CRIPTOGRAFIA E SEGURANÇA INFORMÁTICA

Licenciatura em Engenharia de Sistemas Informáticos

Licenciatura em Engenharia de Sistemas Informáticos (pós-laboral)

Código: 11302

Área Cientifica Predominante: Sistemas e Tecnologias de Informação

Docente: Paulo Adriano Marques Sousa Teixeira

Idioma de Instrução: Português

Regime: S1

Carga Letiva: 60h Carga Trabalho: 100h

ECTS: 6,0

Objetivos

Nesta unidade curricular pretende-se sensibilizar os alunos para a importância da segurança dos sistemas deinformação, dada a crescente dependência das organizações no desempenho dos seus SI nas suas operaçõesdiárias. A unidade curricular irá focar a necessidade de implementar e monitorar políticas de segurança e dosconhecimentos técnicos necessários para as implementar. Os conceitos serão abordados recorrendo a exemplospráticos.

Objetivos:

• Fornecer o conhecimento necessário para implementar, manter, e seguir um programa de segurança

• Sensibilizar para a importância da segurança de Sistemas de Informação numa organização

• Introduzir técnicas e metodologias

Resultados da Aprendizagem

Pretende-se que no decurso da disciplina os alunos:

•Conheçam as noções essenciais inerentes à Segurança dos Sistemas de Informação;

•Saibam definir e implementar um plano de segurança para os Sistemas de Informação;

•Conheçam as principais normas de segurança aplicadas a esta área do conhecimento.

•Saibam identificar e recorrer às principais organizações relacionadas com a segurança;

•Saibam fazer uma análise de risco que lhes permita elaborar e justificar políticas de segurança;

•Adquiram os conhecimentos necessários para fazerem auditorias de segurança a S.I.

•Conheçam os principais sistemas e algoritmos de criptografia.

O tema da Segurança de Sistemas e Tecnologias de Informação é desenvolvido na sua vertente prática

deaplicação às organizações.

São analisados os principais fatores de segurança, o desenvolvimento de planos de segurança, e estudados osprocedimentos de implementação dos mecanismos de segurança.

São estudadas técnicas atuais de criptografia, a implementação de mecanismos criptográficos e a utilização deprocessos de criptoanálise.

Conteúdos Programáticos

1. Segurança dos Sistemas de Informação

1.1. Motivação para a Segurança dos Sistemas de Informação

1.2. Classificação dos recursos de uma Organização

1.3. Evento de segurança

1.4. Incidente de segurança

1.5. Propriedades da Informação

1.6. Ameaças aos Sistemas de Informação

1.7. Ataques

1.8. Medidas de controlo

1.9. Framework para a Segurança da Informação baseado no sistema COBRA (implementa a norma BS7799)

2. Normas de Segurança

2.1. Família de normas ISO 27000

2.2. Família de normas NIST-800

3. Organizações Relacionadas com Segurança

3.1. CERT/CC

3.2. ISACA

3.3. NIST

3.4. SANS

4. Política de Segurança

4.1. Estrutura de Planos de Segurança

4.2. Plano de Recuperação

4.3. Plano de Reposição

4.4. Plano de Contingência

5. Análise de Risco

5.1. Gestão de Risco (Modelo PDCA) vs Análise de Risco

5.2. Metodologia da Análise de Risco – ISO 27005

5.3. Análise Custo/Benefício

5.3.1. Framework de Análise de Risco - OCTAVE

6. Auditoria à Segurança dos Sistemas de Informação

6.1. Auditoria Preventiva

6.2. Auditoria Reativa

6.3. Framework de auditoria - COBIT

7. Criptografia

7.1. Introdução às Técnicas Criptográficas

7.2. Algoritmos de Cifra Simétrica

7.3. Algoritmos de Cifra Assimétrica

7.4. Certificados Digitais

7.5. Assinaturas Digitais

7.6. Protocolos de Acordo de Chaves

7.7. O Protocolo SSL (Secure Socket Layer) e TLS

Bibliografia Recomendada

Whitman, M. E., Mattord, H. J. (2012). Principles of information security (4th ed.). Boston, MA: CourseTechnology.

Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. 2010. “Cryptography Engineering . Design Principles andPractical Applications.” Wiley Publishing, Inc.

Kim, David, and Michael Solomon. 2014. Fundamentals of Information Systems Security. Jones Bartlet Learning. 2ndEdition

Métodos de Ensino e de Aprendizagem

Mais do que transmitir conhecimentos no âmbito de uma abordagem teórica, pretende-se que os estudantesdesenvolvam a capacidade para desenvolver e auditar um programa de segurança de STI em ambienteorganizacional, desenvolvendo para isso trabalhos práticos de desenvolvimento de planos de segurança ou deauditoria a sistemas. Pretende-se que os conhecimentos transmitidos sobre a evolução da criptografia permita queos alunos saibam adotar os procedimentos criptográficos adequados a cada situação e consigam anteverevoluções na criptografia que devem acompanhar para assegurar a segurança dos sistemas sob suaresponsabilidade.

No seu conjunto, os conteúdos programáticos definidos, a variedade de literatura a sugerir (principal ecomplementar) cuja consulta se pretende dinamizar assim como os case studies a discutir, a metodologia deensino preconizada e o método de avaliação a seguir, estimulam o desenvolvimento do espírito crítico doestudante, da sua capacidade de agir em tempos de mudança e da sua capacidade de inovação e intervenção.

Métodos de Avaliação

O desempenho do aluno na disciplina será avaliado através de:

Uma componente teórica composta por um momento de avaliação a realizar no decurso do semestre letivo, cujadata será comunicada em aula com uma antecedência mínima de três semanas. A esta componente teóricacorresponderá uma ponderação de 50% na nota final;

A componente prática, é composta por um conjunto de atividades semanais, com uma ponderação de 20% nanota final, e por um trabalho de grupo que consiste na elaboração de um plano de segurança para uma instituiçãotipo sugerida pelo docente, ou, para uma outra instituição sugerida pelos alunos e sujeita a aprovação pelodocente. O trabalho final deverá ser entregue até ao último dia de aulas e consistirá num relatório e naapresentação do trabalho perante os outros elementos da turma. Juntamente com o relatório cada grupo deveráreferir a contribuição de cada elemento para o trabalho final;

A avaliação do aluno nas restantes épocas que não a normal, que inclui a época de recurso, especial e outrasprevistas no RIAPA, contemplará apenas o exame escrito ponderado com a nota da componente prática jáavaliada. Não será permitido entregar os trabalhos práticos fora do período definido na época normal. A nãorealização dos trabalhos práticos implicará a reprovação à unidade curricular.

Nota: O docente reserva-se o direito de exigir uma defesa individual quando a nota obtida em qualquer avaliação(teórica ou prática) for igual ou superior a quinze valores.

A nota final será o resultado da média ponderada em 50% para a componente teórica e 50% para a componenteprática. Para obter aprovação à disciplina um aluno necessita ter uma classificação igual ou superior a 9 valoresna componente teórica.