6 – "Cibersegurança na Administração Pública"

- **REAGENDADO:** 10/11, 11/11, 17/11, 19/11 e 03/12/2026 (3.ª feira, 4.ª feira, 3ª feira, 5.ª feira e 5.ª feira) – 28 horas

Vagas a atribuir a cada departamento do Governo Regional:

ENTIDADE	N.º DE VAGAS
ASSEMBLEIA LEGISLATIVA REGIONAL	1
SECRETARIA REGIONAL DAS FINANÇAS	3
SECRETARIA REGIONAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA	4
SECRETARIA REGIONAL DE TURISMO, AMBIENTE E CULTURA	2
SECRETARIA REGIONAL DE ECONOMIA	1
SECRETARIA REGIONAL DE SAÚDE E PROTEÇÃO CIVIL	1
SECRETARIA REGIONAL DE AGRICULTURA E PESCAS	2
SECRETARIA REGIONAL DE INCLUSÃO, TRABALHO E JUVENTUDE	2
SECRETARIA REGIONAL DE EQUIPAMENTOS E INFRAESTRUTURAS	3

Objetivos:
- Desenvolver competências para identificar e prevenir ameaças digitais, proteger dados, identidades, dispositivos e redes e aplicar boas práticas de cibersegurança, gestão de incidentes, risco e continuidade na Administração Pública.

Pré-Requisitos (Formandos):

- Conhecimentos básicos de informática e utilização regular de computadores e Internet

Os Fundos Europeus mais próximos de si.

Destinatários:[1]
- Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)

Formador(a):
- Vitorino Gouveia

Responsável pela Coordenação Científica:
- Tânia Vieira

Responsável pela Coordenação Pedagógica:
- Natacha Taboada

Modalidade e Organização da Formação:
- Contínua e presencial

N.º de Formandos:
- 20

Carga Horária:
- 28 horas (4 dias)

Horário:
Dias 10/11, 17/11 e 19/11 – 09h30-13h00/14h00-17h30
Dia 11/11 – 14h00-17h30
Dia 03/12 – 09h30-13h00

Local:
- Centro de Inovação e Competências Digitais (CICD) – **SALA 2**

Rua Alferes Veiga Pestana n.º 12, 9054-505, Santa Luzia – Funchal

[1] Em conformidade com a Portaria nº 782/2009, de 23 de julho, que regula o Quadro Nacional de Qualificações e define os descritores para os níveis de qualificação nacionais.

Programa Detalhado:

1 - Conceitos fundamentais de cibersegurança e segurança da informação: terminologia, enquadramento e evolução da ameaça digital.

2 - Enquadramento estratégico e legal: Estratégia Nacional de Segurança do Ciberespaço, Centro Nacional de Cibersegurança (CNCS), RGPD e Diretiva NIS2.

3 - Princípios da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade.

4 - Panorama de ameaças: *malware* (vírus, *ransomware, spyware, worms*) e engenharia social (*phishing, spear phishing, smishing, vishing*).

5 - Gestão de identidade e acesso: palavras-passe robustas, autenticação multifator (MFA) e princípio do menor privilégio.

6 - Segurança no correio eletrónico e na navegação na Internet: deteção de fraude, sites maliciosos e ligações comprometidas.

7 - Segurança de dispositivos: computadores, dispositivos móveis, suportes amovíveis e teletrabalho.

8 - Segurança de redes: redes internas, Wi-Fi, VPN e acesso remoto seguro.

9 - Proteção de dados pessoais e de informação classificada, em conformidade com o RGPD.

10 - Segurança na utilização de serviços *cloud*, ferramentas colaborativas e Inteligência Artificial.

11 - Políticas de segurança da informação, classificação da informação e gestão de acessos e permissões.

12 - Gestão de incidentes de cibersegurança: identificação, reporte, resposta e articulação com o CNCS/CERT.PT.

13 - Continuidade de negócio, planos de recuperação e gestão de risco em cibersegurança.

14 - Governação da cibersegurança: o papel de dirigentes, chefias e colaboradores na proteção da informação.

15 - Cultura organizacional de cibersegurança: sensibilização, formação contínua e boas práticas na proteção dos ativos digitais.

16 - Estudos de caso reais (incluindo incidentes em entidades públicas) e exercícios práticos de identificação de ameaças e vulnerabilidades.