ONLINE | Responsável de Cibersegurança Em campanha

DATAS
27 e 29 junho, 5, 6, 11 e 13 de julho 2023

HORÁRIO
19:00 - 22:00

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

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

LOCAL
Online

DURAÇÃO
18 horas

ENQUADRAMENTO

A Lei n.º 46/2018, de 13 de agosto, veio estabelecer o Regime Jurídico da Segurança do Ciberespaço (RJSC), transpondo a Diretiva (UE) 2016/1148 (Diretiva SRI), do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União Europeia.

O RJSC aplica-se às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação.

O Decreto-Lei n.º 65/2021, de 30 de julho, veio regulamentar o RJSC e prevê obrigações relativas a vários aspetos centrais, designadamente:

• Estabelece os requisitos mínimos de segurança das redes e dos sistemas de informação que devem ser cumpridos
• Estabelece os requisitos de notificação obrigatória de incidentes que afetem a segurança das redes e dos sistemas de informação
• Estabelece a obrigação de designar e comunicar ao Centro Nacional de Cibersegurança (CNCS) o respetivo Responsável de Segurança.

O Responsável de Segurança tem como função “a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes” (nos termos do RJSC e do Decreto-Lei n.º 65/2021, de 30 de julho).

Mais concretamente, a função do Responsável de Segurança está descrita no Quadro Nacional de Referência para a Cibersegurança, publicado pelo CNCS em 2019 (na altura era é designada por CISO - Chief Information Security Officer) e inclui, designadamente, as seguintes responsabilidades:

• Garantir a segurança da informação da organização;
• Deve reportar à gestão de topo;
• Deve ter conhecimento pleno dos processos chave da organização;
• Deve ser capaz de traduzir os objetivos da organização em requisitos de segurança da informação.

Entretanto, entrou em vigor a 16 de janeiro de 2023 a nova Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 (Diretiva SRI 2) que vem revogar a atual Diretiva SRI e estabelecer um conjunto mais extenso 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 SRI 2 abrange mais entidades e sectores. Os Estados-Membros devem agora transpor os novos requisitos para a legislação nacional e aplicá-los a partir de 18 de outubro de 2024.

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 o Plano de (Ciber)Segurança da organização, em conformidade com o RJSC

- Construir uma Política e respetivos Procedimentos de Gestão de (Ciber)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

Módulo 01 : Enquadramento Normativo do RJSC (1h)
- A interpretação adequada dos conceitos e requisitos do RJSC e do restante quadro normativo aplicável;
- Legislação e Regime Sancionatório.

Módulo 02 : O “Responsável de Segurança” e “Ponto de Contato Permanente” (0.5h)
- Conteúdo funcional e responsabilidades;
- Exercício n.º 1.

Módulo 03 : Política de Segurança da Informação (PSI) (1.5h)
- Segurança Informática e Ciberhigiene;
- Princípios orientadores da elaboração/atualização da PSI;
- Análise de modelos de PSI, alinhados com a ISO/IEC 27001;
- Exercício n.º 2.

Módulo 04 : Inventariação de ativos (1h)
- Abordagem à gestão dos Ativos (essenciais) e dos Equipamentos de Rede;
- Abordagem à classificação de criticidade do Ativo: alta, média e baixa;
- Abordagem aos diagramas de rede;
- Exercício n.º 3 e n.º 4.

Módulo 05 : Análise de Risco (2h)
- A análise de risco e requisitos de segurança;
- Quadros de ameaças, vulnerabilidades, impacto, probabilidade, classificação do risco e matrizes de avaliação do risco (heat maps);
- Tolerância ao Risco, Estratégias de Mitigação e Registo de Riscos;
- Metodologia de Gestão do Risco proposta na ISO/IEC 27005:2022 - Guidance on managing information security risks;
- Exercício n.º 5.

Módulo 06 : Medidas técnicas e organizativas (2h)
- Abordagem ao Quadro Nacional de Referência de Cibersegurança (QNRSC);
- Análise de medidas técnicas e organizativas adequadas para gerir os riscos;
- Exercício n.º 6.

Módulo 07 : Plano de (Ciber)Segurança (1h)
- Os requisitos do Plano de (Ciber)Segurança;
- Análise de modelo;
• Exercício n.º 7.

Módulo 08 : Gestão de Incidentes de Cibersegurança (2h)
- O Ciclo de Vida do Incidente: as fases da gestão de incidentes de cibersegurança
- Taxonomia;
- Deteção dos incidentes de cibersegurança, a análise da perigosidade e do impacto na organização;
- Notificação de incidentes;
- Análise de modelo;
- Exercício n.º 8.

Módulo 09 : Auditoria e Monitorização da Cibersegurança (1h)
- Responsabilidades do Responsável de (Ciber)Segurança;
- Abordagem à auditoria de cibersegurança: a estrutura típica do plano de auditoria
- Análise de modelo;
- Métricas de cibersegurança para monitorização e acompanhamento.

Módulo 10 : Relatório Anual de Cibersegurança (1h)
- Os requisitos do Relatório Anual para conformidade com o RJSC;
- Análise de modelo;
- Exercício n.º 9.

Módulo 11 : Plano de Ação para a conformidade com o RJSC (1h)
- Linha temporal de aplicação do regime jurídico;
- Análise de modelo de plano de ação, com 9 etapas, para a conformidade com o RJSC;

- Exercício n.º 10.

Módulo 12: A nova Diretiva NIS 2 (1h)
- Apresentação da nova Diretiva SRI2, que entrou em vigor a 16 de janeiro de 2023.
- 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.
- Os Estados-Membros devem agora transpor os requisitos da Diretiva SRI2 para a legislação nacional, publicar as medidas necessárias para cumprir com este instrumento jurídico e aplicá-las a partir de 18 de outubro de 2024.

Módulo 13 : Apresentação dos Dossiers Finais (2.5h)
- Apresentação dos exercícios n.º1 a n.º10, constituintes do Dossier Final, e respetiva avaliação.

Módulo 14 : Passos seguintes (0.5h)
- Tendências e desafios futuros.

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

- 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
- Technical Expert do European Privacy Seal certification
- Fundador e diretor-executivo da "NECHO TECHLAW"

Maria José Lima

- Jurista, com mais de 20 anos de atividade profissional
- Especialista em direito da cibersegurança

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