Escola Superior de Tecnologia de Tomar **Ano letivo:** 2019/2020

Engenharia Informática
Licenciatura, 1º Ciclo
Plano: Despacho n.º16228/2009 - 15/07/2009

Ficha da Unidade Curricular: Gestão e Segurança de Redes Informáticas
ECTS: 6; Horas - Totais: 165.0, Contacto e Tipologia, TP:28.0; PL:42.0; OT:5.0; O:5.0;
Ano | Semestre: 3 | S1
Tipo: Obrigatória; Interação: Presencial; Código: 911924
Área Científica: Arquitectura de Computadores e Redes

Docente Responsável
Luís Miguel Lopes de Oliveira
Professor Adjunto

Docente(s)
Luís Miguel Lopes de Oliveira
Professor Adjunto
Renato Eduardo Silva Panda
Professor Adjunto Convidado

Objetivos de Aprendizagem

Aplicar as boas práticas da gestão e manutenção de redes informáticas.
Identificar os serviços críticos de uma infraestrutura, propondo soluções e estratégias que minimizem a sua inoperacionalidade;
Concretizar políticas de segurança recorrendo aos mecanismos mais adequados.

Objetivos de Aprendizagem (detalhado)

1. Conhecer e saber aplicar as boas práticas da gestão e manutenção de redes informáticas.
2. Identificar as principais ameaças à integridade, disponibilidade e confidencialidade de um serviço.
3. Identificar as principais técnicas criptográficas e os seus contributos na garantia da confidencialidade e integridade.
4. Relacionar os principais ataques à segurança com os mecanismos de protecção mais

adequados para os mitigar.
5. Identificar as principais limitações dos mecanismos de segurança.
6. Implementar soluções de segurança adequadas ao risco dos recursos a proteger.

Conteúdos Programáticos

Gestão de redes e sistemas informáticos.
1. Introdução à Gestão Integrada
2. Modelos de gestão
Segurança em redes informáticas
3. Princípios de criptografia computacional
4. Sistemas de autenticação, certificação e controlo de acessos
5. Firewalls e sistemas de detecção de intrusão
6. Segurança em redes Wireless 802.11.
7. Mecanismos de Network Access Control.

Conteúdos Programáticos (detalhado)

Gestão de redes e sistemas informáticos.
1.Introdução à Gestão Integrada
1.1. Modelo Funcional
1.2. Modelo Arquitetural
1.3. Modelo de Informação
1.4. Modelo Relacional
1.5. Modelo de Gestão IETF
1.6. SNMP
Segurança em redes informáticas
2. Conceitos básicos relacionados com a segurança
3. Princípios de criptografia computacional
3.1. Princípio de Kerckhoffs
3.2. Operações de substituição e transposição
3.3. Cifras de blocos
3.4. Cifras sequênciais
3.5. O DES e o AES - casos de estudo
3.6. Gestão de chaves
3.7. Criptografia de chave assimétrica
3.8. Criptografia de chave híbrida
3.9. O TLS
4. Mecanismos de garantia de integridade
4.1. Funções de Hash
4.2. Message Authentication Codes
5. Mecanismos de garantia de autenticidade
5.1. Autenticação de fator único e com múltiplos fatores
5.2. Assinaturas digitais
6. Firewalls e sistemas de detecção de intrusão
6.1. Tipos de firewalls
4.2. Mecanismos de deteção de intrusões

5. Segurança em redes Wireless 802.11.
5.2. WPA 2 - caso de estudo
6. Mecanismos de Network Access Control.
6.1. Mecanismos NAC
6.2. Mecanimos MDA

Metodologias de avaliação

A avaliação é composta por duas componentes:

. Componente teórica com o peso de 60% na nota final e com a nota mínima de 7 valores.
. Componente prática com o peso de 40% na nota final e com a nota mínima de 10 valores.

A avaliação da componente teórica é composta pela classificação de uma prova escrita realizada individualmente e sem consulta.
A avaliação da componente prática corresponde à média da classificação dos trabalhos práticos realizados durante as aulas práticas laboratoriais. Os trabalhos laboratotiais podem ser realizados individualmente ou em grupos de dois alunos.
Estas regras aplicam-se a todas as épocas de avaliação.

Software utilizado em aula

Não aplicável

Estágio

Não aplicável

Bibliografia recomendada

- Boavida, F. e Monteiro, E. (2000). *Engenharia de Redes Informáticas* Lisboa: FCA - Editora de Informática
- William, S. (1998). *Cryptography and Network Security: Principles and Practice* .: Prentice-Hall
- William, S. (2000). *Network Security Essentials* .: Prentice-Hall
- Zúquete, A. (2006). *Segurança em Redes Informáticas* Lisboa: FCA - Editora de Informática

Coerência dos conteúdos programáticos com os objetivos

Objetivo 1: 1,2
Objetivo 2: 2
Objetivo 3: 2,3,45
Objetivo 4: 2,3,4,5
Objetivo 5: 2,3,4,5,6
Objetivo 6: 3,4,5,6

Metodologias de ensino

Aulas teórico-práticas com possibilidade de ensino à distância onde são estudados fundamentos teóricos desta UC. Aulas laboratoriais onde se simulam problemas que ocorrem em ambientes de produção

Coerência das metodologias de ensino com os objetivos

Língua de ensino

Português

Pré-requisitos

Não aplicável

Programas Opcionais recomendados

Não aplicável

Observações

Docente responsável

Luís Miguel Lopes de oliveira

Digitally signed by Luís Miguel Lopes de oliveira
Date: 2020.09.15 09:00:25 +01'00'