Especialista (Centro de Operações de Segurança) | 1 posto de trabalho | Departamento de Serviços de Suporte Tecnológico

Departamento: Departamento de Serviços de Suporte Tecnológico

Carreira: Especialista

Posição Remuneratória: 5.ª posição (3.770,00 €)

Área de atividade do posto de trabalho: Segurança da Informação

Subárea de atividade do posto de trabalho: Centro de Operações de Segurança

Área(s) de formação académica e/ou profissional: Informática

Titularidade de licenciatura e/ou de grau académico superior a esta (preferencialmente na área) – anexar certificado.

Os candidatos possuidores de habilitações literárias obtidas em país estrangeiro deverão apresentar, no ato da candidatura, sob pena de exclusão, documento comprovativo do reconhecimento das suas habilitações por entidade portuguesa competente para esse efeito, de acordo com a legislação portuguesa aplicável em vigor.

Outros requisitos de admissão:

Formação complementar específica na área – anexar certificado;

Pelo menos 4 anos na coordenação de atividades, equipas ou projetos especialmente relevantes para as funções a desempenhar;

Experiência profissional igual ou superior a 8 anos na respetiva área de atuação.

N.º de postos de trabalho a preencher: 1 (Um)

Conteúdo funcional associado ao posto de trabalho (atentas as competências da unidade orgânica):

- Liderar a estratégia, operação e evolução do Centro de Operações de Segurança (SOC), assegurando a sua eficácia operacional e alinhamento com os objetivos da organização;
- Definir e implementar o modelo de governação, processos, procedimentos e indicadores de desempenho do SOC;
- Coordenar equipas de cibersegurança, promovendo o desenvolvimento de competências e a adoção de boas práticas operacionais;
- Supervisionar a gestão, deteção e resposta a incidentes de segurança, assegurando o cumprimento dos níveis de serviço estabelecidos;
- Definir e acompanhar métricas, indicadores de risco e relatórios executivos sobre o estado da segurança e a atividade do SOC;

- Liderar a evolução tecnológica do SOC, incluindo plataformas SIEM, SOAR, EDR/XDR, *Threat Intelligence* e capacidades de *Threat Hunting*;
- Garantir a integração das operações do SOC com os processos de gestão de risco, continuidade de negócio e resposta a incidentes;
- Assegurar a conformidade com os normativos, requisitos regulamentares e referenciais de cibersegurança aplicáveis;
- Promover iniciativas de melhoria contínua, automação e otimização dos processos de monitorização e resposta a ameaças;
- Representar o SOC junto da gestão de topo, entidades externas, fornecedores e organismos de cibersegurança.

Conhecimentos específicos:

- Gestão e operação de Security Operations Centers (SOC);
- Deteção, análise e resposta a incidentes de cibersegurança;
- Threat Intelligence, Threat Hunting e gestão de ameaças avançadas;
- Plataformas SIEM, SOAR, EDR/XDR e Security Analytics;
- Frameworks e referenciais de cibersegurança (NIST CSF, MITRE ATT&CK, CIS Controls, ISO/IEC 27001);
- Monitorização de eventos de segurança e análise forense digital;
- Definição e acompanhamento de indicadores e métricas de segurança;
- Gestão de crises e coordenação de resposta a incidentes de elevada criticidade;
- Requisitos normativos e regulamentares aplicáveis, incluindo NIS2, RGPD e demais legislação relevante;
- Definição de estratégias de proteção, deteção e resposta a ciberameaças;
- Governação de cibersegurança e integração com modelos de gestão de risco organizacional.

Horário de trabalho: 40h semanais (em horário de plataformas flexíveis) com possibilidade de teletrabalho, de acordo com o Regulamento em vigor.

Instrução da candidatura:

As candidaturas devem ser submetidas através do Portal de Recrutamento do IGFEJ, I.P. - https://recrutamento.igfej.justica.gov.pt, devendo ser acompanhadas de:

I. Currículo profissional detalhado e atualizado, datado e assinado, devendo, dele, constar para além de outros elementos julgados necessários, as habilitações literárias, a experiência profissional, designadamente as funções e atividades que exerce e exerceu, com a indicação dos respetivos períodos de duração e atividade relevante, assim como a formação profissional detida em matéria relacionada com a área funcional do posto de trabalho em referência, bem como a indicação expressa das entidades promotoras, datas de realização e respetiva duração;

II. Cópia legível do certificado de habilitações literárias;
III. Cópias legíveis dos comprovativos das ações de formação frequentadas relacionadas ou relevantes para o desempenho de funções do posto de trabalho a ocupar;
IV. Eventual documentação considerada pertinente para a instrução da candidatura.

Local de trabalho: Campus da Justiça - Av. D. João II, 1.08.01 Bloco H, Lisboa