INSTITUTO SUPERIOR DE TECNOLOGIAS AVANÇADAS

CTeSP | Curso Técnico Superior Profissional
Redes e Sistemas Informáticos

Unidade Curricular
Políticas de Segurança

Objetivos

- Definir e analisar as exigências de segurança de um sistema informático;
- Implementar uma estratégia de segurança para uma arquitetura cliente/servidor.

Objetivos Específicos

- Compreender os conceitos fundamentais de criptografia;
- Conhecer os principais algoritmos criptográficos;
- Distinguir entre criptografia simétrica e assimétrica;
- Compreender o papel de entidades de certificação;
- Compreender a noção de domínio como limite de aplicação de regras de segurança;
- Compreender e implementar os diferentes tipos de autenticação de rede;
- Definir políticas de controlo de acessos;
- Implementar sistemas de proteção de dados;
- Planear e implementar sistemas de cópias de segurança;
- Estabelecer e manter mecanismos de transmissão segura de dados através da Internet para a criação de VPNs;
- Implementar mecanismos de proteção de ameaças externas;
- Planeamento, implementação de políticas de segurança em organizações.

Caraterização da Unidade Curricular

1º Ano
2º Semestre
Enquadramento: obrigatória
Créditos: 6 ECTS

Avaliação

Independentemente de se poderem considerar elementos de avaliação continua, a avaliação é individual e realizada através de um exame escrito presencial obrigatório.

Programa

1. Noção de domínio e limites de políticas de segurança

2. Criptografia de chave pública e privada
2.1. Criptografia de chave pública/privada/combinadas
2.2. Chaves criptográficas e certificados

3. Autenticação de utilizadores
3.1. Autenticação de utilizador de computador local
3.2. Autenticação de utilizador na rede (processos de autenticação)
3.3. Autenticação de certificados

4. Configuração e administração da Ative Directory
4.1. Criação / manutenção de unidades organizacionais

5. Controlo de acesso
5.1. Conceito de propriedade (proprietário)
5.2. Contas de utilizadores
5.3. Grupos
5.4. Permissões

6. Proteção de dados armazenados
6.1. Criptografia de ficheiros e diretórios (pastas)
6.2. O processo de criptografia / Considerações
6.3. Codificação de diretórios e ficheiros

7. Proteção da transmissão de dados
7.1. Implementação de transmissão segura de dados: Internet / LAN
7.2. O processo IPSec, configuração

8. Planificação para a implementação da segurança

9. Cópias de segurança

10. Ameaças externas

Bibliografia

1. William Stalling, Cryptography and Network Security: Principles and Practice, Pearson 2014
2. Thomas Shinder, Windows Server 2012 Security from End to Edge and Beyond: Architecting, Designing, Planning, and Deploying Windows Server 2012 Security Solutions, SynGress 2015
3. Niels Ferguson e outros, Cryptography Engineering: Design Principles and Practical Applications, Willey 2010