RECRUTAMENTO EXTERNO

Empresa	**EPAL – Empresa Portuguesa das Águas Livres, SA**	Local:	**Parque das Nações**
Direção:	**Direção de Sistemas de Informação e Transformação Digital**	Data de Publicação:	**10/09/2026**
Função:	**Licenciado/a A de sistemas e tecnologias de informação** Responsável pela equipa de cibersegurança	Data de Fecho:	**24/09/2026**

Objetivos da Função

Integrado(a) na Direção de Sistemas de Informação e Transformação Digital (DSI), reportando ao Diretor de Sistemas de Informação, assegura a definição, implementação e evolução da arquitetura e dos controlos de CiberSegurança em ambientes IT, contribuindo para a proteção, deteção, resposta e recuperação face a ameaças cibernéticas.
A função inclui a coordenação da equipa interna de CiberSegurança, a interface com o Centro Nacional de CiberSegurança e a gestão da postura de segurança, monitorização contínua, conformidade, gestão de vulnerabilidades e resposta a ameaças em infraestruturas críticas.

Principais Tarefas e Responsabilidades

- Implementar e manter o sistema de gestão ISO 27001 e Quadro Nacional de Referência de CiberSegurança
- Administrar e evoluir soluções de CiberSegurança para ambientes IT, incluindo firewalls, VPN, NAC, IDS/IPS e plataformas de proteção industrial;
- Implementar e gerir plataformas de gestão de identidades e acessos (IAM), autenticação multifator (MFA), Single Sign-On (SSO) e gestão de acessos privilegiados (PAM);
- Operar ferramentas de monitorização e deteção de ameaças, incluindo SIEM, SOAR, EDR/XDR e soluções de Network Detection & Response (NDR);
- Coordenar processos de gestão de vulnerabilidades, avaliação de risco, análise de exposição e remediação de falhas de segurança;
- Definir e implementar medidas de hardening de sistemas, servidores, bases de dados, aplicações e equipamentos de rede;
- Garantir a conformidade com referenciais e normas de segurança como IEC 62443, ISO 27001, NIS2, CIS Controls e Purdue Model;
- Participar na definição e implementação da arquitetura de segmentação IT/OT, zonas de segurança e conduits industriais;
- Apoiar a proteção de infraestruturas críticas, plataformas SCADA, sistemas de automação, PLC, DCS e redes industriais;
- Implementar e validar estratégias de ciber-resiliência, incluindo backups imutáveis, recuperação de desastre, continuidade do negócio e recuperação após ciberataques;
- Monitorizar eventos de segurança, investigar incidentes, realizar análise forense preliminar e coordenar ações de resposta e contenção;
- Elaborar e manter documentação de segurança, análise de riscos, arquitetura de referência, inventários de ativos e procedimentos operacionais;

- Participar em auditorias de segurança, testes de intrusão, exercícios de Red Team/Blue Team e avaliações de maturidade;
- Colaborar em projetos de transformação digital, cloud, modernização tecnológica e convergência IT/OT, assegurando a integração dos requisitos de segurança desde a conceção (Security by Design);
- Analisar ameaças emergentes, identificar causas raiz de incidentes e propor medidas corretivas e preventivas para aumento da resiliência cibernética;
- Participar em projetos de implementação da IEC 62443, NIS2, Critical Entities Resilience (CER) e modelos de arquitetura Purdue.

.

Perfil Pretendido

- Nível académico mínimo equivalente a **licenciatura** em área relevante (preferência por Licenciatura Bolonha ou Mestrados pós Bolonha);
- **Qualificações académicas:** Engenharia Informática, Engenharia de Redes e Sistemas, CiberSegurança, Segurança da Informação ou área equivalente;
- Experiência e conhecimentos em arquitetura, implementação e evolução de controlos de CiberSegurança em ambientes IT;
- Conhecimentos em gestão da postura de segurança, monitorização contínua, resposta a ameaças, gestão de vulnerabilidades, hardening e conformidade;
- Experiência na administração de plataformas de CiberSegurança, incluindo IAM, PAM, SIEM, EDR/XDR, NGFW e NAC;
- Capacidade de produção e manutenção de políticas, normas, procedimentos e documentação de arquitetura de segurança;
- Valorizam-se certificações, participação em projetos ou disponibilidade para formação intensiva, a assegurar pela EPAL, nas seguintes áreas ou áreas correlacionadas com a função: CISSP, CISM, ISO 27001, GICSP, IEC 62443 Cybersecurity Specialist, Fortinet NSE/FCX, Palo Alto PCNSA/PCNSE, Cisco CyberOps ou CCNP Security e CCSA – Check Point Certified Security Administrator.

Observações

A presente oferta corresponde ao escalão de entrada da categoria de **Licenciado A de sistemas e tecnologias de informação**, à qual corresponde a remuneração base mensal de **€ 1,862.6** (14 meses) nos termos da tabela salarial em vigor no Acordo de Empresa da EPAL, acrescida dos subsídios e demais componentes aplicáveis à função. O enquadramento remuneratório está sujeito às disposições da Lei do Orçamento do Estado e demais legislação aplicável às Empresas do Grupo AdP.

Envie-nos a sua candidatura, acompanhada de Curriculum Vitae detalhado (em português), para **candidaturas.epal@epal.pt** com a seguinte referência indicada no assunto: **LIC-DSI-NIS**

– Só serão consideradas as candidaturas que reúnam o perfil solicitado.
Temos como referência a igualdade de oportunidades, pelo que acolhemos e valorizamos todas as pessoas, independentemente da raça, etnia, nacionalidade, religião, convicções políticas e ideológicas, idade, estado de saúde, género, identidade ou orientação sexual, visando, inclusive, a promoção da diversidade de pensamento e de experiências numa verdadeira cultura de inclusão e de representatividade e fortalecendo o sentido de pertença de cada pessoa que integre o Grupo AdP.