicas relevantes
• Qualificação da entidade e dever de registo

• A plataforma eletrónica do CNCS: perfis, registo e comunicações
• Produção de efeitos e regime transitório

Governação e funções

• As obrigações dos órgãos de gestão, direção e administração
• O responsável de cibersegurança: designação, funções e comunicação ao CNCS
• O ponto de contacto permanente
• Grupos empresariais e acumulação de funções
• Informar a administração: o que reportar e com que periodicidade

O Quadro Nacional de Referência para a Cibersegurança

• Objetivos: gerir, identificar, proteger, detetar, responder e recuperar
• Categorias e controlos de cibersegurança
• Relação com a ISO/IEC 27001, o NIST Cybersecurity Framework 2.0 e os CIS Controls

Análise e gestão dos riscos

• A matriz de risco e os cenários de risco
• Níveis de conformidade: básico, substancial e elevado
• Ativos e serviços críticos
• Análise de riscos e gestão do risco residual
• Segurança da cadeia de abastecimento

Medidas mínimas e evidências

• As medidas mínimas e os critérios de verificação
• Gestão de identidades, autenticação e controlo de acessos
• Segurança dos dados e das plataformas
• Resiliência da infraestrutura, cópias de segurança e continuidade
• Criptografia e cifragem
• Formação e sensibilização: plano, registos e indicadores
• Caso prático: o ponto de partida de uma entidade face às medidas mínimas

Incidentes

• O que é um incidente significativo
• Notificação inicial, notificação do fim do impacto significativo, relatório intercalar e relatório final
• Formato, procedimento e taxonomia definidos pelo CNCS
• Comunicação aos destinatários dos serviços
• Caso prático: notificar um incidente do início ao fim

Supervisão, relatório anual e melhoria contínua

• O relatório anual
• Supervisão e execução: inspeções, auditorias de segurança, pedidos de informação e instruções do CNCS
• Regime sancionatório
• Melhoria contínua
• Caso prático: plano de adaptação para os 12 meses seguintes