

## Guia de Carreiras em Cibersegurança

### Resumo dos Principais Cargos, Responsabilidades e Caminhos de Aprendizagem

---



#### 1. Analista de Segurança



##### Responsabilidades

- Avaliar redes e sistemas para identificar riscos e propor soluções.
- Trabalhar com diferentes áreas para entender as necessidades de segurança da organização.
- Criar relatórios contínuos sobre vulnerabilidades e medidas corretivas.
- Desenvolver planos de segurança com base em novas ameaças e ferramentas.



##### Caminhos de Aprendizagem

- Pré-Segurança
- Cibersegurança 101
- SOC Nível 1



##### Guias Relevantes

- Tornando-se um Analista de Segurança Cibernética
  - Como se tornar um Analista SOC Nível 1
  - Um dia na vida de um Analista SOC
  - Guia de entrevista SOC L1
  - Do estudante ao Analista SOC: Caso de sucesso de Hayden
- 



#### 2. Engenheiro de Segurança



##### Responsabilidades

- Implementar e testar medidas de segurança.
- Monitorar redes e corrigir vulnerabilidades.
- Desenvolver sistemas robustos contra ameaças cibernéticas.



##### Caminhos de Aprendizagem

- SOC Nível 1
- Pentester Júnior
- Pentesting Ofensivo



##### Guias Relevantes

- Tornando-se um Engenheiro de Segurança
  - Preparando-se para entrevistas
  - Um dia na vida de um Engenheiro de Segurança
  - Caso de sucesso: Richárd
- 

### 3. Respondente de Incidentes

#### Responsabilidades

- Criar planos de resposta a incidentes.
- Agir de forma rápida e eficaz durante ataques.
- Analisar eventos passados para prevenir novos incidentes.

#### Caminhos de Aprendizagem

- SOC Nível 1
- 

### 4. Analista Forense Digital

#### Responsabilidades

- Coletar e analisar evidências digitais de incidentes.
  - Trabalhar em investigações legais e de políticas internas.
  - Documentar descobertas e auxiliar na resolução de casos.
- 

### 5. Analista de Malware

#### Responsabilidades

- Analisar programas maliciosos (malware).
  - Executar engenharia reversa para entender como funcionam.
  - Documentar atividades maliciosas e sugerir soluções.
- 

### 6. Testador de Penetração (Pentester)

#### Responsabilidades

- Testar sistemas em busca de falhas de segurança.
- Realizar auditorias, avaliações e simulações de ataques.
- Elaborar relatórios e propor melhorias.

### Caminhos de Aprendizagem

- Pentester Júnior
- Pentesting Ofensivo

### Guias Relevantes

- Como se tornar um Testador de Penetração
  - Preparação para entrevistas
  - Caso de sucesso: Tom
- 

## 7. Red Teamer

### Responsabilidades

- Simular ataques cibernéticos reais para testar a defesa da organização.
- Avaliar inteligência de ameaças e capacidade de resposta.
- Manter acesso e evitar detecção durante avaliações prolongadas.

### Caminhos de Aprendizagem

- Pentester Júnior
- Pentesting Ofensivo
- Red Teaming

### Guias Relevantes

- Red Teaming: Papéis, Salários e Oportunidades
- 

### Conclusão

As carreiras em cibersegurança são diversas e cruciais para proteger dados, redes e reputações corporativas. Plataformas como **TryHackMe** oferecem **caminhos estruturados de aprendizagem** e **guias de carreira específicos** para preparar profissionais para cada uma dessas áreas.