LICENCIATURA: Engenharia Informática	**ÁREA CIENTÍFICA:** Engenharia Informática
UNIDADE CURRICULAR/CURRICULAR UNIT: Cibersegurança / Cybersecurity	**ECTS: 4**
Duração: Semestral	**Horas de Contacto (Teórico Práticas):** 60 (48 TP+12 OT)

OBJETIVOS DE APRENDIZAGEM/ / LEARNING OUTCOMES OF THE CURRICULAR UNIT

Para concluir com sucesso esta unidade curricular, os estudantes deverão demonstrar possuir os seguintes conhecimentos e capacidades:

1. Ter uma visão holística dos principais problemas de segurança que se colocam aos Sistemas de Informação das organizações.
2. Dominar os meios e técnicas para enfrentar os problemas de segurança e Cibersegurança nos SI
3. Conhecer os elementos de apoio ao planeamento de Sistemas Informáticos e à Auditoria Informática.

(English)

To successfully complete this curricular unit, students must demonstrate the following knowledge and skills:

1. Have a holistic view of the main security problems faced by organizations' Information Systems.
2. Mastering the means and techniques to face security and cybersecurity problems in Information Systems.
3. Know the elements to support the planning of IT Systems and IT Audit.

CONTEÚDOS PROGRAMÁTICOS/SYLLABUS

Parte 1 – Fundamentos de Cibersegurança

1. Conceitos gerais e Princípios de arquitetura de Cibersegurança
2. Cibersegurança de redes, sistemas e aplicações
3. Cibersegurança em Portugal
4. Vulnerabilidades e ataques
5. Contramedidas
6. Planeamento na resposta a incidentes

Parte 2 – Boas práticas operacionais de Cibersegurança

1. Gestão do Risco
2. Identificação, Proteção e Deteção de ameaças de Cibersegurança
3. Resposta e Recuperação a incidentes de Cibersegurança
4. Ferramentas de Cibersegurança

Parte 3 – Governança e Gestão da Cibersegurança

1. Governança e Gestão da Cibersegurança
    a. Função TI e Planeamento nas organizações
    b. Mudança de mentalidades e Formação

2. Conformidade legal e normativa da Cibersegurança
    a. Normas para a Cibersegurança
    b. Privacidade de Dados e RGPD
    c. Política de Segurança
    d. Cibercrime, e Análise Forense
3. Auditoria da Cibersegurança
    a. Análise de Risco
    b. Controlos de Cibersegurança

(English)

Part 1 – Cybersecurity Fundamentals

1. General Concepts and Principles of Cybersecurity Architecture

2. Cybersecurity of networks, systems and applications

3. Cybersecurity in Portugal

4. Vulnerabilities and Attacks

5. Countermeasures

6. Incident response planning

Part 2 - Cybersecurity operational best practices

1. Risk Management

2. Identification, Protection and Detection of Cybersecurity Threats

3. Cybersecurity Incident Response and Recovery

4. Cybersecurity Tools

Part 3 - Cybersecurity Governance and Management

1. Cybersecurity Governance and Management

   a. IT Function and Planning in Organizations

   b. Mindset change and training

2. Cybersecurity legal and regulatory compliance

   a. Standards for Cybersecurity

   b. Data Privacy and GDPR

   c. Security policy

   d. Cybercrime, and Forensic Analysis

3. Cybersecurity Audit

a. Risk analysis

b. Cybersecurity Controls

DEMONSTRAÇÃO DA COERÊNCIA DOS CONTEÚDOS PROGRAMÁTICOS COM OS OBJETIVOS DA UNIDADE CURRICULAR/ DEMONSTRATION OF THE SYLLABUS COHERENCE WITH THE CURRICULAR UNIT'S OBJECTIVES

Correspondência dos objetivos com os conteúdos programáticos:

1. Ter uma visão holística dos principais problemas de segurança que se colocam aos Sistemas de Informação das organizações.

- Parte 1 – Fundamentos de Cibersegurança – estes conteúdos permitem atingir o objetivo enunciado.

2. Dominar os meios e técnicas para enfrentar os problemas de segurança e Cibersegurança nos SI

- Parte 2 – Boas práticas operacionais de Cibersegurança – estes conteúdos permitem atingir o objetivo enunciado.

3. Conhecer os elementos de apoio ao planeamento de Sistemas Informáticos e à Auditoria Informática.

- Parte 3 – Governança e Gestão da Cibersegurança – estes conteúdos permitem atingir o objetivo enunciado.

(English)

Correspondence of objectives with syllabus contents:

1. Have a holistic view of the main security problems faced by organizations' Information Systems.

- “Part 1 – Fundamentals of Cybersecurity” – these contents allow achieving the stated objective.

2. Mastering the means and techniques to face IS security and cybersecurity issues

“Part 2 – Good operational practices in Cybersecurity” – these contents allow achieving the stated objective.

3. Know the elements to support the planning of IT Systems and IT Audit.

“Part 3 – Governance and Management of Cybersecurity” – these contents allow achieving the stated objective.

METODOLOGIAS DE ENSINO E AVALIAÇÃO / TEACHING METHODOLOGIES INCLUDING EVALUATION

De acordo com o Regulamento de Funcionamento do ISTEC Porto a avaliação é efetuada através de um exame final obrigatório. Na classificação final, poderão ser considerados elementos de avaliação contínua, tais como testes, trabalhos individuais ou em grupo, assim como a participação nas aulas presenciais e com recursos de aprendizagem proporcionados por sistemas de e-learning. O estudante que realize os trabalhos práticos propostos nas aulas e nas condições aprovadas, poderá prescindir da realização da Prova prática final.

Nas aulas práticas, os estudantes têm de desenvolver projetos onde utilizam as técnicas de Cibersegurança aprendidas, sendo incentivados a estudar aplicações específicas da Cibersegurança atual e olhar para técnicas e tecnologias emergentes neste domínio.

(English)

In accordance with ISTEC Porto's Operating Regulations, assessment is carried out through a mandatory final exam. In the final classification, elements of continuous assessment may be considered, such as tests, individual or group work, as well as participation in face-to-face classes and with learning resources provided by e-learning systems.

The student who carries out the practical work proposed in the classes and under the approved conditions, may waive the final practical test.

In practical classes, students have to develop projects where they use the Cybersecurity techniques learned, where they are encouraged to study specific applications of current Cybersecurity and look at emerging techniques and technologies in this field.

DEMONSTRAÇÃO DA COERÊNCIA DAS METODOLOGIAS DE ENSINO COM OS OBJETIVOS DA UNIDADE CURRICULAR / DEMONSTRATION OF THE COHERENCE BETWEEN THE TEACHING METHODOLOGIES AND THE LEARNING OUTCOMES

Correspondência dos objetivos com metodologias:

1. Ter uma visão holística dos principais problemas de segurança que se colocam aos Sistemas de Informação das organizações.

- Os trabalhos de grupo / individuais, focam os temas principais dos conteúdos programáticos, que por sua vez estão alinhados com os objetivos da Unidade Curricular. Não é possível realizar os trabalhos nos temas propostos sem uma compreensão holística da Cibersegurança. A prova teórica final, versa os referidos temas pelo que o objetivo 1 é também cumprido.

2. Dominar os meios e técnicas para enfrentar os problemas de segurança e Cibersegurança nos SI

- Os trabalhos de grupo / individuais, obrigam à compreensão e utilização dos meios e técnicas para enfrentar os problemas de segurança e Cibersegurança, pelo que estão alinhados com os objetivos da Unidade Curricular. Não é possível realizar os trabalhos nos temas propostos sem o domínio dos meios e técnicas referidos. A prova teórica final, versa os referidos meios e técnicas, pelo que o objetivo 2 é também cumprido.

3. Conhecer os elementos de apoio ao planeamento de Sistemas Informáticos e à Auditoria Informática.

- Os trabalhos de grupo / individuais, obrigam à compreensão e utilização dos elementos de apoio ao planeamento de Sistemas Informáticos e à Auditoria Informática, pelo que estão alinhados com os objetivos da Unidade Curricular. Não é possível realizar os trabalhos nos temas propostos sem o domínio dos elementos referidos. A prova teórica final, versa os referidos elementos e técnicas, pelo que o objetivo 3 é também cumprido.

(English)

Correspondence of objectives with methodologies:

1. Have a holistic view of the main security problems faced by organizations' Information Systems.

- Group/individual projects focuses on the main themes of the syllabus, which are in line with the objectives of the Curricular Unit. It is not possible to carry out work on the proposed topics without a holistic understanding of Cybersecurity. The final theoretical test deals with the aforementioned topics, so objective 1 is also fulfilled.

2. Mastering the means and techniques to face IS security and cybersecurity issues

- Group/individual projects require understanding and use of means and techniques to address security and cybersecurity issues, so they are in line with the objectives of the Curricular Unit. It is not possible to carry out work on the proposed themes without mastering the aforementioned means and techniques. The final theoretical test deals with the aforementioned means and techniques, so objective 2 is also fulfilled.

3. Know the elements to support the planning of IT Systems and IT Audit.

- The group/individual projects require the understanding and use of elements to support the planning of IT Systems and IT Auditing, so they are aligned with the objectives of the Curricular Unit. It is not possible to carry out work on the proposed themes without mastering the aforementioned elements. The final theoretical test deals with the aforementioned elements and techniques, so objective 3 is also fulfilled.

BIBLIOGRAFIA / BIBLIOGRAPHY

FUNDAMENTAL/ ESSENTIAL:

Antunes, M., Rodrigues B. (2018). *Introdução à Cibersegurança*. FCA.

Carneiro, A. (2018). *Introdução à Segurança dos Sistemas de Informação*. FCA.

COMPLEMENTAR/ COMPLEMENTARY:

Bruce, G. & Dempsy, R. (1997). *Security in Distributed Computing*. Hewllett Packard Professional Books.

Stallings, W. (2006). *Cryptography and Network Security*. Prentice Hall.

Fitzgerald, J. & Dennis A. (1996). *Business Data Communications and Networking*. John Wiley & Sons.

Davis, C., Schiller, M. & Wheeler, K. (2007). *IT Auditing - Using controls to protect information assets*. McGraw Hill.

Sanson, M. & Guttman, B. (1996). *Generally accepted principles and practices for securing IT systems*. National Institute of Standards and Technology, US Department of Commerce.

Derrien, Y. (1992). *Les techniques de l'audite informatique*. Editions Dunod.

Gil, A. L. (2011). *Auditoria de computadores*. Editora Atlas.

INTERNET:

Acesso a publicações da especialidade, gratuitamente, através da rede SPRINGER:

https://link.springer.com/