

\* Escola Superior de Tecnologia de Abrantes

Ano letivo: 2021/2022

**Informática e Tecnologias Multimédia**

Licenciatura, 1º Ciclo

Plano: Despacho n.º 9184/2020 - 25/09/2020

**Ficha da Unidade Curricular: Segurança Informática**

ECTS: 5; Horas - Totais: 135.0, Contacto e Tipologia, TP:28.0; PL:28.0;

Ano | Semestre: 3 | S2

Tipo: Optativa; Interação: Presencial; Código: 814334

Área Científica: Tecnologias Multimédia

**Docente Responsável**

Valter José Gonçalves Bouça

Assistente 1º Triénio

**Docente(s)**

Valter José Gonçalves Bouça

Assistente 1º Triénio

**Objetivos de Aprendizagem**

Os estudantes que terminam com sucesso esta unidade curricular serão capazes de compreender os principais tipos de ameaças à segurança de sistemas informáticos e agir no sentido de os prever e solucionar.

**Objetivos de Aprendizagem (detalhado)**

Os estudantes que terminam com sucesso esta unidade curricular serão capazes de:

1. Compreender os principais tipos de ameaças à segurança de sistemas informáticos;
2. Compreender, escolher e utilizar mecanismos e protocolos criptográficos, incluindo aspetos da gestão de chaves;
3. Compreender, escolher e utilizar modelos e mecanismos para o controlo de acesso;
4. Identificar vulnerabilidades existentes em programas e usar técnicas adequadas à sua correção.

**Conteúdos Programáticos**

1. Esquemas e protocolos criptográficos e métodos de gestão de chaves
2. Tecnologias de segurança
3. Modelos e mecanismos para controlo de acessos
4. Escrita de código seguro

### **Conteúdos Programáticos (detalhado)**

1. Esquemas e protocolos criptográficos e métodos de gestão de chaves
  - 1.1. Esquemas de cifra simétrica e assimétrica, esquemas MAC e de assinatura digital
  - 1.2. Protocolos de autenticação e estabelecimento de chaves
  - 1.3. Infraestruturas de chave pública
2. Tecnologias de Segurança
  - 2.1. Firewalls
  - 2.2. Sistemas de Detecção de Intrusão (IDS)
  - 2.3. Canais Seguros
    - 2.3.1. IPSec
    - 2.3.2. SSL/TLS
    - 2.3.3. VPN
  - 2.4. Segurança em WLAN
3. Modelos e mecanismos para controlo de acessos
  - 3.1. Monitor de referências e "Trusted Computer Base"
  - 3.2. Modelos e mecanismos de autorização clássicos
    - 3.2.1. Matriz de controlo de acessos
    - 3.2.2. Listas de controlo de acessos e "capabilities"
    - 3.2.3. Modelos baseados em reticulados e modelo de Clark-Wilson
  - 3.3. Modelos RBAC ("Role Based Access Control")
  - 3.4. Modelos e mecanismos baseados na identidade do código
  - 3.5. Modelos baseados no paradigma Trust Management
4. Escrita de código seguro
  - 4.1. Vulnerabilidades típicas
  - 4.2. Técnicas de proteção
  - 4.3. Metodologias de desenho e desenvolvimento

### **Metodologias de avaliação**

#### Avaliação Contínua:

- 15%: Observação direta em sala de aula
- 40%: Nota prática: nota média de 4 trabalhos práticos, realizados individualmente ou em grupo. Nota mínima de 10 valores.
- 45%: Nota teórica: prova escrita. Nota mínima de 7 valores.

#### Avaliação Periódica ou Final:

- 50%: Nota prática: nota média de 2 a 4 trabalhos práticos, realizados individualmente ou em grupo. Nota mínima de 10 valores.
- 50%: Nota teórica: prova escrita. Nota mínima de 7 valores.

Para obter aprovação à UC é necessário obter média final não inferior a 9,5 valores e cumprir todos os critérios de nota mínima.

### **Software utilizado em aula**

Oracle's Virtual Box / VMWare Player  
Microsoft Windows Server 2012  
CentOS 7  
Kali Linux  
Plataforma de eLearning

### **Estágio**

Não aplicável

### **Bibliografia recomendada**

- Gollman, D. (2011). *Computer Security (3 ed.)* (Vol. ). (pp. - ). Addison-Wesley. USA  
- Bishop, M. (2018). *Computer Security: Art and Science (2 ed.)* (Vol. ). (pp. - ). Addison-Wesley. USA

### **Coerência dos conteúdos programáticos com os objetivos**

1. Compreender os principais tipos de ameaças à segurança de sistemas informáticos: obtido pela globalidade dos conteúdos programáticos.
2. Compreender, escolher e utilizar mecanismos e protocolos criptográficos, incluindo aspetos da gestão de chaves: obtido maioritariamente no pontos 1 e 2 dos conteúdos programáticos;
3. Compreender, escolher e utilizar modelos e mecanismos para o controlo de acesso: obtido maioritariamente no ponto 3 dos conteúdos programáticos;
4. Identificar vulnerabilidades existentes em programas e usar técnicas adequadas à sua correcção: obtido maioritariamente no ponto 4 dos conteúdos programáticos

### **Metodologias de ensino**

Ensino teórico-prático com recurso a meios áudio-visuais, a equipamento laboratorial e a exemplos práticos.

### **Coerência das metodologias de ensino com os objetivos**

Promove-se a aprendizagem através da experiência prática e da resolução de problemas. Assim, nas aulas teórico-práticas são apresentados os fundamentos teóricos devidamente enquadrados em cenários reais. Nas aulas práticas são testadas e avaliadas as soluções propostas pelos alunos para cada um dos problemas identificados.

### **Língua de ensino**

Português

**Pré-requisitos**

Não aplicável

**Programas Opcionais recomendados**

Não aplicável

**Observações**

O funcionamento da UC seguirá os tópicos definidos nos Objetivos de Desenvolvimento Sustentável, com ênfase nos pontos "Educação de Qualidade" e "Energias Renováveis e Acessíveis".

Objetivos de Desenvolvimento Sustentável:

- 4 - Garantir o acesso à educação inclusiva, de qualidade e equitativa, e promover oportunidades de aprendizagem ao longo da vida para todos;
- 9 - Construir infraestruturas resilientes, promover a industrialização inclusiva e sustentável e fomentar a inovação;

---

**Docente responsável**

**Valter José**  
**Gonçalves Bouça**

Digitally signed by  
Valter José Gonçalves  
Bouça