EMENTA DO CURSO

Cybersecurity
Segurança digital e proteção de dados

Formação para o mercado de tecnologia e segurança digital

Instituto Percorre

SOBRE O CURSO

Cybersecurity
Segurança digital e proteção de dados (160h)

O curso de Cibersegurança do Instituto Percorre prepara os participantes para compreender e aplicar práticas fundamentais de proteção digital em ambientes pessoais e corporativos.
A formação aborda desde os princípios da segurança da informação até a utilização prática de ferramentas e técnicas voltadas à análise de ameaças, proteção de sistemas e resposta a incidentes.
Com uma abordagem prática e atual, o curso integra temas como ética, privacidade de dados, ESG e sustentabilidade digital, preparando os alunos para atuar em diferentes contextos do mercado de segurança cibernética.

EMENTA

O curso apresenta os fundamentos da cibersegurança e sua aplicação prática na proteção de dados, sistemas e redes.
Ao longo da formação, os participantes desenvolvem habilidades para identificar vulnerabilidades, analisar ameaças e aplicar medidas de segurança utilizando ferramentas e metodologias do mercado.
Também são abordados temas como criptografia, redes, sistemas operacionais, testes de invasão (PenTest), ética hacker, privacidade e resposta a incidentes.
A formação combina teoria e prática por meio de laboratórios, simulações e desafios, culminando em um projeto integrador com foco em segurança digital aplicada.

OBJETIVO GERAL

Formar profissionais capazes de compreender o ecossistema da cibersegurança, identificar vulnerabilidades e aplicar práticas de proteção digital de forma ética e responsável, atuando na prevenção e resposta a incidentes.

OBJETIVOS ESPECÍFICOS

- Compreender os princípios da segurança da informação e suas aplicações
- Identificar ameaças digitais e propor estratégias de mitigação
- Aplicar medidas de segurança em redes, sistemas e dados
- Utilizar ferramentas de análise e testes de segurança de forma ética
- Desenvolver políticas básicas de proteção e resposta a incidentes
- Integrar conceitos de responsabilidade digital e ESG às práticas de segurança
- Desenvolver projetos práticos que consolidem o aprendizado técnico

COMPETÊNCIAS DESENVOLVIDAS

- Pensamento analítico aplicado à segurança digital
- Identificação e mitigação de vulnerabilidades
- Uso prático de ferramentas e metodologias de segurança
- Postura ética no ambiente digital
- Comunicação técnica e trabalho em equipe
- Desenvolvimento de políticas e planos de segurança
- Capacidade de resposta a incidentes

METODOLOGIA

A formação combina teoria e prática por meio de aulas dialogadas, estudos de caso, atividades em laboratório e simulações de incidentes reais.

Os participantes utilizam ambientes virtuais e ferramentas profissionais para análise, testes e resposta a ataques de forma controlada.

O aprendizado é progressivo, integrando conceitos técnicos e aplicação prática ao longo dos módulos, com desenvolvimento de um projeto final.

RECURSOS DIDÁTICOS

- Ambientes virtuais e simuladores (Packet Tracer, máquinas virtuais e laboratórios controlados)
- Plataformas de aprendizagem (Moodle e NetAcad)
- Ferramentas open source (Nmap, Wireshark)
- Atividades gamificadas e quizzes
- Projetos práticos e estudos de caso

ESTRUTURA DO CURSO

A formação está estruturada em módulos progressivos que integram teoria e prática, permitindo o desenvolvimento das competências de forma gradual. Cada etapa aborda conhecimentos essenciais da área, combinados com atividades aplicadas que preparam os participantes para desafios reais.

MÓDULOS:

Módulo 1 — Fundamentos de Cibersegurança e ESG

Conceitos essenciais de segurança da informação, ética hacker, normas, LGPD e a relação entre tecnologia, sustentabilidade e responsabilidade digital.

Módulo 2 — Ameaças Digitais e Proteção

Estudo de malware, engenharia social e proteção de identidade, com práticas de prevenção e análise de ataques.

Módulo 3 — Redes e Segurança de Redes

Fundamentos de redes e aplicação de medidas de segurança, incluindo segmentação e criptografia.

Módulo 4 — Sistemas Operacionais e Segurança

Configuração e proteção de sistemas Windows e Linux, com foco em controle de acesso, logs e atualização segura.

Módulo 5 — Criptografia e Proteção de Dados

Aplicação de criptografia, boas práticas de backup e estratégias de recuperação de dados.

Módulo 6 — Ferramentas e Testes de Segurança (PenTest)

Uso de ferramentas como Nmap e Wireshark para identificação de vulnerabilidades e testes controlados.

Módulo 7 — Projetos e Simulação de Incidentes

Planejamento de segurança, definição de políticas e simulação de ataques com resposta estruturada.

Módulo 8 — Soft Skills em Cibersegurança

Desenvolvimento de competências comportamentais como comunicação, pensamento crítico e trabalho em equipe.

RESULTADOS ESPERADOS

Ao final do curso, os participantes estarão preparados para atuar na identificação de riscos, aplicação de medidas de segurança e resposta a incidentes em ambientes digitais.
Mais do que conhecimentos técnicos, a formação desenvolve uma visão crítica e responsável sobre o uso da tecnologia e a proteção de dados.


Instituto
Percorre