Escola Superior de Tecnologia e Gestão
Descritor de Unidade Curricular

Nível de ciclo de estudos:
Mestrado
Curso:
Engenharia de Segurança Informática

Unidade Curricular: **1989112 – Segurança Organizacional**

Ano 2 **Trimestre 1** **Área CNAEF: 481** **ECTS: 4**

Tipo de Unidade Curricular: Obrigatória **Modo de Ensino:** Presencial **Língua de Trabalho:** Português

DOCENTE RESPONSÁVEL: José Carlos Lourenço Martins

TEMPO DE TRABALHO DO ESTUDANTE EM HORAS

HORAS TOTAIS	**Horas de Contacto**								**Horas de Trabalho Autónomo**
	Ensino teórico (T)	Ensino teórico-prático (TP)	Ensino prático e laboratorial (PL)	Trabalho de campo (TC)	Seminário (S)	Estágio (E)	Orientação tutorial (OT)	Outra (O)	
100		**15**	**15**						**70**

Pré-requisitos (se aplicável):

OBJETIVOS EDUCACIONAIS / RESULTADOS DE APRENDIZAGEM

(1) Explicar os principais conceitos utilizados no âmbito da Segurança da Informação (SegInfo).
(2) Explicar algumas das principais ameaças físicas a uma Organização.
(3) Explicar algumas das principais ameaças de Engenharia Social.
(4) Explicar algumas das principais ameaças à infraestrutura tecnológica.
(5) Modelar cenários de ameaças / métodos de ataque de um adversário.
(6) Identificar alguns dos principais problemas de Segurança da Informação.
(7) Identificar e explicar as principais abordagens de Segurança da Informação.
(8) Identificar as principais dimensões e controlos de Segurança da Informação.
(9) Saber realizar uma identificação e avaliação de riscos de Segurança da Informação.
(10) Design de processos, planos, políticas e procedimentos de Segurança da Informação.
(11) Saber como elaborar um plano de auditorias de Segurança da Informação.
(12) Saber como planear a implementação de um Sistema de Gestão de SegInfo.

CONTEÚDOS PROGRAMÁTICOS

1. Explicar algumas das principais técnicas para analisar a estrutura de uma Organização
2. Modelar métodos de ataque e caraterizar ações maliciosas
3. Identificar e explicar as principais abordagens de SegInfo ao nível das organizacões
4. Identificar alguns dos principais problemas de SegInfo e Cibersegurança
5. Identificar e analisar algumas das principais normas internacionais de gestão de riscos de SegInfo
6. Explicar como realizar o design de uma política de SegInfo e de um processo de gestão de incidentes
7. Explicar algumas das principais ameaças físicas e identificar os principais controlos a implementar
8. Explicar algumas das principais ameaças de Engenharia Social e identificar os principais controlos a implementar
9. Explicar algumas das principais ameaças tecnológicas e identificar os principais controlos a implementar

10. Elaborar um plano de auditoria de SegInfo e descrição da implementação de um Sistema de Gestão de SegInfo

DEMONSTRAÇÃO DA COERÊNCIA DOS CONTEÚDOS PROGRAMÁTICOS COM OS OBJETIVOS DE APRENDIZAGEM

Objectivo 1, conteúdo programático 1.

Objectivo 2, conteúdos programáticos 2 e 7.

Objectivo 3, conteúdos programáticos 2 e 8.

Objectivo 4, conteúdos programáticos 2 e 9.

Objectivo 5, conteúdos programáticos 2, 7, 8 e 9.

Objectivo 6, conteúdos programáticos 4, 7, 8 e 9.

Objectivo 7, conteúdo programático 3.

Objectivo 8, conteúdos programáticos 4, 7, 8 e 9.

Objectivo 9, conteúdo programático 5.

Objectivo 10, conteúdo programático 6.

Objectivo 11, conteúdo programático 10.

Objectivo 12, conteúdo programático 10.

MÉTODOS DE ENSINO E APRENDIZAGEM

(1) O ensino tem uma orientação essencialmente prática, com o recurso sempre que pertinente ao estudo de casos reais e em cuja discussão será solicitada a participação dos discentes.

(2) Sessões teóricas – práticas com a duração de três horas.

(3) Exposição teórica complementada com a realização de trabalhos práticos e leitura de artigos académicos.

(4) O ensino baseia-se fundamentalmente: (i) no método pedagógico expositivo e demonstrativo; (ii) em casos de estudo; (iii) e na discussão em grupo, como técnicas pedagógicas.

DEMONSTRAÇÃO DA COERÊNCIA DAS METODOLOGIAS DE ENSINO COM OS OBJETIVOS DAS APRENDIZAGENS*

Utilizam-se métodos expositivos para desenvolver os assuntos teóricos.

No caso da implementação de tecnologias de segurança, utilizam-se métodos demonstrativos.

Em ambos os métodos se utilizam perguntas de controlo para auxiliar o discente a descobrir a solução e a mais facilmente identificar uma possível solução para o problema proposto.

As técnicas mais utilizadas são a discussão de grupo (e.g., escolher os melhores controlos de segurança a implementar para mitigar um risco), a simulação (e.g., identificar cenários de incidentes de segurança da informação) e por fim os Casos de Estudo (e.g., análise do ciberataque à Estónia em 2007).

MÉTODOS DE AVALIAÇÃO

(1) A avaliação é composta por uma componente prática, constituída no mínimo por dois trabalhos de investigação aplicada, de reduzida dimensão e por uma componente teórica constituída pela realização de uma prova de avaliação.

(2) O peso na nota final de cada uma das componentes é definido no início de cada semestre de funcionamento da Unidade Curricular, sendo no mínimo de 40% a avaliação da componente prática.

BIBLIOGRAFIA PRINCIPAL

[1] Pfleeger and Pfleeger (2007). Security in Computing (4th ed.). New Jersey: Prentice Hall.

[2] Smith, Richard (2013). Elementary Information Security, Jones and Bartlett Learning.

[3] Whitman, Michael and Herbert, Mattord (2012). Principles of Information Security (4a ed), Cengage Learning.

[4] ISO/IEC 27001, 27005, 27032, 27035 e 310008.

[5] Finne, T. (1998). A Conceptual Framework for Information Security Management. Computers & Security, 17(4), 303-307.

[6] Martins and Santos (2010). Methods of Organizational Information Security - A Literature Review. Paper presented at the 6th International Conference on Global Security, Safety and Sustainability, Braga.

[7] Martins, Santos, Nunes e Silva (2012a). Framework de Gestão de Segurança da Informação para Organizações Militares Orientada pelos Principais Vetores de Ataque. Paper presented at the Associação Portuguesa de Sistemas de Informação, Universidade do Minho, Guimarães, Portugal.

Ano letivo de entrada em vigor: 2018/2019 | Data de aprovação em Conselho Técnico-Científico: