Asignatura: **SEGURIDAD INFORMÁTICA**	**Código**: 16908
	Tipo: OBLIGATORIA
Titulación I.T.I.G. (plan 2003)	**Curso**: 2º CURSO
Equipo docente: HERNANDO SILVA	**Duración:** 2 º CTRE.
Departamento: INFORMÁTICA Y AUTOMÁTICA	**Créditos (T+P):** 3+1,5
Área de conocimiento: LENGUAJES Y SISTEMAS OPERATIVOS	

OBJETIVOS:
Introducir al alumno al campo de la seguridad informática, las facetas que ésta presenta, los esquemas más comunes de protección de la información y protección del sistema, así como una breve semblanza de la seguridad en redes de comunicación.

OBSERVACIONES
Es conveniente que para la parte teórica de la asignatura el alumno tenga conocimientos de matemática discreta. Para la parte práctica, será conveniente disponer de conocimientos de programación, estructuras de datos, el lenguaje de programación C y desenvolverse bien en entornos Windows y Linux.

EVALUACIÓN
La evaluación de esta asignatura se llevará a cabo en dos apartados: teoría y prácticas. La nota final se obtiene sumando ambas partes dando a la teoría un peso de dos tercios y a la parte práctica un peso de un tercio. Para llevar a cabo esta operación tanto la parte teórica como la parte teórica deben tener una nota mínima de cuatro respecto a diez.
La nota de la parte teórica se obtiene mediante examen escrito en la cual el alumno responderá de manera breve y concisa a algunas preguntas, además de resolver algunos problemas planteados por el profesor.
La nota de la parte práctica se obtiene a partir de las prácticas que realiza el alumno. En cada práctica se le plantea al alumno un problema que debe resolver mediante el análisis, diseño e elaboración de uno o varios programas.
El alumno entregará, para cada práctica, los programas solicitados y un reporte (informe) en papel que describa y comente la solución que propone. El formato del informe, así como los enunciados de las prácticas, se podrán consultar en las páginas de hipertexto del profesor.

PROGRAMA DE TEORÍA
Tema 1: Introducción a la Seguridad Informática.

Tema 2: Sistemas de cifrado simétrico: criptografía de clave privada.

Tema 3: Sistemas de cifrado asimétrico: criptografía de clave pública.

Tema 4: Mecanismos de autentificación y firma digital.

Tema 5: Código dañino: virus, trampas, bombas lógicas, troyanos, gusanos, etc.

Tema 6: Seguridad en redes de comunicaciones.

PROGRAMA DE PRÁCTICAS
Práctica 1: Algoritmos elementales de cifrado.

Práctica 2: Algoritmos de cifrado de clave pública

Práctica 3: Algoritmos de intercambio de clave.

Práctica 4: Ataques por solución al problema del logaritmo discreto

Práctica 5: Ataques por factorización

Práctica 6: Detección y eliminación de virus informáticos

Práctica 7: Detección de intrusos.

BIBLIOGRAFÍA

STALLINGS, WILLIAM (2004),"Seguridad en Redes: aplicaciones y estándares", 2ª edición, Pearson – Prentice Hall.

STINSON, DOUGLAS R. (2002), "Criptography: theory and practice", Second edition, Chapman & Hall/CRC.

SCHNEIER, BRUCE (2001), "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2a. Edición, John Wiley.

PASTOR BLANCO, JOSÉ y SARASA LOPEZ, MIGUEL ÁNGEL (1998), "Criptografía Digital: Fundamentos y Aplicaciones", Prensas Universitarias de Zaragoza.