ONLINE | NIS2 CONTINUIDADE - Continuidade de Atividades, Recuperação de Desastres e Gestão de Crises

DATAS
3, 10 e 17 de novembro de 2026 (terças-feiras)

HORÁRIO
14:30 – 17:30

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

LOCAL
Online

DURAÇÃO
9 horas

ENQUADRAMENTO

NIS2 CONTINUIDADE - Continuidade de Atividades, Recuperação de Desastres e Gestão de Crises
Preparar, manter, recuperar e validar serviços, funções ou atividade críticas perante incidentes, interrupções ou desastre

Sabe quais as atividades que não podem parar e durante quanto tempo? Tem cópias de segurança, planos e recursos, mas já verificou se permitem recuperar dentro dos critérios definidos? Consegue demonstrar quem decide o regresso à operação, com que fundamento e com que evidência?
O curso foi concebido para capacitar profissionais que precisam de transformar requisitos de continuidade em critérios, planos, cópias de segurança, verificações, testes, recuperação e evidência, articulando as necessidades do negócio com as capacidades técnicas e organizacionais da entidade.

O curso enquadra estes temas no Regime Jurídico da Cibersegurança, no Regulamento n.º 756/2026 e nas medidas aplicáveis do QNRCS 2.0, distinguindo o que é exigível em função da qualificação, do nível de conformidade ou do grupo aplicável. As orientações técnicas da ENISA são utilizadas como apoio à operacionalização, de acordo com a respetiva natureza e força.

A formação distingue expressamente:

- medidas aplicáveis a Entidades Essenciais e Importantes, de acordo com o nível de conformidade;
- medidas aplicáveis a Entidades Públicas Relevantes, de acordo com o grupo aplicável;
- instrumentos utilizados como preparação, operacionalização ou boa prática técnica.

O curso transforma esta exigências num ciclo:
obrigação aplicável ? atividade crítica ? impacto ? risco ? requisito de continuidade ? medida ? preparação ? teste ? ativação ? recuperação ? validação ? comunicação ? evidência ? ação corretiva ? reteste

É disponibilizado o Toolkit Essencial NIS2 — Continuidade das Atividades, com seis templates editáveis e reutilizáveis, a utilizar nos exercícios:

- Análise de Impacto e Requisitos de Continuidade;
- Plano Integrado de Continuidade e Recuperação;
- Política e Procedimento de Cópias de Segurança;
- Plano de Verificação, Restauro e Testes de Recuperação;
- Plano de Gestão de Crises e Comunicação;
- Registo de Ativação, Recuperação, Validação do Regresso à Operação, Comunicações, Risco Residual e Ações Corretivas.

Consulte todos os cursos do percurso NIS2 aqui.

OBJETIVOS

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

1. identificar o enquadramento e as medidas de continuidade aplicáveis à entidade;
2. identificar serviços, funções ou atividades críticas, ativos TIC, partes interessadas e dependências relevantes;
3. realizar uma análise de impacto simplificada e definir prioridades, requisitos e objetivos de continuidade;
4. distinguir e relacionar MAO/MTPD, RTO, RPO e SDO com o contexto da entidade e os objetivos de recuperação;
5. estruturar os elementos essenciais dos Planos de Continuidade de Negócio e de Recuperação de Desastres;

6. definir os elementos essenciais da Política e dos Procedimentos de Cópias de Segurança, estabelecendo critérios de integridade, completude, disponibilidade, utilização, restauro e validação das cópias;
7. avaliar necessidades de redundância e capacidade de recuperação;
8. preparar verificações e testes de restauro, recuperação, failover, redundância e capacidade;
9. estruturar responsabilidades, autoridade, critérios de ativação e comunicação em situação de crise;
10. avaliar resultados, desvios risco residual, ações corretivas e necessidades de reteste;
11. definir critérios técnicos e funcionais para validar o regresso à operação;
12. organizar decisões, medidas, testes, resultados, comunicações e evidências no Toolkit.

PROGRAMA

SESSÃO 1 — Enquadrar, analisar impactos e definir requisitos de continuidade
Pergunta central: Que medidas de continuidade são aplicáveis à entidade e a que atividades?

- Enquadramento de medidas de continuidade aplicáveis
- Entidades Essenciais e Importantes e Entidades Públicas Relevantes
- Requisitos de resiliência dos serviços críticos
- Plano de Continuidade do Negócio
- Política de Recuperação de Desastres
- Política de Cópias de Segurança
- Medidas de Redundância e testes aos planos
- Critérios e Registos associados à Recuperação
- Medidas do Anexo IV aplicáveis às Entidades Públicas Relevantes

Exercício principal: quatro atividades disputam recursos limitados e dependem de ativos, serviços externos e fornecedores comuns. Os participantes têm de decidir o que é crítico, definir prioridades e objetivos de recuperação, identificar conflitos e iniciar os elementos do plano.
Outputs trabalhados: Análise de Impacto e Requisitos de Continuidade; Plano Integrado de Continuidade e Recuperação.
Exercício facultativo: mini-análise de impacto de uma atividade, processo ou serviço da entidade, ou do caso pedagógico, sem entrega obrigatória e sem integração na carga horária.

SESSÃO 2 — Preparar cópias de segurança, redundância e recuperação de desastres
Pergunta central: As cópias de segurança, os recursos e os procedimentos permitem recuperar dentro dos critérios definidos?

- Política e Procedimento de Cópias de segurança
- Esquema de Redundância
- Mecanismos de verificação e testes à integridade e disponibilidade
- Cópia executada vs Cópia íntegra vs Cópia utilizável vs Recuperação conseguida
- Opções técnicas adequadas ao risco e ao contexto
- Protação e acessibilidade dos planos e procedimentos

Exercício principal: existe uma cópia recente, mas surgem problemas de integridade, completude, configuração, chave de cifragem, capacidade, dependência do ambiente afetado, disponibilidade do fornecedor e ausência de teste recente. Os participantes têm de decidir se a cópia pode ser utilizada, definir verificações, critérios de sucesso, ações de regularização e evidências.
Outputs trabalhados: Política e Procedimento de Cópias de Segurança; Plano de Verificação, Restauro e Testes de Recuperação.
Exercício facultativo: análise da capacidade de recuperação de um sistema ou serviço, desde a cópia até ao restauro verificável, sem execução de testes reais obrigatórios.

SESSÃO 3 — Testar, gerir a crise, recuperar e validar o regresso à operação
Pergunta central: As medidas funcionam e existem condições para autorizar o regresso à operação?

- Passagem da preparação para a verificação das capacidades de continuidade e recuperação
- Periodicidade e gatilhos para teste, revisão e atualização
- Declaração de crise e ativação da recuperação
- Desativação da crise e declaração do fim da recuperação
- Equipa de gestão de crise, procedimentos de emergência e canais alternativos de comunicação
- Participação de fornecedores nos exercícios e testes
- Restaurar dados vs Recuperar Sistema vs Recuperar Seviço vs Recuperar Atividade vs Validar regresso à Operação

Exercício final integrador: um serviço crítico encontra-se parcialmente recuperado, os objetivos estão em risco, existe capacidade insuficiente, um fornecedor está atrasado, há operação degradada e o canal normal de comunicação falhou. Os participantes têm de decidir sobre crise, prioridades, recuperação, comunicações, risco residual, regresso à operação, ações corretivas e reteste.
Outputs trabalhados: Plano de Gestão de Crises e Comunicação; Registo de Ativação, Recuperação, Validação do Regresso à Operação, Comunicações, Risco Residual e Ações Corretivas.

METODOLOGIA

Metodologia
Cada sessão responde a uma pergunta operacional, integra um exercício principal e desenvolve um conjunto limitado de outputs do Toolkit Essencial NIS2 — Continuidade das Atividades.
Os casos são apresentados por vagas sucessivas de informação. Os participantes identificam factos, pressupostos e informação em falta, atualizam impactos e prioridades, fundamentam decisões, definem critérios de verificação e teste e organizam progressivamente a evidência.
A formação segue a assinatura pedagógica: APRESENTAR ? DEMONSTRAR ? PRATICAR ? DISCUTIR ? VERIFICAR ? CONSOLIDAR.
Nos casos de uso em que seja pedagogicamente adequado, o CYBERSECURE é utilizado como plataforma de apoio à realização dos exercícios e à organização da informação sobre atividades críticas, dependências, requisitos, responsabilidades, medidas, verificações, testes, resultados, ações de regularização, risco residual e

evidências. A utilização da plataforma é articulada com os artefactos editáveis do Toolkit e não substitui a análise, a decisão, a aprovação, a implementação, a verificação, o teste, a validação, a supervisão ou a responsabilidade das funções competentes.
Existem dois exercícios assíncronos facultativos, associados às sessões 1 e 2.. Os exercícios facultativos não integram a carga horária, não exigem entrega e não condicionam a avaliação ou certificação.
O Toolkit é trabalhado durante as sessões e disponibilizado em formato editável e reutilizável. A Documentação Pedagógica Complementar é disponibilizada como referência para aplicação posterior.
A avaliação é contínua e formativa.

FORMADORES

Henrique Necho

- Engenheiro e 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
- 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 Continuidade, Henrique Necho orienta os participantes na identificação de atividades críticas e dependências, na análise de impactos, na definição de requisitos e objetivos de recuperação, na preparação de planos, cópias de segurança, redundância e testes, na avaliação do risco residual e das ações corretivas, na gestão de crises e na validação técnica e funcional do regresso à operação.

DESTINATÁRIOS

A formação destina-se prioritariamente a profissionais com responsabilidades na continuidade das atividades, recuperação de desastres, cibersegurança, TIC, operações, infraestruturas, gestão dos riscos e gestão de crises, nomeadamente:

- Responsáveis de Cibersegurança e CISOs;
- CIOs e responsáveis de TIC;
- responsáveis de continuidade das atividades e recuperação de desastres;
- responsáveis de operações, infraestruturas, redes e sistemas;
- responsáveis de gestão dos riscos e gestão de crises;
- donos de serviços, funções ou atividades críticas;
- responsáveis por sistemas, aplicações, capacidade e disponibilidade;
- gestores de fornecedores críticos com impacto na continuidade;
- profissionais de Entidades Públicas Relevantes responsáveis por funções ou atividades críticas e pelos ativos TIC que as suportam;
- profissionais de segurança da informação, resposta a incidentes, auditoria, compliance, jurídico, proteção de dados e comunicação;
- consultores que apoiem continuidade, recuperação ou gestão de crises.

É especialmente adequado para quem participa na identificação de atividades críticas, análise de impactos, definição de requisitos e objetivos de recuperação, preparação de planos, acompanhamento de cópias de segurança, realização de verificações e testes, gestão de crises ou validação do regresso à operação.

Não é uma formação técnica aprofundada sobre plataformas ou tecnologias específicas de backup, replicação, disaster recovery ou alta disponibilidade.

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