

## **IA NA CIBERSEGURANÇA**

Mestrado em Inteligência Artificial Aplicada

---

Código: 28515

Área Científica Predominante: Arquitetura de Computadores, Sistemas Distribuídos e Cibersegurança

Docente: Nuno Alberto Ferreira Lopes

Idioma de Instrução: Português

Regime: S1

Carga Letiva: 30h Carga Trabalho: 138h

ECTS: 6,0

---

### **Objetivos**

O objectivo desta UC é dotar os estudantes com a capacidade de identificar técnicas de inteligência artificial para a resolução de problemas de cibersegurança.

### **Resultados da Aprendizagem**

Os estudantes conhecerão os conceitos de cibersegurança: propriedades da segurança da informação, conceitos de ataque, vulnerabilidade e ameaça, e padrões de ataque comuns.

Os estudantes adquirirão competências na utilização de ferramentas de segurança para cenários de segurança típicos e na aplicação de técnicas de IA e de aprendizagem automática para prevenir e detetar ataques.

### **Conteúdos Programáticos**

Conceitos de cibersegurança:

Propriedades da segurança da informação C.I.A.

Comunicações (protocolos) seguras

Conceitos de ataque, vulnerabilidade e ameaça

Padrões de ataque comuns

Ferramentas de segurança:

Sistemas de detecção de intrusão e firewalls

Detecção de malware

Detecção de correio electrónico spam

Impedir o acesso não autorizado ao login

Aplicação de técnicas de IA e de aprendizagem automática para prevenir e detectar ataques:

Agrupamento

Classificação

Regressão

Conjuntos de dados específicos para a cibersegurança

### **Bibliografia Recomendada**

Emmanuel Tsukerman, Machine Learning for Cybersecurity Cookbook, 2019, Packt (ISBN: 978-178-961-467-1)

Alessandro Parisi, Hands-On Artificial Intelligence for Cybersecurity, 2019, Packt (ISBN: 978-178-980-402-7)

### **Métodos de Ensino e de Aprendizagem**

Os conteúdos programáticos abordam por um lado os conceitos teóricos e alguns casos práticos de cibersegurança, por outro lado a aplicação de técnicas de inteligência artificial. Estas duas abordagens fazem com que os estudantes consigam relacionar a interação entre ambas e assim cumprir com os objectivos da UC.

### **Métodos de Avaliação**

Trabalho prático (individual), abrangendo todo o programa (70%).

O trabalho prático terá de ser apresentado.

Artigo científico escrito (30%).

A avaliação fora do período de avaliação contínua terá uma penalização de 5 valores para o trabalho prático.