English version at the end of this document

Ano Letivo	2022-23
Unidade Curricular	INTELIGÊNCIA ARTIFICIAL APLICADA À CIBERSEGURANÇA
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381008
Área Científica	
Sigla	
Código CNAEF (3 dígitos)	481
Contributo para os Objetivos de Desenvolvimento Sustentável - ODS (Indicar até 3 objetivos)	4,9,11
Línguas de Aprendizagem	English

Modalidade de ensino

B-Learning

Docente Responsável José Luís Valente de Oliveira

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
José Luís Valente de Oliveira	S	S1	4S

* Para turmas lecionadas conjuntamente, apenas é contabilizada a carga horária de uma delas.

ANO	PERÍODO DE FUNCIONAMENTO*	HORAS DE CONTACTO	HORAS TOTAIS DE TRABALHO	ECTS
1º	S1		25	1

* A-Anual;S-Semestral;Q-Quadrimestral;T-Trimestral

Precedências

Sem precedências

Conhecimentos Prévios recomendados

Não aplicável

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

O Módulo de Inteligência Artificial aplicada à Cibersegurança pretende dotar o estudante com conhecimentos que lhe permita utilizar técnicas de inteligência artificial e machine learning na cibersegurança. É ainda objetivo desenvolver conhecimento de modelação e deteção de ameaças através de algoritmos de Inteligência Artificial contra ataques cibernéticos. Pretende ainda dotar o estudante de conhecimentos de como utilizar a inteligência artificial na gestão e registo de eventos.

Conteúdos programáticos

- Conceitos de inteligência artificial e de machine learning;
- Técnicas utilizadas para a modelação de ameaças e deteção de vulnerabilidades;
- Algoritmos de Inteligência Artificial na utilização contra modelos de ataques cibernéticos;
- A inteligência artificial e o machine learning na gestão, monitorização de eventos para deteção de possíveis ataques informáticos.

Metodologias de ensino (avaliação incluída)

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através da componente teórica
- Prática laboratorial de aplicação de algoritmos de inteligência artificial e machine learning
- Atendimento individual ou em grupo para esclarecimento de dúvidas
- Apoio às atividades e esclarecimento sobre funcionamento da unidade curricular.

A avaliação é efetuada através de um teste de avaliação:

- Teste individual para a avaliação de conhecimentos (100%)

Os estudantes que obtiverem uma classificação final inferior a 9,5 valores no teste individual terão acesso a um exame de recurso.

Bibliografia principal

Referência principal:

Alessandro Parisi (2019), *Hands-on Artificial Intelligence for Cybersecurity* , Packt Publishing, ISBN-10: 978-1789804027

Referências complementares

Cylance Data Team (2017), *Introduction to Artificial Intelligence for Security Professionals* , The Cylance Press.

Yvonne R. Masakowski (2020), *Artificial Intelligence and Global Security: Future Trends* , Threats and Considerations, Emerald Publishing Limited.

Archie Addo and Srini Centhala (2020), *Artificial Intelligence for Security* , Business Expert Press.

Yevgeniy Vorobeychik and Murat Kantarciogluv (2018), *Adversarial Machine Learning* , Morgan & Claypool Publishers

Academic Year	2022-23
Course unit	
Courses	
Faculty / School	FACULTY OF SCIENCES AND TECHNOLOGY
Main Scientific Area	
Acronym	
CNAEF code (3 digits)	481
Contribution to Sustainable Development Goals - SGD (Designate up to 3 objectives)	4,9,11
Language of instruction	English
Teaching/Learning modality	B-learning

Coordinating teacher José Luís Valente de Oliveira

Teaching staff	Type	Classes	Hours (*)
José Luís Valente de Oliveira	S	S1	4S

* For classes taught jointly, it is only accounted the workload of one.

Contact hours

T	TP	PL	TC	S	E	OT	O	Total
0	0	0	0	0	0	0	0	25

T - Theoretical; TP - Theoretical and practical ; PL - Practical and laboratorial; TC - Field Work; S - Seminar; E - Training; OT - Tutorial; O - Other

Pre-requisites

no pre-requisites

Prior knowledge and skills

Not Applicable

The students intended learning outcomes (knowledge, skills and competences)

Artificial Intelligence applied to Cybersecurity intents for the student to acquire knowledge that allows to apply artificial intelligence and machine learning techniques applied to cybersecurity. It is also a goal the knowledge acquisition by the student in the modeling and threat detection through artificial intelligence algorithms against cybernetic attacks. The management and record events registration allows the discovery of patterns only perceptible by applying artificial intelligence, which is another knowledge to be learned by the students.

Syllabus

- Artificial intelligence and machine learning concepts.
- Modeling and vulnerability detection techniques.
- Using artificial intelligence algorithms in threat detection against cybernetic attacks.
- Artificial intelligence and machine learning in management and event monitorization to detect patterns and possible cybernetic attacks.

Teaching methodologies (including evaluation)

This curricular unit combines several teaching methods:

- Theoretical classes syllabus exposition
- Conception, configuration, and implementation of firewall modules during the seminar and autonomous work.
- Individual or group doubt clarification
- Activity support and curricular unit functioning clarification

The evaluation is an evaluation test:

- Individual knowledge evaluation test (100%)

The students that do not acquire 9.5 values in 20 in the individual test will have access to an appel exam.

Main Bibliography

Text book:

Alessandro Parisi (2019), *Hands-on Artificial Intelligence for Cybersecurity* , Packt Publishing, ISBN-10: 978-1789804027

Complementary references

Cylance Data Team (2017), *Introduction to Artificial Intelligence for Security Professionals* , The Cylance Press.

Yvonne R. Masakowski (2020), *Artificial Intelligence and Global Security: Future Trends* , Threats and Considerations, Emerald Publishing Limited.

Archie Addo and Srini Centhala (2020), *Artificial Intelligence for Security* , Business Expert Press.

Yevgeniy Vorobeychik and Murat Kantarciogluv (2018), *Adversarial Machine Learning* , Morgan & Claypool Publishers.