



REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública



Cofinanciado pela
União Europeia

Os Fundos Europeus mais próximos de si.

6 – “Cibersegurança na Administração Pública”

- 10/11 e 11/11, 17/11 e 19/11/2026 (3.ª feira e 4.ª feira, 3ª 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



Avenida Zarco, Palácio do Governo Regional, 3.º andar, 9004-527 Funchal • Telf. (+351) 291 145 150

www.madeira.gov.pt/drap • drap@madeira.gov.pt



Entidade Formadora Certificada
ÁREAS DE EDUCAÇÃO E FORMAÇÃO:
Portaria n.º 254/2005 de 16 de Março
090, 322, 344, 345, 346, 380, 482, 862.



REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública



**Cofinanciado pela
União Europeia**

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 Seixas

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:

- 7 horas/dia – 09:30/13:00 e 14:00/17:30

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 n.º 782/2009, de 23 de julho, que regula o Quadro Nacional de Qualificações e define os descritores para os níveis de qualificação nacionais.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública



Cofinanciado pela
União Europeia

Os Fundos Europeus mais próximos de si.

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 - Governança 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.

