DIÁRIO DA REPÚBLICA

2.ª série
N.º 124
30-06-2026

CULTURA, JUVENTUDE E DESPORTO

Instituto Português do Desporto e Juventude, IP

Aviso (extrato) n.º 16283/2026/2

Sumário: Abertura de procedimento concursal para um posto de trabalho da carreira especial de especialista de sistemas e tecnologias de informação, para exercício da função de Chief Information Security Officer (CISO).

Procedimento concursal comum, para preenchimento de 1 (um) posto de trabalho da carreira especial de Especialista de Sistemas e Tecnologias de Informação do mapa de pessoal do Instituto Português do Desporto e Juventude, I. P. para exercício de funções na Divisão de Infraestruturas Tecnológicas

Nos termos do disposto no artigo 33.º da Lei Geral do Trabalho em Funções Públicas, aprovada pela Lei n.º 35/2014, de 20 de junho, na redação atual e no n.º 4 do artigo 11.º da Portaria n.º 233/2022, de 9 de setembro, torna-se público que se encontra aberto o procedimento concursal em epígrafe, nos seguintes termos:

1 — Entidade que realiza o procedimento: Instituto Português do Desporto e Juventude, I. P.

2 — Local de trabalho: Rua Rodrigo da Fonseca, n.º 55, 1250-190 Lisboa

3 — Número de postos de trabalho: 1 (um)

4 — Carreira/categoria: Especialista de Sistemas e Tecnologias de Informação

5 — Remuneração: Remuneração de origem ou superior, se aplicável

6 — Caracterização do posto de trabalho:

Estratégia e Governação da Segurança da Informação:

Desenvolver e implementar a estratégia global de segurança da informação do IPDJ;

Definir políticas, normas, procedimentos e controlos de segurança alinhados com boas práticas (ISO/IEC 27001, ENS, NIST, etc.);

Coordenar o SGSI — Sistema de Gestão de Segurança da Informação;

Assegurar conformidade com legislação relevante, incluindo RGPD, Lei do Cibercrime, NIS2 e regulamentos nacionais.

Gestão de Risco e Continuidade de Negócio:

Realizar avaliações regulares de risco tecnológico e operacional;

Analisar vulnerabilidades e priorizar ações de mitigação;

Desenvolver e manter planos de continuidade de negócio e recuperação de desastre (BCP/DRP). Monitorização e Incidentes de Segurança

Liderar o processo de identificação, resposta e reporte a incidentes de segurança:

Coordenar com entidades externas relevantes (CNCS, operadores TIC, parceiros);

Supervisionar sistemas de monitorização, deteção e prevenção (SIEM, EDR, firewalls, etc.). Formação e Cultura de Segurança:

Promover ações de sensibilização para colaboradores e parceiros;

Criar programas de formação contínua em boas práticas de cibersegurança. Gestão de Projetos e Conformidade Tecnológica:

Acompanhar projetos de transformação digital para garantir que incorporam requisitos de segurança;

Avaliar fornecedores e soluções tecnológicas sob critérios de risco, privacidade e segurança.

7 — Certificações específicas/outros requisitos:

Certificações Técnicas (fortemente valorizadas):

CISSP (Certified Information Systems Security Professional)

CISM (Certified Information Security Manager)

CEH (Certified Ethical Hacker)

ISO/IEC 27001 Lead Implementer ou Lead Auditor

CompTIA Security+, CySA+, CASP+

Certificação em gestão de risco ou resposta a incidentes Competências Técnicas Obrigatórias:

Conhecimento profundo de cibersegurança, redes, arquitetura de sistemas e modelos Cloud.

Experiência com ferramentas de proteção: firewalls, antivírus corporativo, SIEM, IDS/IPS, EDR, MFA, DLP.

Domínio de metodologias de gestão de risco (ISO 27005, NIST RMF).

Conhecimento de RGPD e legislação aplicável a organismos públicos. O/A Candidato/a deverá possuir:

Capacidade de liderança e coordenação multidisciplinar.

Comunicação clara e eficaz com equipas técnicas e direção superior.

Tomada de decisão baseada em risco.

Espírito de missão e elevado sentido de responsabilidade.

Capacidade de gerir crises e atuar em situações de pressão. Valoriza-se ainda:

Experiência mínima de 3 anos em funções de segurança da informação, auditoria, gestão de risco ou administração de sistemas com forte enfoque em segurança.

Experiência prévia em organismos públicos.

Disponibilidade para formação contínua e interação com entidades reguladoras.

8 — Requisitos de admissão:

8.1 — Podem ser admitidos ao presente procedimento concursal trabalhadores com vínculo de emprego público por tempo indeterminado, previamente constituído, que cumpram os requisitos de admissão constantes do aviso integral publicado na BEP.

8.2 — Habilitações Académicas: Licenciatura na área da Engenharia Informática, Ciências da Computação, Cibersegurança, Tecnologias de Informação, ou áreas afins, sem possibilidade de substituição do nível habilitacional por formação e, ou, experiência profissionais

8.3 — Não são admitidos ao procedimento candidatos titulares de licenciatura ou grau superior em áreas académicas distintas da área a concurso.

8.4 — Os candidatos com certificados comprovativos da posse de habilitações literárias obtidas em país estrangeiro, deverão, sob pena de exclusão, apresentar documento comprovativo da obten-

Aviso (extrato) n.º 16283/2026/2

ção de reconhecimento das habilitações em território nacional, em conformidade com o disposto no Decreto-Lei n.º 66/2018, de 16 de agosto, e na Portaria 33/2019, de 25 de janeiro.

8.5 — Os candidatos devem reunir os requisitos até à data-limite de apresentação das candidaturas.

9 — Prazo de candidatura: 10 dias úteis a contar do dia seguinte ao da publicação integral do Aviso do procedimento na Bolsa de Emprego Público (BEP)

10 — Publicação integral: A publicação integral do procedimento pode ser consultada na BEP, em www.bep.gov.pt e no Portal do IPDJ, IP, em https://ipdj.gov.pt/documentos-de-recursos-humanos

8 de junho de 2026. — A Vogal do Conselho Diretivo, Lídia Praça.

320016231