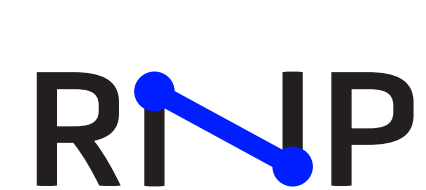




# Formação em Cibersegurança





# Programação dos Cursos

Confira agora a grade completa da formação **Hackers do Bem**:

## Nivelamento - 80h

### 1 - Introdução à cibersegurança

- Aula 1 - O que são hackers e seus tipos- White/Grey/Black hat
- Aula 2 - Ethical hackers - Conceito de ética/O que é ethical hacking?
- Aula 3 - Profissões em cibersegurança - Red Team/Blue Team/Forense/ Governança, Risco e Compliance/DevSecOps
- Aula 4 - Conceitos iniciais - Vírus/Worms/Phishing/Cavalo de Troia
- Aula 5 - Como se proteger - Noções de boas práticas para senhas/sites/e-mails

### 2 - Identificar componentes de hardware de computador

- Aula 1 - Grandezas computacionais/Sistemas numéricos
- Aula 2 - Arquitetura de hardware - CPU/Placa mãe/Memória/BIOS
- Aula 3 - Arquitetura de hardware - Armazenamento/Fontes/Gabinete/Placas de expansão
- Aula 4 - Virtualização
- Aula 5 - Instalação de SO (Windows/Linux via pendrive)

### 3 - Compreender internet e camada de acesso à rede

- Aula 1 - História da internet
- Aula 2 - Tipos de Conexões (DSL/Coaxial/FTTH/MPLS/Dedicado)
- Aula 3 - LAN/WAN/Topologias
- Aula 4 - Intranet/Extranet
- Aula 5 – Ativos de rede (Switch/Roteador/Firewall/AP)
- Aula 6 - Conectividade - Camada Física - Full/Half duplex
- Aula 7 - Par metálico
- Aula 8 - Fibra
- Aula 9 - Rádio (sem fio)

### 4 - Compreender acesso à rede e camada de internet (IP)

- Aula 1 - Camada de acesso à rede (física e enlace OSI) - Frame/Quadro endereçamento camada 2
- Aula 2 - Endereço MAC e como o dado trafega pelas redes de comunicação dos ativos das camadas 1 e 2
- Aula 3 - Protocolo ARP
- Aula 4 - Endereçamento IPv4 - Binário - Redes/Host/Broadcast - Classfull/Classless - Multicast/Broadcast/Únicas
- Aula 5 - IP Público/Privado/NAT
- Aula 6 - Subrede

### 5 - Compreender IPv6 e camada de transporte

- Aula 1 - Endereçamento IPv6 - Necessidade IPv6/Mostrar cabeçalho/ Hexadecimal/Hexadecateto
- Aula 2 - Tipos de endereço (GUA/LLA/Loopback/Unique local) - Unicast/ Multicast/Anycast
- Aula 3 - Abreviações IPv6
- Aula 4 - Subrede IPv6
- Aula 5 - Camada transporte/Cabeçalho e portas TCP/UDP/Netstat/Portas e serviços de redes principais
- Aula 6 - Protocolo TCP
- Aula 7 - Protocolo UDP

### 6 - Compreender camada de aplicação/serviços de rede

- Aula 1 - E-mail
- Aula 2 - Web (HTTP/HTTPS)
- Aula 3 - DNS
- Aula 4 - DHCP
- Aula 5 – Acessos remotos (Telnet, SSH, RDP, via aplicativos)
- Aula 6 - Transferência de arquivo (SMB, CIFS, Torrent, FTP)
- Aula 7 - Controle de usuário (LDAP, RADIUS)
- Aula 8 - SNMP/NTP/SYSLOG

### 7 - Utilizar sistemas operacionais

- Aula 1 - Versões licenciamento/Server e desktop/Histórico e versões
- Aula 2 - Estrutura de diretórios
- Aula 3 - Entendendo o File System
- Aula 4 - Criar, renomear, apagar, visualizar arquivos/pastas, comandos básicos (Gráfica e Prompt)
- Aula 5 - Criação de usuários, grupos e permissões de segurança e compartilhamento
- Aula 6 - Backup/Pontos de restauração/Registro
- Aula 7 - Instalações de programas/Pacotes/Drivers

### 8 - Lógica de programação

- Aula 1 - Fluxograma/Lógica de programação
- Aula 2 - Programas compilados e interpretados
- Aula 3 - Programação estruturada
- Aula 4 - Algoritmo
- Aula 5 - Entrada e saída
- Aula 6 - Variável
- Aula 7 - Estrutura condicional
- Aula 8 - Estrutura de repetição

### 9 - Desenvolvimento de scripts

- Aula 1 - Scripts Windows
- Aula 2 - Scripts Linux





**Básico - 64h****1 - Compreender os tipos, modelos e conceitos da computação em nuvem**

- Aula 1 - Histórico da computação em nuvem
- Aula 2 - Diferenças entre on-premise e nuvem
- Aula 3 - Características da nuvem
- Aula 4 - Modelos de implantação em nuvem (pública, privada e híbrida)
- Aula 5 - Modelos de serviços em nuvem (IaaS, PaaS e SaaS)
- Aula 6 - Principais provedores de nuvem

**2 - Compreender os principais conceitos de desenvolvimento**

- Aula 1 - Principais tipos de linguagem de programação
- Aula 2 - Principais tipos de aplicações
- Aula 3 - Metodologias de desenvolvimento
- Aula 4 - Conceitos básicos de banco de dados

**3 - Identificar as principais ameaças cibernéticas**

- Aula 1 - Tipos de ataques
- Aula 2 - Atores de ameaças
- Aula 3 - Engenharia social
- Aula 4 - Malwares

**4 - Compreender os principais elementos associados e vulnerabilidades**

- Aula 1 - Conceitos
- Aula 2 - Frameworks e padrões
- Aula 3 - Ferramentas e processos

**5 - Compreender as principais aplicações de criptografia 1 e 2**

- Aula 1 - Protocolos seguros
- Aula 2 - Hash
- Aula 3 - Tipos de chaves
- Aula 4 - Certificado digital
- Aula 5 - Infraestrutura de chave pública

**6 - Compreender os principais elementos relacionados a Governança, Risco e Compliance 1 e 2**

- Aula 1 - Confidencialidade, integridade e disponibilidade
- Aula 2 - Principais frameworks
- Aula 3 - Controles de segurança
- Aula 4 - Políticas
- Aula 5 - Aspectos legais, proteção de dados e privacidade (LGPD)
- Aula 6 - Ética





## Fundamental - 96h

### 1 - Princípios de segurança e engenharia social

- Aula 1 - Fundamentos da segurança da informação: Triade CIA, Least Privilege, Segurança em Profundidade
- Aula 2 - Atores de ameaças, atributos, vetores de ataque e fontes de inteligência
- Aula 3 - Engenharia social
- Aula 4 - Segurança ofensiva x defensiva: Ferramentas, técnicas e papéis

### 2 - Ameaças, malwares e controles

- Aula 1 - Tipos de malware
- Aula 2 - Análise de indicadores de malware e prevenção de malware
- Aula 3 - Categorias de controle de segurança
- Aula 4 - Fontes de ameaça: Darknet e Darkweb

### 3 - Técnicas utilizadas na identificação de ameaças

- Aula 1 - Gerenciamento de vulnerabilidades
- Aula 2 - Scanner de vulnerabilidades: Ativo x Passivo
- Aula 3 - Honey pots e outras armadilhas
- Aula 4 - Análise de tráfego TCP/IP

### 4 - Controles de acesso

- Aula 1 - Gerenciamento de identidade e acesso
- Aula 2 - Autenticação baseada em conhecimento
- Aula 3 - Tecnologias de autenticação
- Aula 4 - Autenticação por biometria

### 5 - Gerenciamento de identidades e contas

- Aula 1 - Tipos de contas e identidades
- Aula 2 - Políticas de contas
- Aula 3 - Soluções de autorização e políticas de pessoal
- Aula 4 - Políticas de pessoal

### 6 - Proteção Web e desenvolvimento seguro

- Aula 1 - Ataques e proteção Web - Parte 1
- Aula 2 - Ataques e proteção Web - Parte 2
- Aula 3 - Práticas de codificação segura e análise de código
- Aula 4 - Scripts em ambientes seguros

### 7 - Redundância, backup, segurança física e destruição de dados

- Aula 1 - Redundância e replicação
- Aula 2 - Backup
- Aula 3 - Segurança física
- Aula 4 - Técnicas para destruição segura de dados

### 8 - Conceitos de criptografia

- Aula 1 - Propriedades da criptografia
- Aula 2 - Criptografia simétrica
- Aula 3 - Funções Hash
- Aula 4 - Criptografia assimétrica

### 9 - Infraestrutura de chaves públicas

- Aula 1 - Autoridades certificadoras
- Aula 2 - Certificado digital
- Aula 3 - Gerenciamento de infraestrutura de chaves públicas (PKI)
- Aula 4 - Blockchain

### 10 - Segurança no host

- Aula 1 - Proteção do endpoint
- Aula 2 - Segurança em sistemas embarcados
- Aula 3 - Firmware seguro
- Aula 4 - Segurança em virtualização e nuvem

### 11 - Equipamentos de segurança

- Aula 1 - Balanceadores de carga, VPN e NAC
- Aula 2 - Segmentação de rede e port security
- Aula 3 - Equipamentos de segurança de rede (Firewall, IDS/IPS)
- Aula 4 - Segurança em redes sem fio

### 12 - Resposta a incidentes e protocolos seguros

- Aula 1 - Processo de resposta a incidentes
- Aula 2 - Protocolos seguros
- Aula 3 - Governança, compliance e gerenciamento de risco
- Aula 4 - Forense digital





## Especializado - 80 h

### Especialização Governança, Risco e Compliance

#### 1 - Governança

- Aula 1 - Conceitos fundamentais de gestão da segurança
- Aula 2 - Visão geral da ISO 27001, 27002 e 27701
- Aula 3 - Política de segurança da informação
- Aula 4 - Verificação da conformidade com requisitos legais, políticas e normas de segurança da informação
- Aula 5 - Mapeamento de processos

#### 2 - Risco

- Aula 1 - Conceitos fundamentais de gestão de riscos
- Aula 2 - A norma NBR ISO/IEC 27005 e 31000
- Aula 3 - Metodologias de gestão de riscos
- Aula 4 - Processo de tratamento, redução e retenção dos riscos
- Aula 5 - Processo de comunicação e monitoramento dos riscos

#### 3 - Compliance

- Aula 1 - Fundamentos da governança corporativa e governança corporativa de TIC
- Aula 2 - Governança corporativa de TIC x Gestão de TIC x Auditoria de TIC
- Aula 3 - Modelo do COSO
- Aula 4 - Modelo do COBIT
- Aula 5 - Normas brasileiras de compliance de TI

#### 04 - Estudo de caso

- Aula 1 - Estudo de caso

### Especialização Blue Team

#### 1 - Design de rede segura e segurança

- Aula 1 - Arquitetura e design de rede segura
- Aula 2 - Ataques e estratégias de defesa
- Aula 3 - Infraestrutura de chaves públicas
- Aula 4 - Gerenciamento de configuração e infraestrutura como serviço
- Aula 5 - Segurança em estações de trabalho

#### 2 - Segurança em sistemas operacionais e ativos de rede

- Aula 1 - Segurança em sistema Windows
- Aula 2 - Segurança em sistema Linux
- Aula 3 - Segurança de ativos de rede
- Aula 4 - segurança em ambientes virtualizados
- Aula 5 - Protocolos seguros de rede

#### 3 - Monitoramento e segurança em demais tecnologias

- Aula 1 - Gerenciando e monitorando vulnerabilidades
- Aula 2 - Segurança em redes sem fio
- Aula 3 - Técnicas de autenticação
- Aula 4 - Monitoramento e análise de tráfego
- Aula 5 - Gerenciamento de logs centralizados

#### 4 - Estudo de caso

- Aula 1 - Estudo de caso

### Especialização Red Team

#### 1 - Metodologias de pentest

- Aula 1 - Introdução ao pentest
- Aula 2 - Pré-engajamento
- Aula 3 - Reconhecimento
- Aula 4 - Scan e enumeração - Parte 01
- Aula 5 - Scan e enumeração - Parte 02

#### 2 - Teste de penetração em sistemas operacionais e ativos de rede

- Aula 1 - Ataque de engenharia social
- Aula 2 - Ataques em demais tecnologias
- Aula 3 - Ataque Web – Client-Side
- Aula 4 - Ataque Web – Server-Side
- Aula 5 - Ataques de força Bruta

#### 03 - Teste de penetração em demais tecnologias

- Aula 1 - Reconhecimento em Linux
- Aula 2 - Escalação de privilégios em Linux
- Aula 3 - Reconhecimento em Windows
- Aula 4 - Escalação de privilégios em Windows
- Aula 5 - Coleta de evidências e relatório

#### 04 - Estudo de caso

- Aula 1 - Estudo de caso

### Especialização Resposta a Incidentes e Forense

#### 1 - Tratamento de incidentes

- Aula 1 - Ameaças cibernéticas (Cyber Threats) e metodologia de cadeia de eliminação (Kill Chain Methodology)
- Aula 2 - Tratamento de incidentes e processo de resposta
- Aula 3 - Tratamento de incidentes - Malware e e-mail
- Aula 4 - Tratamento de incidentes - Rede e aplicativo web
- Aula 5 - Criando uma equipe de resposta a incidentes

#### 2 - Tratamento de dados

- Aula 1 - Coleta, tratamento e análise de dados usando um SIEM/SOAR
- Aula 2 - Detecção aprimorada de incidentes com inteligência de ameaças
- Aula 3 - Processo de investigação
- Aula 4 - Coleta de evidências: discos rígidos e sistemas de arquivos
- Aula 5 - Coleta de evidências: memória e rede

#### 3 - Forense computacional

- Aula 1 - Introdução à forense computacional - Windows e Linux
- Aula 2 - Análise forense em discos rígidos e sistemas de arquivos
- Aula 3 - Análise forense em memória
- Aula 4 - Análise forense em rede
- Aula 5 - Investigando ataques na web

#### 4 - Estudo de caso

- Aula 1 - Estudo de caso



Especialização DevOps/DevSecOps

1 - Processo de desenvolvimento seguro

- Aula 1 - Introdução ao SDLC (Software Development Lifecycle)
- Aula 2 - Modelos de SDLC (Waterfall, Lean e Agile)
- Aula 3 - Modelo DevOps
- Aula 4 - Secure SDLC
- Aula 5 - Containers

2 - DevOps e InfraAgil

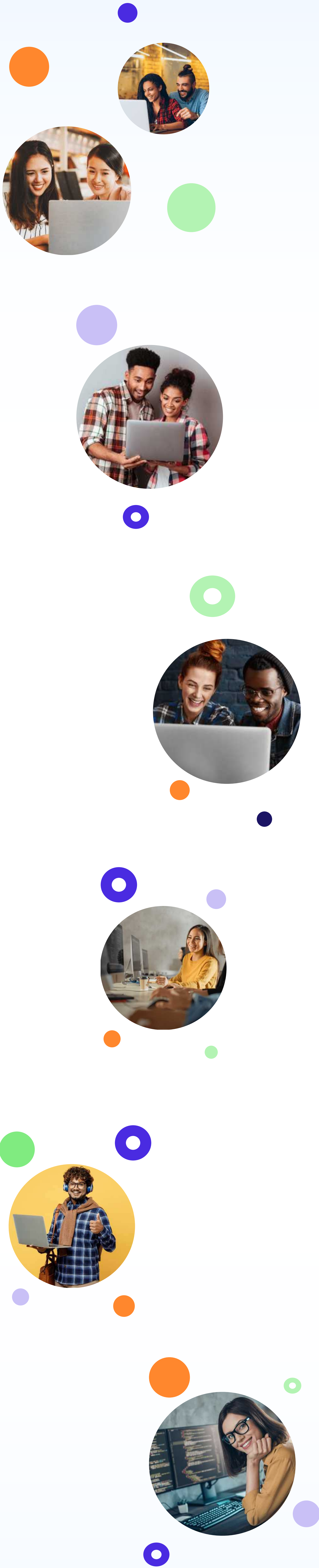
- Aula 1 - Introdução ao Git e GitLab
- Aula 2 - Infraestrutura ágil com o GitLab - Continuação
- Aula 3 - Controle de versão e resolução de conflitos com GitLab
- Aula 4 - Pipelines e integração continua com GitLab
- Aula 5 - Testes automatizados e sua importância

3 - DevSecOps

- Aula 1 - Introdução ao DevSecOps
- Aula 2 - Segurança de software e análise de vulnerabilidades
- Aula 3 - Desenvolvimento seguro e automação de tarefas de segurança
- Aula 4 - Monitoramento e resposta a incidentes em DevSecOps
- Aula 5 - Práticas em DevSecOps

4 - Estudo de caso

- Aula 1 - Estudo de caso



Residência Tecnológica

Em breve maiores informações.