ONLINE | Responsável de Cibersegurança

DATAS
18, 23 e 30 de abril, 7, 9 e 14 de maio de 2024

HORÁRIO
19:00 - 22:00

PREÇO
Associado AEP: **648€**
Outros: **720€**

10% desconto* grupo a partir de 3 inscrições
*não acumula com outros descontos

Poderá ser reembolsado do valor pago, mediante a aprovação da candidatura ao **Cheque-Formação + Digital - IEFP, I.P.**

LOCAL
Online

DURAÇÃO
28 horas:
 18 horas sincronas
 10 horas prática assíncrona

ENQUADRAMENTO

Este curso intensivo de "Responsável de Cibersegurança" foi especialmente preparado para os profissionais que procuram aprofundar os seus conhecimentos e competências na implementação e gestão de estratégias de cibersegurança eficazes, alinhadas com o Regime Jurídico da Segurança do Ciberespaço. Neste curso, também abordamos a nova Diretiva SRI 2, o NIST Cybersecurity Framework 2.0 e as práticas recomendadas pela norma ISO/IEC 27001:2022.

Destinado a uma ampla gama de profissionais, incluindo os já atuantes e os aspirantes a Responsáveis de Segurança, Responsáveis de Sistemas e Tecnologias de Informação, Consultores e Auditores IT e aos Encarregados da Proteção de Dados, o curso oferece uma base sólida para compreender as complexidades legais e técnicas da cibersegurança moderna.

Os participantes serão orientados através de um currículo abrangente que cobre a interpretação de legislação específica, a avaliação da maturidade da cibersegurança organizacional, a identificação e proteção de ativos críticos e a elaboração de políticas e planos de segurança detalhados s. Além disso, o curso realça a importância da gestão de riscos, a construção de políticas de gestão e notificação de incidentes e a preparação de relatórios anuais, todos alinhados com as exigências regulamentares e com as melhores práticas internacionais.

No final do curso, os formandos estarão equipados não apenas com o conhecimento teórico necessário, mas também com competências práticas para planear e implementar um programa de conformidade com o Regime Jurídico da Segurança do Ciberespaço, promovendo assim a resiliência organizacional e a confiança digital. Este curso representa uma oportunidade única para os profissionais se posicionarem na vanguarda da cibersegurança, prontos para enfrentar os desafios atuais e futuros no que concerne à proteção do ciberespaço.

OBJETIVOS

No final da ação, os formandos deverão ser capazes de:

- Interpretar corretamente os conceitos e requisitos do RJSC e legislação complementar (já com a nova Diretiva SRI 2)
- Auditar e identificar a maturidade da organização, em matéria de cibersegurança
- Inventariar e categorizar os ativos essenciais para a prestação dos serviços
- Realizar análise de riscos aos ativos de informação
- Identificar as medidas técnicas e organizativas adequadas para gerir os riscos, baseado na metodologia do QNRSC
- Elaborar uma Política de Segurança da Informação
- Elaborar o Plano de Cibersegurança da organização, em conformidade com o RJSC
- Construir uma Política e respetivos Procedimentos de Gestão de Incidentes
- Elaborar o Relatório Anual de Cibersegurança, em conformidade com o RJSC
- Desenhar um Plano de Ação para a conformidade regulatória da organização
- Elaborar os documentos e relatórios obrigatórios, instituídos nas Instruções Técnicas emanadas do CNCS
- Elaborar os elementos obrigatórios no âmbito do RJSC
- Adotar boas práticas em matéria de gestão da cibersegurança

PROGRAMA

Mód. 1 - Enquadramento Normativo do RJSC
. A interpretação adequada dos conceitos e requisitos do RJSC e do restante quadro normativo aplicável;
. Legislação e Regime Sancionatório:
- Lei n.º 46/2018, de 13 de agosto;
- Decreto-Lei n.º 65/2021, de 30 de julho;
- Regulamento n.º 183/2022, do CNCS;
- Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 (Diretive NIS 2);
- Aviso n.º 1517/2024, do CNCS.

. Linha Temporal de aplicação;
. Definições.

Mód. 2 -O "Responsável de Cibersegurança" e "Ponto de Contato Permanente"
. Conteúdo funcional e responsabilidades;
. O Ponto de Contato Permanente;
. O Responsável de Segurança;
. O caso particular do CISO. Casos de estudo.

Mód. 3 -Política de Segurança da Informação (PSI)
. Princípios orientadores da elaboração/atualização da PSI;
. Análise de modelo de PSI, alinhadas com a ISO/IEC 27001;

COMPONENTE PRÁTICA ASSÍNCRONA
. Exercício n.º 1 e 2 – Elementos da Designação de Funções
. Exercício n.º 3 - Elaboração de PSI adequada à entidade em análise

Esclarecimento de dúvidas; boas práticas.

Mód. 4 - Inventário de Ativos
. Abordagem à gestão dos ativos essenciais para a prestação dos serviços e dos equipamentos de rede;
. Abordagem à classificação de criticidade do ativo: alta, média e baixa;
. Abordagem aos diagramas de rede;

Mód. 5 - Análise de Risco
. A análise da gestão do risco no contexto do RJSC;
. Princípio da Análise de Riscos, em matérias de segurança da informação e cibersegurança;
. Quadros de ameaças, vulnerabilidades, impacto, probabilidade, classificação do nível de risco e matrizes de avaliação do risco (heatmaps);
. Estratégias, Controlos e Planos de Tratamento dos Riscos;
. Comunicação, Documentação, Risk Register, Monitorização e Revisão dos Riscos;
. Abordagem à Metodologia de Gestão do Risco proposta na ISO/IEC 27005 - Guidance on managing information security risks;

COMPONENTE PRÁTICA ASSÍNCRONA
. Exercício n.º 4.1 Elaboração de inventário de todos os ativos de informação em uso na entidade selecionada
. Exercício n.º 4.2 - Elaboração do diagrama de rede da entidade em análise
. Exercício n.º 5 – Elaboração da análise e gestão de risco, de ativos inventariados no exercício n.º 3.

Esclarecimento de dúvidas; debate orientado; boas práticas.

Mód. 6 – Medidas técnicas e organizativas
. Abordagem ao Quadro Nacional de Referência de Cibersegurança (QNRSC);
. Análise de medidas técnicas e organizativas adequadas para gerir os riscos; Exemplo de implementação de controlos;
. Abordagem aos níveis de maturidade dos controlos aplicados

Mód. 7 – Novas medidas de gestão dos riscos de cibersegurança (Diretive NIS 2 e NIST CSF 2.0)
. Abordagem às medidas de Gestão dos Riscos de Cibersegurança, estipuladas na Diretive NIS 2:
- Políticas de análise dos riscos e de segurança dos sistemas de informação;
- Tratamento de incidentes;
- Continuidade das atividades, a recuperação de desastres, e gestão de crises;
- Segurança da cadeia de abastecimento;
- Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação
- Políticas e procedimentos de gestão dos riscos de cibersegurança;
- Práticas básicas de ciber-higiene e formação em cibersegurança;
- Políticas e procedimentos relativos à utilização de criptografia;
- Segurança dos recursos humanos (controlo do acesso e gestão de ativos);
- Soluções de autenticação multifator ou de autenticação contínua.

. Abordagem à NIST CSF 2.0

COMPONENTE PRÁTICA ASSÍNCRONA
. Exercício n.º 6 – Elaborar plano de ação com (pelo menos) 5 controlos adequadas à organização em análise, alinhado com o QNRSC
. Exercício n.º 7 - Elaborar plano de ação com (pelo menos) 5 controlos adequadas à organização em análise, alinhado com a Directive NIS 2

Esclarecimento de dúvidas; boas práticas.

Mód. 8 - Plano de Cibersegurança
. Os requisitos do Plano de Cibersegurança;
. Análise de modelo;

Mód. 9 - Gestão de Incidentes de Cibersegurança
. O Ciclo de Vida do Incidente: as fases da gestão de incidentes de cibersegurança

. Taxonomia de classificação;
. Deteção dos incidentes de cibersegurança (percursores, indicadores);
. Abordagem à análise da perigosidade e do impacto do incidente na organização;
. Notificação de incidentes;
. Análise de modelo;

Mód. 10 – Relatório Anual de Cibersegurança
. Os requisitos do Relatório Anual para conformidade com o RJSC;
. Análise de modelo;

COMPONENTE PRÁTICA ASSÍNCRONA
. Exercício n.º 8 – Elaborar um Plano de Cibersegurança adequado à entidade em análise
. Exercício n.º 9 - Elaborar os elementos de notificação ao CNCS, de situação de ocorrência de um ataque de ransomware na entidade em análise.
. Exercício n.º 10 – Elaborar um Relatório Anual adequado à entidade em análise.

Esclarecimento de dúvidas; boas práticas.

Mód. 11 - Auditoria e Monitorização da Cibersegurança
. Responsabilidades do Responsável de Cibersegurança;
. Abordagem à auditoria de conformidade com o RJSC;
. Análise de estrutura típica de projeto de auditoria;
. Métricas de cibersegurança para monitorização e acompanhamento da cibersegurança
. Análise de modelos;

Mód. 12 – Plano de Ação para a conformidade com o RJSC
. Linha temporal de aplicação do regime jurídico;
. Análise de modelo de plano de ação, com 10 etapas, para conformidade com o RJSC;

Mód. 13 – A Nova Diretive NIS 2
. Apresentação da nova Diretive NIS 2 (ou Diretiva SRI 2), que **deverá ser transposta até 17 de outubro de 2024.**
. Apresentação do conjunto mais extenso e harmonizado de requisitos de cibersegurança para as organizações, designadamente, o reforço dos requisitos de segurança, a abordagem da segurança das cadeias de abastecimento, o agilizar das obrigações de informação e a introdução de medidas de supervisão e aplicação mais rigorosos, incluindo sanções harmonizadas em toda a UE. A nova Diretiva SRI2 abrange mais entidades e sectores

COMPONENTE PRÁTICA ASSÍNCRONA
. Exercício n.º 11 - Elaborar um Plano de Ação para conformidade com o RJSC.

Esclarecimento de dúvidas; boas práticas.

Mód. 14 – Apresentação dos Dossiers Finais
. Apresentação e avaliação dos trabalhos individuais.

Mód. 15 – Passos seguintes
. Tendências e desafios futuros da Cibersegurança.
. Apresentação do European Cybersecurity Skills Framework (ENISA).
. Recursos extra.

Esclarecimento de dúvidas; boas práticas.

METODOLOGIA

Será utilizada uma metodologia, expositiva, interrogativa e ativa, fomentadora da participação dos formandos.

Como entidade Formadora Certificada pela DGERT a AEP, no final do curso, vai emitir Certificados de Formação Profissional de acordo com a legislação em vigor. Para ter aprovação devem verificar-se cumulativamente as seguintes condições:

• assiduidade igual ou superior a 80% da carga horária total da ação (18 horas)
• aproveitamento igual ou superior a 50% no trabalho prático (Dossier Final)

Nos restantes casos é emitido um Certificado de Frequência.

FORMADORES

Henrique Necho
CISO/DPO, CISM, CISA, ISO 27001 LI, ISO 27005 RM, CIPP/E, CIPM, CIPT, MBA

- Profissional certificado na área da cibersegurança e da proteção de dados, com mais de 25 anos de atividade profissional desenvolvida na área dos Sistemas de Informação, tanto no sector privado como no público.
- Certificado CISM (Certified Information Security Manager) e CISA (Certified Information Security Auditor) pelo ISACA
- Certificado ISO/IEC 27001 Lead Implementer e ISO/IEC 27005 Risk Manager
- Fundador e diretor-executivo da "NECHO TECHLAW"

DESTINATÁRIOS

- Profissionais designados pela entidade patronal para o exercício das funções de Responsável de Segurança

- Profissionais que pretendam vir a exercer as funções de Responsável de Segurança

- Responsáveis de Sistemas e Tecnologias de Informação

- Consultores IT

- Auditores IT

- Encarregados da Proteção de Dados

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