Seguridad TICs

Denominación de la materia: Seguridad TICs					
Módulo de 5 semanas	**Frecuencia de la oferta**	**Duración**	**Tipo**	**Puntos ECTS**	**Carga de trabajo de los estudiantes**
Un módulo de tres semanas	anual	3 semanas	Materia obligatoria	4 puntos ETCS	100 horas de carga de trabajo

Requisitos para la participación	**Aplicación**	**Tipo de evaluación/ Duración de la evaluación**	**Métodos de enseñanza y aprendizaje**	**Responsable del Módulo**
N/A.	Carrera: Tecnologías de la Información Empresarial.	Participación activa en clase (30%) Trabajo de grupo (30%) Examen escrito (40%)	• Clase interactiva • Ejercícios en classe • Retroalimentación • Trabajo grupal	Claus Kaldeich

Objetivos generales: Resultados de aprendizaje

El desarrollo de sistemas de software seguros constituye un desafío cada vez más importante y a la vez más difícil. Incluye tanto la aplicación de propiedades de seguridad deseadas (por ejemplo control de acceso) así como el impedimento de comportamientos no deseados (por ejemplo a través de la validación de inputs). En este módulo se establecen los fundamentos de la Seguridad IT se trabajan los conceptos elementales, métodos y técnicas en el área de la Seguridad IT en general.

Competencias académicas y metodológicas

Una vez culminado exitosamente este módulo

- Los estudiantes entienden los conceptos fundamentales de seguridad, métodos y técnicas,
- Conocen típicos puntos débiles importantes de los sistemas de seguridad actuales,
- Comprenden los fundamentos básicos de procedimientos criptográficos y algoritmos,
- Pueden captar y modelar los requerimientos de seguridad en sistemas informáticos,
- Pueden desarrollar politicas de secudidad de buena calidad,
- Están capacitados para analizar y evaluar la seguridad IT de sistemas informáticos.

Alineamiento constructivo

En el punto Alineamiento Constructivo se presenta, de qué manera los siguientes factores estarán sincronizados entre sí:

1. Los resultados de aprendizajes concretos esperados de este módulo, es decir, las competencias esperadas
2. Las formas concretas de evaluación definidas para este módulo
3. Los métodos de enseñanza y activación elegidos para este módulo

Contenido didáctico y metodología

Esta materia se concentra en las siguientes contenidos académicos:

- Conceptos fundamentales (confidencialidad, integridad, disponibilidad, no repudiación, amenazas, riesgos)
- Seguridad multilateral, seguridad en internet 8https, ...)
- Mecanismos de seguridad (control de intervención, control de acceso, autenticación, ...)
- Modelos de seguridad
- Principios de diseño/modelos (Bell-LaPadula, BIBA, MAC, DAC y otros)
- Fundamentos criptográficos
- 'Randomness', 'Passwords' y 'Entropy'
- 'Digital Signatures'
- Algoritmos de encriptación

Recomendaciones de literatura para la preparación y refuerzo

Li Shancang, Imed Romdhani, William Buchanan, "Password Pattern and Vulnerability Analysis for Web and Mobile Applications", School of Computing, Edinburgh Napier University, Edinburgh, Scotland, UK, http://www.cnki.net/kcms/detail/34.1294.TN.20160630.1830.002.html, June 30, 2016.

Umesh Hodeghatta Rao, Umesha Nayak, "The InfoSec Handbook An Introduction to Information Security", Apress Media, 2014.

Oded Goldreich, "Foundations of Cryptography - Basic Tools", Weizmann Institute of Science, □□□□□□□□□ □□□□□□□□□□ □□□□□, Cambridge, UK, 2006

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, "Security in Computing", 5th Ed., Pearson Press, 1996.

William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, McGraw-Hill, 2013.