CURSO	Licenciatura em Informática		
UNIDADE CURRICULAR	Segurança Informática	Obrigatória	X
		Opcional	
ÁREA CIENTÍFICA	Engenharia Informática		

Ano: 3º	Semestre: 2º	ECTS: 4	Horas de Contacto teórico práticas: 60h

OBJETIVOS DA APRENDIZAGEM

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

1. Compreender os conceitos fundamentais da segurança digital;
2. Compreender e saber implementar procedimentos gerais e específicos relacionados com a gestão da informação e de proteção de operações críticas;
3. Compreender e saber implementar os standards e as práticas de segurança;
4. Compreender e saber definir e implementar políticas de segurança, privacidade e gestão de acessos;
5. Compreender as alternativas de segurança em cloud computing;
6. Compreender os mecanismos de segurança física e as técnicas biométricas de proteção da informação digital;
7. Saber implementar políticas e mecanismos de proteção de identidade online e prevenção e deteção de intrusões;
8. Saber utilizar instrumentos de análise de packets em redes de computadores;
9. Compreender as potencialidades e as formas de utilização de firewalls;
10. Compreender e saber implementar sistemas de segurança para proteção de infraestruturas e prevenção e deteção de crimes ataques cibernéticos.

PROGRAMA

1. Introdução à segurança de sistemas e redes de computadores
2. Gestão da segurança da informação e planos de recuperação
3. Standards e políticas de segurança
4. Privacidade, segurança e gestão de acessos
5. Segurança em sistemas de cloud computing
6. Segurança física
7. Segurança biométrica
8. Identidade online e gestão de utilizadores
9. Prevenção e deteção de intrusões
10. Análise das comunicações em rede
11. Firewalls: desenho e configuração
12. Segurança de infraestruturas
13. Cyber crime e cyber warfare

DEMONSTRAÇÃO DE COERÊNCIA ENTRE CONTEÚDOS PROGRAMÁTICOS E RESULTADOS DA APRENDIZAGEM

O objetivo 1 é concretizado no ponto 1 do programa. O ponto 2 permite atingir o objetivo 2. O objetivo 3 é concretizado através do ponto 3. O ponto 4 permite concretizar o objetivo 4. O objetivo 5 é concretizado através o ponto 5 do programa. Os pontos 6 e 7 permitem concretizar o objetivo 6. O objetivo 7 é concretizado através dos pontos 8 e 9. O ponto 10 permite concretizar o objetivo 8. O objetivo 9 é concretizado através do ponto 11. Os pontos 12 e 13 permitem concretizar o objetivo 10.

METODOLOGIA DE ENSINO E AVALIAÇÃO

Estão previstas 60 horas de contato. O tempo total de trabalho do aluno corresponde a 108 horas. A metodologia baseia-se em exposições teóricas para apresentação dos conceitos científicos e em aplicações práticas utilizando plataformas de software de simulação e previsão.

De acordo com o Regulamento de Funcionamento do ISTEC a avaliação é efetuada através de um exame escrito individual e 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 em recursos de aprendizagem proporcionados por sistemas de e-learning.

DEMONSTRAÇÃO DE COERÊNCIA ENTRE METODOLOGIAS DE ENSINO E RESULTADOS DE APRENDIZAGEM

A unidade curricular visa proporcionar aos alunos uma visão compreensiva e integradora das questões relacionadas com a segurança digital, com exceção das matérias relacionadas com a criptografia que são abordadas numa unidade curricular própria (Criptografia). A metodologia expositiva, com recurso a aplicações práticas é considerada adequada face aos objetivos definidos para a unidade curricular.

BIBLIOGRAFIA

Fundamental:

Vacca, John R., Computer and Information Security Handbook, 3rd Edition (2017), Morgan Kaufmann

Complementar:

Death, Darren, Information Security Handbook (2017), Packt Publishing

INTERNET:

Acesso a publicações da especialidade, gratuitamente, através da rede SPRINGER: https://link.springer.com/