
Ano Letivo 2022-23

Unidade Curricular DESENVOLVIMENTO DE SOFTWARE SEGURO

Cursos CIBERSEGURANÇA

Unidade Orgânica Faculdade de Ciências e Tecnologia

Código da Unidade Curricular 19381013

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 Inglês

Modalidade de ensino

B-Learning

Docente Responsável

Adriano Pires

| DOCENTE | TIPO DE AULA | TURMAS | TOTAL HORAS DE CONTACTO (*) |
|---------------|--------------|--------|-----------------------------|
| Adriano Pires | 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 | S2 | | 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 Desenvolvimento de Software Seguro pretende dotar o estudante com conhecimentos das mais modernas metodologias de segurança informática no desenvolvimento aplicacional, web e os padrões atuais de arquitetura de desenvolvimento. É ainda objetivo desenvolver conhecimento de implementação de segurança no desenvolvimento de frontend e backend.

Pretende ainda dotar o estudante de conhecimentos de segurança em serviços de bases de dados, armazenamento de objetos e das infraestruturas atuais de segurança no desenvolvimento.

Conteúdos programáticos

- Os mais modernos métodos de segurança informática em desenvolvimento aplicacional e web;
- Padrões de arquitetura para um desenvolvimento ágil e seguro;
- Segurança no desenvolvimento de frontend e backend;
- Serviços de Bases de Dados, armazenamento de objetos, infraestruturas de segurança e redundância, load balancers, orquestradores e contentorização;
- Erros típicos conhecidos pela OWASP;
- Técnicas mais conhecidas de Safecoding, Code revision e plataformas de secure coding enforcement;
- Implementação de um software Development Life Cycle Software (SDLC)

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 configuração de sistemas de redundância, orquestração e contentorização.
- 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 igual ou superior a 9,5 valores em cada elemento de avaliação estão dispensados do exame final.

Bibliografia principal

- Liz Rice (2020), Container Security, O'Reilly, ISBN-10: 1492056707
- Kasun Indrasiri and Prabath Siriwardena, Microservices for the Enterprise: Designing, Developing and Deploying, Apress, ISBN-10: 1484238575
- Andrew Hoffman (2020), Web application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly, ISBN-10: 1492053112
- Malcolm McDonald (2020), Web Security for Developers: Real Threats, Practical Defense, No Starch Press, ISBN-10: 1593279949
- Dafydd Stuttard and Marcus Pinto (2011), The Web Application Hacker's Handbook, Wiley, ISBN-10: 1118026470
- Mark A. Russo (2019), The Agile/Security development Life Cycle, Independently Published, ISBN-10: 1794490574

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

Adriano Pires

| Teaching staff | Type | Classes | Hours (*) |
|----------------|------|---------|-----------|
| Adriano Pires | 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 Aplicable

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

The Secure Software Development Module aims to provide the student with knowledge of the most modern computer security methodologies in the application, web development and current standards of development architecture. It is also pretends to develop knowledge of security implementation in frontend and backend development.

It also intends to provide the student with security knowledge in database services, storage of objects and current security infrastructures in development.

Syllabus

- Latest computer security methods in application and web development;
- Architectural patterns in agile and secure software development;
- Frontend and Backend software development security;
- Database services, object storage, security and redundancy infrastructures, load balancers, orchestration and containers;
- OWASP well known common errors;
- Well known Safecoding techniques, Code revision and secure coding enforcement platforms;
- Implementing a Software Development Life Cycle (SDLC)

Teaching methodologies (including evaluation)

This curricular unit combines various teaching methods:

- Program content exhibition through theoretical lectures
- Practice laboratorial lessons, with an autonomous hands on project on redundancy systems, orchestration and containers;
- Individual or group attendance for out of classroom support;
- Activity support and curricular unit functioning clarification

Evaluation is determined by an individual test in which:

- Individual knowledge evaluation test (100%)

Students that achieve a final grade of 9.5 or higher in each of the evaluation components, are excused from the final exam.

Main Bibliography

- Liz Rice (2020), Container Security, O'Reilly, ISBN-10: 1492056707
- Kasun Indrasiri and Prabath Siriwardena, Microservices for the Enterprise: Designing, Developing and Deploying, Apress, ISBN-10: 1484238575
- Andrew Hoffman (2020), Web application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly, ISBN-10: 1492053112
- Malcolm McDonald (2020), Web Security for Developers: Real Threats, Practical Defense, No Starch Press, ISBN-10: 1593279949
- Dafydd Stuttard and Marcus Pinto (2011), The Web Application Hacker's Handbook, Wiley, ISBN-10: 1118026470
- Mark A. Russo (2019), The Agile/Security development Life Cycle, Independently Published, ISBN-10: 1794490574