



GRADE CURRICULAR COMPLETA

2.400 HORAS

SEMESTRE 1 - FUNDAMENTOS SÓLIDOS (480H)

Introduction to Computer Science - 60h

Base sólida em computação para entender sistemas, arquiteturas e fundamentos tecnológicos. Certificação alvo: CompTIA IT Fundamentals+

Mathematics for Computing - 60h

Matemática aplicada à segurança: criptografia, estatística e lógica computacional.

Networking and Communication - 60h

Protocolos de rede, TCP/IP, roteamento e comunicação segura. Certificação alvo: CompTIA Network+, Cisco CCNA

Operating Systems Fundamentals - 60h

Linux, Windows Server, administração e hardening de sistemas. Certificação alvo: Linux Essentials (LPI)

Programming Logic and Algorithms - 60h

Lógica de programação com foco em automação de segurança.

Formal and Written Communication for Technology Professionals - 60h

Comunicação técnica, relatórios de segurança e apresentações executivas.

Projeto Multidisciplinar Extensionista I - 120h

Projeto prático integrando os conhecimentos do semestre em ambiente simulado.



SEMESTRE 2 - SEGURANÇA APLICADA (480H)

Database Fundamentals – 60h

Bancos de dados, SQL injection e proteção de dados. Certificação alvo: Oracle Database SQL

Introduction to Programming – 60h

Python para automação de segurança e desenvolvimento de ferramentas. Certificação alvo: Python Institute PCAP

Cybersecurity Fundamentals – 60h

Princípios básicos de segurança, CIA Triad, frameworks de segurança. Certificação alvo: CompTIA Security+

Network Security – 60h

Firewalls, IDS/IPS, VPN e monitoramento de rede. Certificação alvo: Cisco CyberOps Associate

Operating Systems Security – 60h

Hardening, controles de acesso e monitoramento de sistemas. Certificação alvo: CompTIA Linux+

Governance, Risk, and Compliance – 60h

ISO 27001, LGPD, frameworks de compliance e gestão de riscos. Certificação alvo: ISACA CISM

Projeto Multidisciplinar Extensionista II – 120h

Implementação de controles de segurança em ambiente corporativo simulado.



SEMESTRE 3 - ESPECIALIZAÇÃO TÉCNICA (480H)

Ethics, Morals, and Human Rights in IT – 60h

Ética hacker, direitos digitais e responsabilidade profissional.

Ethical Hacking – 60h

Técnicas de penetration testing e metodologias de ethical hacking. Certificação alvo: EC-Council CEH, Offensive Security OSCP

Identity and Access Management (IAM) – 60h

Gestão de identidades, SSO, LDAP e controles de acesso. Certificação alvo: Certified Identity and Access Manager (CIAM)

Cyber Threat Intelligence – 60h

Análise de ameaças, IOCs, MITRE ATT&CK e inteligência cibernética. Certificação alvo: CompTIA CySA+

Systems Security Architecture for Cybersecurity – 60h

Arquitetura segura, design patterns de segurança e Zero Trust. Certificação alvo: CISSP-ISSAP

Cryptography, Blockchain and Secure Communication – 60h

Criptografia moderna, PKI, blockchain e comunicações seguras. Certificação alvo: EC-Council ECES

Projeto Multidisciplinar Extensionista III – 120h

Desenvolvimento de arquitetura de segurança completa para empresa fictícia.



SEMESTRE 4 - OPERAÇÕES DEFENSIVAS (480H)

Digital Forensics – 60h

Forense computacional, análise de evidências e investigação digital. Certificação alvo: CHFI (Computer Hacking Forensic Investigator)

Incident Response – 60h

Resposta a incidentes, playbooks e gerenciamento de crises. Certificação alvo: EC-Council ECIH

Cyber Defense Operations (SOC Analysis) – 60h

Operações de SOC, SIEM, análise de logs e hunting de ameaças. Certificação alvo: Splunk Core Certified User

Business Continuity and Disaster Recovery – 60h

Continuidade de negócios, planos de recuperação e resiliência. Certificação alvo: ISO 22301 Lead Implementer

Critical Infrastructure Security – 60h

Segurança de infraestruturas críticas, SCADA, IoT e sistemas industriais. Certificação alvo: GIAC GICSP

Education for Ethnic-Racial Relations and Sociodiversity – 60h

Diversidade e inclusão aplicada ao ambiente corporativo de tecnologia.

Projeto Multidisciplinar Extensionista IV – 120h

Simulação completa de SOC com resposta a incidentes reais.



SEMESTRE 5 - OPERAÇÕES OFENSIVAS E CLOUD (480H)

Offensive Security Operations – 60h

Red Team operations, Advanced Persistent Threats (APT) e ataques complexos. Certificação alvo: Offensive Security OSCP, GIAC GRTP

Application Security – 60h

Segurança de aplicações, OWASP, code review e DevSecOps. Certificação alvo: Certified Application Security Engineer (CASE)

Machine Learning & Artificial Intelligence – 60h

IA aplicada à cibersegurança, detecção de anomalias e automação. Certificação alvo: Certified Artificial Intelligence Practitioner (CAIP)

Malware Analysis – 60h

Engenharia reversa, análise de malware e desenvolvimento de assinaturas. Certificação alvo: GIAC Reverse Engineering Malware (GREM)

Cloud Security – 60h

Segurança em AWS, Azure, GCP e arquiteturas multi-cloud. Certificação alvo: CSA CCSK, AWS Security Specialty

Brazilian Sign Language (Libras) – 60h

Comunicação inclusiva e acessibilidade no ambiente de trabalho.

Projeto Multidisciplinar Extensionista V – 120h

Projeto final integrando todas as competências: Red Team vs Blue Team em ambiente real.