Informação Geral:

Unidade Orgânica	Escola Superior de Tecnologia e Gestão	**Ano Letivo**	2015/2016
Curso	Licenciatura em Engenharia Informática	**Grau**	Licenciatura
UC/Módulo	Segurança da Informação	**ECTS**	6
Área Científica	Engenharia Informática - Sistemas de Informação	**Carácter**	Obrigatório

Horas Totais	162	**T**	30	**TP**	0	**PL**	45	**TC**	0	**S**	0	**E**	0	**OT**	0

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutorial

Docente responsável:

Vitor Manuel Basto Fernandes

Docentes que lecionam a unidade curricular:

Vitor Manuel Basto Fernandes (108,00 horas semanais de contacto: T: 30,00; PL: 45,00; T: 30,00; PL: 3,00;)

Rui Miguel Bragança Ferreira (135,00 horas semanais de contacto: PL: 45,00; PL: 45,00; PL: 45,00;)

Pré-requisitos:

Nenhum.

Idioma:

Português e Inglês

Enquadramento:

Esta unidade curricular, enquadrada no ramo de Sistemas de Informação do curso de Licenciatura em Engenharia Informática, proporciona ao estudante a aquisição de competências na área da segurança da informação.

Esta UC permite ainda ao estudante a aquisição de conhecimentos e técnicas específicas de segurança para desenvolvimento de software, permitindo-lhe desenvolver as suas competências para construir código seguro e para analisar código já desenvolvido.

Objetivos de aprendizagem:

Gerais:

C1) Obtenção de conhecimentos essenciais e de noções básicas sobre os principais mecanismos e tecnologias de segurança;

C2) Obtenção de conhecimento do funcionamento dos algoritmos e protocolos de segurança mais relevantes.

Específicos:

C3) Desenvolvimento de capacidades técnicas necessárias para o desenvolvimento de código seguro em sistemas de informação organizacionais;

C4) Realização de julgamento/tomada de decisões ao nível da segurança, para a conceção e implementação de

sistemas distribuídos seguros;

C5) Aquisição de capacidades para realizar tarefas de teste, monitorização e auditoria de segurança em software.

Transversais:

C6) Capacidade de trabalhar em equipa

C7) Capacidade de realizar projetos

Programa:

Conteúdos Programáticos:

1 - Introdução à Segurança da Informação

2 - Introdução à Criptografia

3 - Modos de Cifragem Simétrica

4 - Algoritmos Simétricos

5 - Comprimentos de Chaves

6 - Criptografia Assimetrica - O caso do RSA

7 - Funções de Hash

8 - MACs e Estabelecimento de Chaves

9 - SSL e TLS

10 - Email Seguro - PGP e GPG

11 - CACert e SMIME

12 - O Cartão do Cidadão Português

Fundamentação da coerência dos conteúdos programáticos com os objetivos/competências da unidade curricular:

1 - Introdução à Segurança da Informação (C1, C2)

2 - Introdução à Criptografia (C1)

3 - Modos de Cifragem Simétrica (C1, C2)

4 - Algoritmos Simétricos (C1, C2, C4, C5)

5 - Comprimentos de Chaves (C4, C5)

6 - Critpgrafia Assimétrica - O caso do RSA (C1, C2, C4, C5)

7 - Funções de Hash (C1, C2, C4,C5)

8 - MACs e Estabelecimento de Chaves (C1, C2, C4, C5)

9 - SSL e TLS (C1, C2, C3, C4, C5)

10 - Email Seguro - PGP e GPG (C1, C2, C3, C5)

11 - SMIME e CACERT (C1, C2, C3)

12 - O Cartão de Cidadão Português (C1, C2, C3, C6, C7)

Metodologia de Ensino / Aprendizagem:

Presencial:

Ensino teórico:

Esta metodologia privilegia a apresentação pelo professor dos conteúdos programáticos e a sua assimilação por parte dos estudantes.

Ensino prático e laboratorial:

Esta metodologia assenta na realização de trabalhos que correspondem à consolidação dos conhecimentos teóricos abordados e na resolução de problemas reais .

Autónoma:

1. Estudo

1.1 Leitura da bibliografia proposta para a unidade curricular

1.2 Resolução/revisão dos desafios colocados na aula

2. E-aprendizagem

2.1 Consulta de material relativo à unidade curricular

Recursos Específicos:

Laboratório de Sistemas de Informação

Plataforma de gestão e distribuição de conteúdos

Software específico: Windows, Visual Studio, .Net, Browsers

Elementos de apoio disponibilizados pelos docentes

Avaliação:

Descrição:

Avaliação periódica

Os resultados de aprendizagem são avaliados através de uma prova teórica escrita individual (PE) complementada por um trabalho de pesquisa teórico com entrega de relatório (RTP) e uma apresentação dos resultados do trabalho de pesquisa (ATP), destinados a avaliar as competências C1, C2, C4, C5 e um projeto prático, destinado a avaliar as competências C3, C4, C5, C6 e C7, com os seguintes pesos:

a) Prova teórica escrita 35% (PE) + 7.5% Trabalho de pesquisa teórico com entrega de relatório (RTP) + 7.5% Apresentação dos resultados do trabalho de pesquisa (ATP)
b) Projeto laboratorial: 50%

Mínimos obrigatórios de 9,5 valores a todas e cada uma das componentes, PE, RTP e ATP.

Avaliação por exame

Os resultados de aprendizagem são avaliados através de prova escrita individual destinada a avaliar as competências C1, C2,

C4 e C5 e num exame prático, destinado a avaliar as competências C3, C4, C5 e C7 com os seguintes pesos:

a) Prova escrita: 50%

b) Projeto laboratorial: 50%

Mínimos obrigatórios de 9,5 valores em cada uma das componentes

Caso o estudante tenha obtido avaliação positiva apenas a uma das componentes da avaliação (componente teórica ou componente prática) poderá optar por submeter-se a avaliação apenas à outra componente de avaliação em que não obteve aproveitamento, durante todas as épocas de exame do mesmo ano letivo.
Não se preservam notas de componentes da avaliação entre anos letivos diferentes.

Número de elementos de avaliação final:	2
Número de elementos de avaliação contínua/periódica:	3

Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:

Ensino teórico:

Esta metodologia privilegia a apresentação pelo professor dos conteúdos programáticos e a sua assimilação por parte dos estudantes.(C1, C2, C3, C4, C5)

Ensino prático e laboratorial:

Esta metodologia assenta na realização de trabalhos que correspondem à consolidação dos conhecimentos teóricos abordados e na resolução de problemas reais. (C3, C4, C5, C6, C7)

Orientação tutorial:

Esta metodologia baseia-se em sessões de orientação pessoal, de pequenos grupos ou em sala de aula, para conduzir o processo de aprendizagem, nomeadamente orientar o trabalho individual do estudante e esclarecer dúvidas.(C1, C2, C3, C4, C5)

Bibliografia:

Recomendada:

Bruce Schneier, “Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth)”, John Wiley & Sons, Inc., 1996.

William Stallings, “Cryptography and Network Security Principles and Practices, Fourth Edition”, Prentice Hall, 2005.

Stephen A Thomas, "SSL & TLS Essentials: Securing the Web", 2009

C. Paar and J. Pelzl, “Understanding Cryptography: A Textbook for Students and Practitioners”, Springer, 2010.

Complementar:

Rivest, R., Shamir, A., Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Volume 21, Number 2, February 1978.

Matt Bishop, Introduction to Computer Security, Addison-Wesley, 2005.