AUDITORIA FORENSE DE REDES E SISTEMAS

Curso Técnico Superior Profissional em Redes e Segurança Informática

---

Código: 322014

Área Cientifica Predominante: Redes e arquitetura de computadores

Docente: Vitor Manuel Viana Manso

Idioma de Instrução: Português

Regime: S1

Carga Letiva: 60h Carga Trabalho: 108h

ECTS: 6,0

Objetivos

O objetivo da unidade curricular de Auditoria Forense de Redes e Sistemas, consiste em:

Transmitir os princípios fundamentais de Auditoria Forense de Redes e Sistemas, focando os aspetos maisrelevantes;

Compreender os passos e técnicas necessárias para planear e desenvolver uma auditoria assim como proceder àavaliação geral da segurança da informação de uma organização;

Transmitir os princípios fundamentais para a análise de conformidade da segurança da informação;

Transmitir os princípios fundamentais para a recuperação de dados em sistemas de ficheiros.

Resultados da Aprendizagem

Os alunos que concluam com sucesso a unidade curricular, deverão ser capazes de obter uma visão global sobreos vários elementos que constituem a Auditoria Forense de Redes e Sistemas e qual a sua importância nosprocessos de auditoria assim com a sua aplicação em deferentes cenários;

Dominar as seguintes temáticas com especial destaque para:

A importância da Informática Forense

Princípios gerais de auditoria

Contexto legal e normativo no domínio da informática forense

Norma ISO 27001 e COBIT 5

Sistemas de proteção de dados

Ferramentas Forenses

Proteção da propriedade e informação confidencial

Práticas de Encriptação

Técnicas forense on-line e off-line

Conteúdos Programáticos

A importância da Informática Forense

Princípios gerais de auditoria

Contexto legal e normativo no domínio da informática forense

Norma ISO 27001 e COBIT 5

Sistemas de proteção de dados

Ferramentas Forenses

Proteção da propriedade e informação confidencial

Práticas de Cifra

Técnicas forenses on-line e off-line

Bibliografia Recomendada

Michael A. Caloyannides: Computer Forensics and Privacy, Artech House Publishers

Chris Prosise, Kevin Mandia, Matt Pepe: Incident Response and Computer Forensics, Second Edition,

McGraw?Hill Osborne Media

Brian Carrier: File System Forensic Analysis, Addison?Wesley Professional

Harlan Carvey: Windows Forensics and Incident Recovery, Addison?Wesley Professional

Métodos de Ensino e de Aprendizagem

Ao adquirirem os conhecimentos ministrados no conteúdo programático, os alunos serão capazes de obter umavisão global sobre os diversos procedimentos de Auditoria Forense de Redes e sistemas, da sua função erelacionamento, dominar diversas técnicas e ferramentas Forense on-line e off-line, proteção de deados ecifra, conhecer as normas ISO 27001 e COBIT 5 e respetiva interpretação e aplicabilidade, conhecer ocontexto legal e normativo no domínio da informática forense.

Saberão compreender e implementar as principais técnicas de proteção de informação confidencial.

Métodos de Avaliação

Metodologias de Avaliação:

A avaliação é composta por duas componentes teóricas e uma componente prática. As componentes teóricas têmum peso total de 50% (25% + 25%), e a componente prática um peso de 40%, assiduidade + Participação e aula(10%). O trabalho prático é obrigatório. É exigido a obtenção de 7,5 valores a cada uma das componentes, amédia final terá de ser maior ou igual a 10 valores, para aprovação.

Avaliação contínua:

Dois Testes Escritos (25% + 25%)

Componente pratica (40%)

Assiduidade + Participação (10%)

Presença pelo menos a dois terços das horas de contacto

Avaliação Recurso e Especial:

Teste Escrito (70%)

Trabalho Prático realizado na Avaliação Contínua (mantém nota, não é permitida nova entrega) (20%)

Assiduidade + Participação (10%)

Presença pelo menos a dois terços das horas de contacto