

Especialização Information Security Operation and Support

Tecnologias de Informação - Segurança

- **Nível:**
 - **Duração:** 81h
-

Sobre o curso

Atualmente, a Segurança da Informação é uma preocupação visível e crescente nas Organizações. A competitividade empresarial é altamente dependente do acesso e da geração de mais e melhores informações. O perímetro das Organizações com o exterior é mais permissivo. Os processos de negócios são executados num contexto de troca contínua de informações com elementos externos como clientes e fornecedores.

Os hábitos sociais dos colaboradores mudaram o acesso às redes da Organização, usando os seus próprios dispositivos, nem sempre devidamente protegidos, tendo em consideração os seus dados pessoais, permitindo a criação de backdoors para dados corporativos, mesmo em comportamentos e atitudes aparentemente inofensivos.

Garantir a segurança cibernética e a conformidade, requer avaliação, implementação e manutenção contínuas.

Destinatários

- Gestores, técnicos e consultores de sistemas e tecnologias da informação
 - Executivos interessados em perceber a Segurança Cibernética, Proteção de Dados e Continuidade de Negócios, para aumentar a resiliência e trazer valor para as organizações
 - Recém-licenciados que desejam adquirir conhecimentos em Segurança da Informação para expandir suas possibilidades no mercado de trabalho
-

Programa

- Cryptography and Penetration Testing (18 horas / 3 ECTS)
 - por: [João Magalhães](#), CTO @ Globinnova Cyber Intelligence

- Secure Applications Development (18 horas / 3 ECTS)
 - por: [Alexandre Barão](#), University Professor @ Atlântica
- Systems and Networks Security (15 horas / 2,5 ECTS)
 - por: [Sérgio Nunes](#), University Professor @ Atlântica
- Cloud Security (9 horas / 1 ECTS)
 - por: [José Casinha](#), Chief Information Security Officer @ Outsystems
- Security Incident Response (9 horas / 1 ECTS)
 - por: [Daniel Caçador](#), IT Security Manager @ Caixa Económica Montepio Geral
- Auditing Information Systems and Forensics (12 horas / 2 ECTS)
 - por: [Sérgio Nunes](#), University Professor @ Atlântica

Cryptography and Penetration Testing

- Criptografia
 - Cifras simétricas
 - Análise de frequências
 - Cifras assimétricas (Public Key Cryptography)
 - Funções de hash, assinatura digital e Message Authentication Codes
 - Autenticação e controlo de acessos
 - Certificados e infraestruturas de chave pública
- Testes de Penetração
 - Fases dos ataques
 - Reconhecimento
 - Footprinting
 - Exploração
 - Enumeração
 - Hacking de sistemas
 - Testes de penetração

Secure Applications Development

- Conceitos chaves de Segurança e Internet
- Visão geral de Ameaças
 - Malware
 - Quebras de segurança
 - Negação de serviço
 - Ataques da Web
 - Sequestro de Sessão (Session Hijacking)
 - Envenenamento de DNS (DNS Poisoning)
 - Fraudes cibernéticas
- Analisando SQL Injection e outras técnicas de hacking

- Visão geral das ferramentas
- O ciclo de vida de desenvolvimento de software
- Aplicação de segurança através do SDLC
- Problemas na criação de aplicativos seguros
- Políticas de segurança e melhores práticas
- Análise de vulnerabilidades de rede

Systems and Networks Security

- Segurança dos sistemas operativos
- Autenticação segura
- Comunicações seguras
- Arquiteturas de segurança de rede
- Firewalls
- IDS
- Segurança de sistemas distribuídos
- Segurança IOT
- Segurança móvel

Cloud Security

- Conceitos de arquitetura e requisitos de desenho
 - NIST SP800-145
 - IaaS, PaaS, SaaS
 - Public Cloud, Private Cloud, Hybrid Cloud
- Segurança de dados da cloud
 - Ciclo de vida dos dados na Cloud
 - Gestão de direitos de informação
 - Prevenção de fugas de informação
 - Encriptação de dados
- Plataformas de Cloud
 - Hypervisors
 - Segurança da virtualização
 - Segurança de Perímetro
- Segurança de Aplicações na Cloud
 - Secure Software Lifecycle
 - Cloud threads
 - OWASP
- DevSecOps

Security Incident Response

- Gestão de incidentes de segurança
- Detecção de eventos e incidentes
- Vulnerabilidades de segurança
- Equipas de Resposta a Incidentes de Segurança de Computadores

Auditing Information Systems and Forensics

- Princípios de Sistemas de Informação de Auditoria
- Comportamento e Perfil do Auditor
- Metodologias de Auditoria
- Gestão da equipe de auditoria
- Recolha de informações
- Escrever e apresentar um relatório de auditoria
- Evidência CoC (Chain of Custody)
- Ciclo de vida de evidências
- Ferramentas forenses