## Informação Geral:

| | | | |
|---|---|---|---|
| **Unidade Orgânica** | Escola Superior de Tecnologia e Gestão | **Ano Letivo** | 2017/2018 |
| **Curso** | Mestrado em Engenharia Informática - Computação Móvel (D) [M238] | **Grau** | Mestrado |
| **Ano Curricular** | 1 | **Período** | S1 |
| **UC/Módulo** | Cibersegurança | **ECTS** | 6 |
| **Área Científica** | Engenharia Informática | **Carácter** | Obrigatório |

| **Horas Totais** | 162 | **T** | 0 | **TP** | 30 | **PL** | 30 | **TC** | 0 | **S** | 0 | **E** | 0 | **OT** | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

*T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutorial*

## Docente responsável:

Carlos Manuel da Silva Rabadão

## Docentes que lecionam a unidade curricular:

Carlos Manuel da Silva Rabadão ( 60,00 horas semanais de contacto: TP: 30,00; PL: 30,00; )

## Pré-requisitos:

Não aplicável.

## Idioma:

Português e Inglês

## Enquadramento:

Cibersegurança é o processo de aplicação de medidas de segurança para garantir a confidencialidade, integridade e disponibilidade dos dados. A cibersegurança garante a proteção dos ativos tangíveis e intangíveis das organizações, nomeadamente dados, equipamentos terminais, servidores, edifícios, e mais importante, a privacidade dos seres humanos.
O objetivo principal da cibersegurança é a proteção dos dados/informação tanto em trânsito como em repouso, adotando-se para o efeito um conjunto de contramedidas destinadas a garantir a segurança dos dados.

Nesta UC pretende-se consolidar as competências de segurança dos estudantes, com principal incidência sobre os desafios emergentes da mobilidade e da computação em nuvem.

## Objetivos de aprendizagem:

C1. Conhecimento dos desafios de segurança em sistemas distribuídos
C2. Conhecimento sobre os novos desafios de segurança associados à mobilidade
C3. Competências para identificar os riscos e ameaças associados a sistemas distribuídos e para adotar medidas com vista à sua mitigação
C4. Realização de julgamento/tomada de decisão ao nível da segurança, para a conceção e implementação de sistemas distribuídos seguros
C5. Capacidade para selecionar as ferramentas mais adequadas à implementação de cenários de segurança e justificar as opções tomadas
C6. Capacidade para realizar tarefas de teste, monitorização e auditoria

C7. Aplicação da aprendizagem em novas situações e contextos
C8. Reforço das competências de investigação, análise e avaliação de cenários de cibersegurança
C9. Capacidade para expor e defender com clareza as principais vantagens e fraquezas das soluções adotadas

## Programa:

**Conteúdos Programáticos:**

1. Desafios colocados pela mobilidade, pela virtualização e pela computação em nuvem
2. Nova geração de malware
3. Mitigação de risco da utilização de dispositivos/aplicações móveis
4. Políticas de segurança aplicadas a aplicações e serviços móveis
5. Gestão da segurança dos dispositivos móveis em ambientes empresariais
6. Firewalls de nova geração
7. Desafios colocados à segurança pelo Big Data
8. Desafios emergentes na área da segurança em sistemas distribuídos e ubíquos

**Fundamentação da coerência dos conteúdos programáticos com os objetivos/competências da unidade curricular:**

Os conteúdos dos capítulos 1 a 7 possibilitam aos estudantes a obtenção e consolidação dos conhecimentos relacionados com a segurança ao nível dos sistemas distribuídos, com particular incidência sobre os desafios colocados pela mobilidade, virtualização e computação em nuvem, identificados nas competências C1 e C2. Permitem ainda dotar os estudantes dos conhecimentos e técnicas essenciais para a resolução de problemas reais, a resolver em ambiente laboratorial, que contribuem para a obtenção das competências identificadas em C3, C4,C5 e C6. Por fim, os conteúdos do capítulo 8, relacionados com a abordagem de desafios emergentes na área da segurança em sistemas distribuídos e ubíquos, são apresentados pelos estudantes, em sala de aula aberta, na sequência da elaboração dos seus trabalhos de investigação. Esta metodologia, a par com o projeto realizado em ambiente laboratorial, contribui para a obtenção das competências identificadas em C7,C8 e C9.

## Metodologia de Ensino / Aprendizagem:

**Presencial:**

EP.1.Teórico: Apresentação pelo professor dos conteúdos programáticos referentes aos capítulos 1 a 6 e a sua assimilação por parte dos estudantes
EP.2.Teórico-prático: Apresentação pelos estudantes, com discussão oral, de temas relacionados com os desafios emergentes na área da segurança em sistemas distribuídos e ubíquos; Consolidação dos conhecimentos teóricos, através da especificação das questões de segurança e privacidade associadas a exemplos de serviços de nova geração
EP.3. Realização de projeto laboratorial que correspondem à consolidação dos conhecimentos adquiridos nas fases anteriores

**Autónoma:**

AA.1.Realização de um trabalho de pesquisa bibliográfica individual sobre temas emergentes na área da Cibersegurança e respetivo relatório/artigo sobre o tema abordado

**Recursos Específicos:**

- Plataforma de gestão e distribuição de conteúdos
- Elementos de apoio disponibilizados pelos docentes

## Avaliação:

**Descrição:**

AP=Avaliação periódica
AP.1.Trabalho escrito (individual) (TE)
AP.2.Projeto (P)
AP.3.Classificação final: CF=0,4*TE+0,6*P

EA.Avaliação por exameEA.1.Trabalho escrito (individual) (TE)
EA.2.Projeto (P)
AP.3.Classificação final: CF=0,4*TE+0,6*P

- Quando tiverem sido obtidos os mínimos exigidos, as notas obtidas numa época de avaliação podem ser guardadas para as épocas subsequentes do mesmo ano letivo, caso o estudante assim o pretenda.

- Não são guardadas notas de anos letivos anteriores.

- O estudante que se inscreva para melhoria de nota tem que realizar todos os elementos de avaliação da época em causa. Não serão tidas em conta classificações obtidas em épocas de avaliação anteriores.

| | |
|---|---|
| **Número de elementos de avaliação final:** | 2 |
| **Número de elementos de avaliação contínua/periódica:** | 2 |

## Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:

A metodologia de ensino teórico baseia-se na transmissão de conhecimentos sobre a segurança ao nível dos sistemas distribuídos, com particular incidência sobre os desafios emergentes colocados pela mobilidade, pela virtualização e pela computação em nuvem, que permite aos estudantes a obtenção dos conhecimentos essenciais sobre os principais desafios de segurança em sistemas distribuídos (CI) e dos conhecimentos sobre os novos desafios de segurança associados à mobilidade (C2), fornecendo-lhe competências para identificar os riscos e ameaças associados a sistemas distribuídos e para adotar medidas com vista à sua mitigação (C3)
A metodologia utilizada na componente laboratorial, que se baseia na resolução de problemas reais, e que contempla as seguintes fases: a) caracterização do problema a resolver, b) conceção de um sistema para resolver esse problema, c) implementação de um protótipo, d) realização de testes e e) apresentação e defesa do projeto realizado, permitem desenvolver nos estudantes os objetivos/competências específicos (C4,C5,C6,C7)
A metodologia de ensino teórico-prático, associada com a metodologia de estudo autónomo, baseia-se no execução de trabalhos de investigação/pesquisa bibliográfica e da sua apresentação e defesa em sala de aula, que permitem reforçar as competências de investigação, análise e avaliação de cenários de cibersegurança (C8) e aprofundar a capacidade para expor e defender com clareza as principais vantagens e fraquezas das soluções adotadas (C9)

## Bibliografia:

**Recomendada:**

Apontamentos das aulas teóricas e práticas
Shon Harris, “CCISP Exam Guide”, ISBN 978-0-07-178174-9, McGraw-Hill, 2013
Jennifer L. Bayuk et all, “Cyber Security Policy Guidebook”, ISBN 978-1-118-02780-6, John Wiley & Sons, 2012
Neil Bergman, Mike Stanfield, Jason Rouse, Joel Scambray, “Hacking Exposed: Mobile Security - Secrets & Solutions”, ISBN: 978-0-07-181702-8, McGraw-Hill, 2013

**Complementar:**

Pennie Walters, “The Risks of Using Portable Devices”, White Paper, US-Cert - Carnegie Mellon University, 2012
Mobility Security Guide, White Paper, National Security Agency, 2013
Steve Piper, “Big Data Security For Dummies”, ISBN: 978-1-118-51727-72013, John Wiley & Sons, Inc., 2013