

Processo seletivo

SUPERVISOR DE SEGURANÇA CIBERNÉTICA

COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO (Assistente técnico II)

INFORMAÇÕES

Cargo: Comissionado

Regime de contratação: Estatutário

Carga horária: 40 horas semanais

Modalidade: Híbrido (3x por semana)

Horário: a combinar

Local: Rua Boa Vista, 200, Centro, São Paulo – SP

VENCIMENTOS

Salário base: R\$ 9.619,79

Gratificação de Representação: R\$ 932,22

Vale Transporte: R\$ 18,80 por dia trabalhado

Auxílio Alimentação: R\$ 66,00

OUTROS DIREITOS E BENEFÍCIOS

- 13º salário
- Férias
- Auxílio Saúde
- Adicional de Qualificação
- Bonificação de Resultados
- IAMSPE - Instituto de Assistência Médica ao Servidor Público Estadual
- Programas: Pró-Hardware, Pró-Software e Pró-Livro
- Convênios: Sesc (Matrícula de Interesse Social) e UNISA (Atendimento Psiquiátrico)

SOBRE A DEFENSORIA

A Defensoria Pública do Estado de São Paulo é uma instituição permanente cuja função, como expressão e instrumento do regime democrático, é oferecer, às pessoas necessitadas, de forma integral e gratuita, a orientação jurídica, a promoção dos direitos humanos e a defesa, em todos os graus, judicial e extrajudicial, dos direitos individuais e coletivos. A Constituição Federal a prevê como órgão de função essencial à Justiça e no Estado de São Paulo foi criada pela Lei Complementar Estadual nº 988 de 9 de janeiro de 2006.

A Defensoria Pública, apesar de ser uma instituição estadual, não é vinculada ao governo. Sua autonomia é prevista pela Constituição Federal e é uma garantia para que Defensoras e Defensores Públicos possam representar os direitos da população sem qualquer tipo de constrangimento. Internamente, cada membro da Defensoria possui independência funcional para seguir livremente sua convicção, em cada caso em que atua.

Atualmente, há 827 Defensoras e Defensores Públicos no Estado de São Paulo, que trabalham em 66 unidades espalhadas por 44 cidades. Processos de parte dos municípios que integram as mesmas comarcas também são atendidos, nas áreas de execução penal e de medidas socioeducativas.

A administração superior da instituição é conduzida pela Defensoria Pública-Geral – órgão dirigido por um Defensor ou Defensora nomeado/a pelo/a Governador/a, a partir de uma lista tríplice formada pelas pessoas que obtiverem mais votos em eleição com participação de toda a carreira.

DESCRIÇÃO DO CARGO

Supervisionar a área de Segurança da Informação (Cyber Segurança e Data Protection), planejando e monitorando as atividades técnicas e operacionais, liderando equipes de trabalho, abrangendo profissionais diretamente subordinados e prestadores de serviços. Garantindo a continuidade operacional dos recursos de Tecnologia da Informação.

Tarefas e responsabilidades:

- Supervisionar a implementação e manutenção de controles, soluções/tecnologias e processos de segurança cibernética;
- Supervisionar, desenvolver e testar recursos de proteção de dados (backup, restore e DR);
- Monitorar e analisar incidentes e violações de segurança, coordenando atividades de resposta a incidentes e conduzindo análises pós-incidentes para identificar lições aprendidas e melhorar as capacidades de resposta;
- Revisar e validar os resultados de Pentest, SOC, Resposta a Incidentes (IR), Inteligência de Ameaças e outras atividades de segurança.
- Projetar, desenvolver e testar recursos de segurança cibernética em nuvem privada e pública;
- Alinhar, melhorar e implementar estratégias, políticas e procedimentos de segurança da informação para proteger nossos ativos de dados e mitigar os riscos de segurança cibernética;
- Fornecer métricas e artefatos que apoiam atividades de auditoria;
- Liderar equipes de trabalho.

REQUISITOS PARA O CARGO

- Superior completo em Engenharia da Computação, Ciência da Computação, Análise de Sistemas, Tecnologia da Informação, Segurança da Informação e áreas afins;
- Pós-graduação na área de Segurança da Informação, Segurança Cibernética ou áreas correlatas;
- 3 (três) anos de experiência em segurança cibernética, auditoria de TI ou função de gerenciamento de riscos corporativos;
- Certificação técnica FORTINET NSE4 ou NSE5;
- Conhecimento em Cloud Security, Firewalls e IDS/IPS, WAF e segurança do ambiente de TI.

Certificações/Cursos Específicos Desejáveis:

- Conhecimento em solução Veeam de Proteção de Dados;
- Diferencial ter CISSP;
- Diferencial ter ITIL.

CARACTERÍSTICA DO PROFISSIONAL

- Dinâmico e proativo no comprometimento com a missão institucional;
- Bom relacionamento interpessoal;
- Trabalho em equipe;
- Habilidade de compreensão de texto e boa escrita

INFORMAÇÕES PARA CANDIDATURA

Candidatos/as interessados/as devem se inscrever até o dia 19 de julho de 2024 através do link:

<https://forms.gle/ptPAEj8qBysEuhYB8>

- Após o prazo de inscrição, iniciaremos a fase de triagem dos inscritos, a qual terá a duração de 10 dias úteis.
- Em caso de dúvidas, encaminhar mensagens para o e-mail selecao@defensoria.sp.def.br
- Currículos não serão aceitos por e-mail.