Departamento de Ingeniería de Sistemas Informáticos y Telemáticos
Área de Ingeniería Telemática
Escuela Politécnica
Cáceres

Programa de la Asignatura

Seguridad y Protección de la Información

5º curso Ingeniería Informática

curso 2011-2012

CRÉDITOS: 6 (4'5+1'5). - Asignatura Optativa 1er Cuatrimestre.
HORARIO: 3 horas de teoría:
Lunes (9^{30}-10^{30} y 10^{30}-11^{30}) y Martes (10^{30}-11^{30}), Aula I.5
1 hora de prácticas:
Miércoles 11:30-12:30h (provisional), Lab. Sala Sun-I1.

PROFESORADO: **Lorenzo M. Martínez Bravo.**
(lorenzom@unex.es)

DESCRIPTORES:

Integridad, disponibilidad y confidencialidad de la información. Seguridad física y lógica. Criptografía. Seguridad en la transmisión de datos. Planes de recuperación.

OBJETIVOS:

La asignatura de *Seguridad y Protección de la Información* (SyPI) se encuentra enmarcada en el 2º ciclo de la Ingeniería Informática, con carácter optativo. Esta asignatura, pretende presentar al alumno toda la problemática relacionada con la seguridad de la información gestionada por medios automáticos. La importancia de la seguridad informática ha ido creciendo, y tomando peso, a medida que ha aumentado el número de usuarios, y sobre todo, el valor y la necesidad del tratamiento automatizado de la información. Hoy día, no es posible concebir el mundo en el que vivimos sin la existencia de los servicios informáticos, y la aplicación de éstos a todo tipo de situaciones reales en las que, en muchos casos, el valor de la información es muy alto, hace necesario la utilización de unos mecanismos de seguridad acordes a dicho valor.

En este sentido, cabe una mención especial a las redes de ordenadores, que permiten la circulación global de información a distintos ámbitos. Estos elementos, a la vez que han potenciado de forma impresionante el crecimiento de la informática, han introducido y han aumentado los peligros relacionados con la falta de seguridad, inherentes a cualquier sistema informático. Teniendo en cuenta todo lo mencionado, y las necesidades y posibilidades del entorno en el que nos encontramos, enunciamos los objetivos específicos de la asignatura:

- Definir el problema de la Seguridad Informática, y todas sus implicaciones actuales.
- Esbozar una metodología de análisis y solución de los problemas de Seguridad.

- Estudiar la criptografía, como principal mecanismo de control para la Seguridad.
- Analizar en detalle los problemas particulares de Seguridad que se presentan en las redes telemáticas.

CRITERIOS DE EVALUACIÓN:

Teoría y Práctica se evaluarán de forma separada.

La evaluación de la parte de teoría se realizará de forma continua a lo largo del cuatrimestre, en una serie de exámenes parciales que permitirán eliminar materia. Aquellos alumnos que no superen adecuadamente estos exámenes, deberán realizar el examen final de teoría en Febrero. Los alumnos que no superen la asignatura en Febrero podrán optar por un examen final, en Junio o en Septiembre.

La evaluación de la parte práctica se basará en la corrección y/o defensa de una serie de trabajos prácticos, que serán propuestos a lo largo del cuatrimestre.

La nota final de la asignatura se calculará según la expresión:

*Nota Final = Nota Teoría * 0'7 + Nota Práctica * 0'3*

teniendo en cuenta que sólo se aprobará la asignatura si (Nota Teoría >=4'5) y (Nota Práctica>=5).

Se tendrán en cuenta las siguientes consideraciones:

- En caso de aprobar la teoría y suspender la práctica, se guardará la nota de teoría hasta las convocatorias siguientes (Junio y Septiembre).
- La práctica aprobada se guardará de forma indefinida, mientras no se modifiquen las características de la misma.

PROGRAMA:

I. *Principios de Seguridad.*

Tema 1. El problema de la Seguridad Informática.
Tema 2. Problemas de seguridad en redes y soluciones.
Tema 3. Política de Seguridad.
Tema 4. Herramientas de seguridad no informáticas.

II. *Criptografía.*

Tema 5. Introducción a la Criptografía.
Tema 6. Criptografía de Clave Privada.
Tema 7. Criptografía de Clave Pública.
Tema 8. Cifrado contínuo.
Tema 9. Funciones Hash.
Tema 10. Esquemas y servicios de seguridad.

III *Seguridad en las Redes: Internet*

Tema 11. Seguridad perimetral.
Tema 12. Otras herramientas de seguridad.
Tema 14. Servicios en redes seguras.
Tema 15. Protocolos de Seguridad.
Tema 16. Comercio electrónico.

IV Apéndices.

Apéndice A. Criptografía clásica.

PRÁCTICAS:

- Utilización y análisis de algunas herramientas de seguridad.
- Estudio e implementación de algoritmos de cifrado de diversos tipos.
- Diseño y construcción de una aplicación con algoritmos de seguridad.

BIBLIOGRAFÍA BÁSICA:

Carracedo,04	Justo Carracedo Gallardo *"Seguridad en Redes Telemáticas"* McGraw-Hill, Madrid 2004
Pfleeger,89	Charles P. Pfleeger *"Security in Computing"* 2ª Edición, Prentice Hall International, Inc., 1997
Schneier,93	B. Schneier *"Applied Criptography"* John Weley & Sons Ltd., 1993 (Ba-2424)
Díaz,04	G. Díaz, F. Mur, E. Sancristóbal, M-A. Castro y J. Peire *"Seguridad en las Comunicaciones y en la Información"* UNED, 2004

Cáceres, 26 de Septiembre de 2011

Fdo: Lorenzo M. Martínez Bravo.