



Um **Engenheiro de Segurança** é um profissional responsável por projetar, implementar e gerenciar sistemas e políticas de segurança, protegendo informações, infraestrutura e ativos organizacionais contra ameaças e vulnerabilidades. Ele atua como um guardião técnico da segurança da informação, com foco em prevenção, detecção e resposta a incidentes.

Principais Funções e Responsabilidades

1. **Análise de Riscos e Vulnerabilidades**
  - Realizar auditorias de segurança.
  - Identificar riscos e vulnerabilidades em redes, sistemas e aplicativos.
  - Recomendar e implementar medidas corretivas.
2. **Desenvolvimento de Políticas e Protocolos**
  - Criar e manter políticas de segurança alinhadas aos requisitos organizacionais e normativos.
  - Estabelecer controles de acesso e diretrizes para o uso de recursos de TI.
3. **Monitoramento e Detecção de Ameaças**
  - Implementar e gerenciar sistemas de monitoramento, como SIEM [Security Information and Event Management].
  - Analisar logs e eventos em busca de atividades suspeitas.
4. **Implementação de Tecnologias de Segurança**
  - Configurar firewalls, sistemas de detecção de intrusões [IDS/IPS], antivírus e VPNs.
  - Garantir a aplicação de patches e atualizações em sistemas e softwares.
5. **Gestão de Incidentes**
  - Responder rapidamente a incidentes de segurança.
  - Conduzir análises forenses em caso de violações.
  - Propor melhorias para evitar recorrências.
6. **Educação e Conscientização**
  - Treinar colaboradores em práticas seguras de TI.
  - Promover uma cultura de segurança dentro da organização.

Competências e Habilidades Necessárias

- **Técnicas:**
  - Proficiência em ferramentas e tecnologias como firewalls, IDS/IPS, criptografia, e sistemas de gerenciamento de vulnerabilidades.
  - Conhecimento em linguagens de programação e scripting [Python, Bash, etc.].
  - Experiência com arquiteturas de redes, sistemas operacionais [Linux, Windows] e nuvem [AWS, Azure, GCP].
- **Gerenciais:**
  - Habilidades de gerenciamento de riscos.
  - Capacidade de elaborar relatórios técnicos e apresentá-los para diferentes públicos.
  - Planejamento estratégico em segurança da informação.
- **Certificações Relevantes:**
  - CISSP** [Certified Information Systems Security Professional].
  - CEH** [Certified Ethical Hacker].
  - CompTIA Security+**.
  - OSCP** [Offensive Security Certified Professional].
  - Certificações específicas de fornecedores [Cisco, Microsoft, AWS].

Mercado de Trabalho

A demanda por engenheiros de segurança é crescente, devido ao aumento das ameaças cibernéticas. Profissionais podem atuar em:

- Empresas de tecnologia.
- Bancos e instituições financeiras.
- Empresas de telecomunicações.
- Consultorias de TI e segurança cibernética.
- Órgãos governamentais.

Formação Acadêmica

- Graduação em áreas como:
  - Engenharia de Redes.
  - Ciência da Computação.
  - Sistemas de Informação.
- Pós-graduação ou especialização em Segurança da Informação ou áreas correlatas é um diferencial.

Salários e Benefícios

Os salários variam com base na experiência, localização e setor. Em média:

- Júnior:** R\$ 6.000 - R\$ 8.000.
- Pleno:** R\$ 9.000 - R\$ 15.000.
- Sênior:** R\$ 16.000 ou mais.

Profissionais frequentemente recebem benefícios como bônus, planos de saúde e cursos de capacitação.

O Engenheiro de Segurança é um pilar essencial para proteger organizações em um cenário cada vez mais dependente da tecnologia. Sua atuação garante a continuidade dos negócios e a proteção contra prejuízos financeiros e reputacionais.