UNIVERSIDAD PONTIFICIA
ICAI ICADE
COMILLAS
MADRID

Seguridad Informática:
Programa de la asignatura

Titulación: Ingeniero en Informática
Curso 5º - Cuatrimestral (2006-2007)

Javier Jarauta Sánchez
Rafael Palacios Hielscher

Presentación

Presentación

Profesores:

- **Javier Jarauta (DSI)**
- **Rafael Palacios (DSI, IIT)**

Universidad Pontificia Comillas

Escuela Técnica Superior de Ingeniería ICAI

*Departamento de Sistemas Informáticos

*Instituto de Investigación Tecnológica

Página web de la asignatura:

`http://www.iit.upcomillas.es/palacios/seguridad/`

Objetivos de la Asignatura

Objetivos de la Asignatura

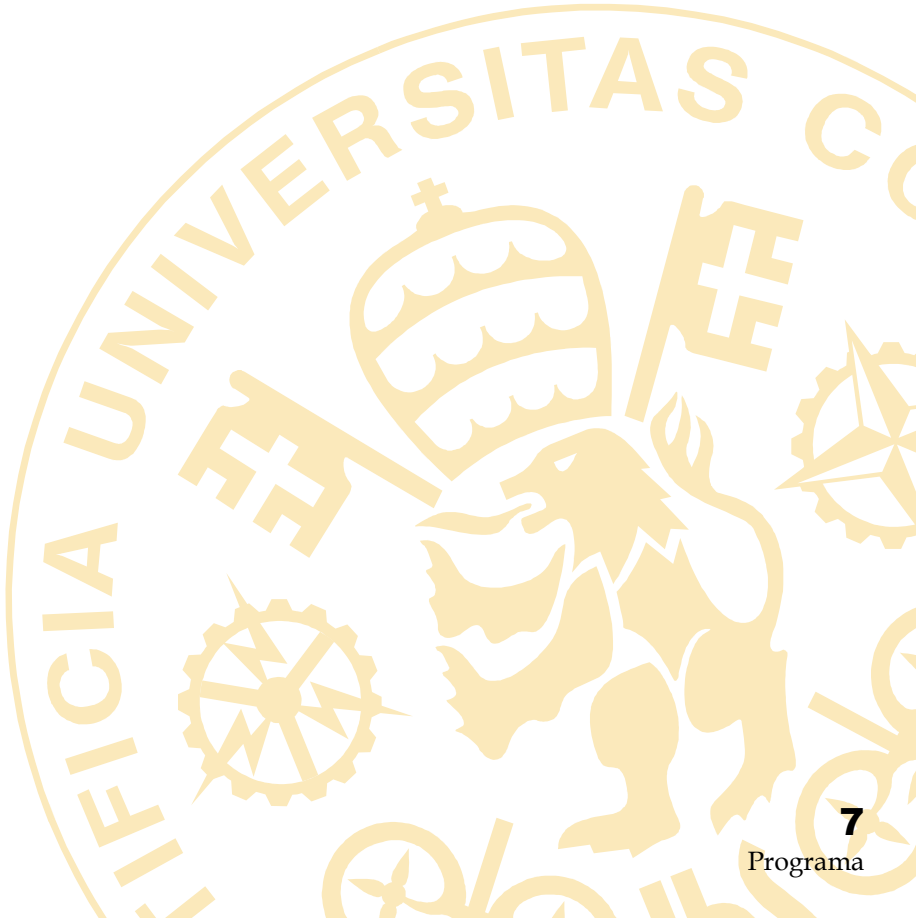
- Conceptos básicos sobre protección de la información y de los equipos informáticos.
- Conocer métodos, técnicas y herramientas de protección.
- Conocer metodologías para el diseño de planes de seguridad.

Objetivos de la Asignatura

Al terminar el curso el alumno debe conocer y manejar:

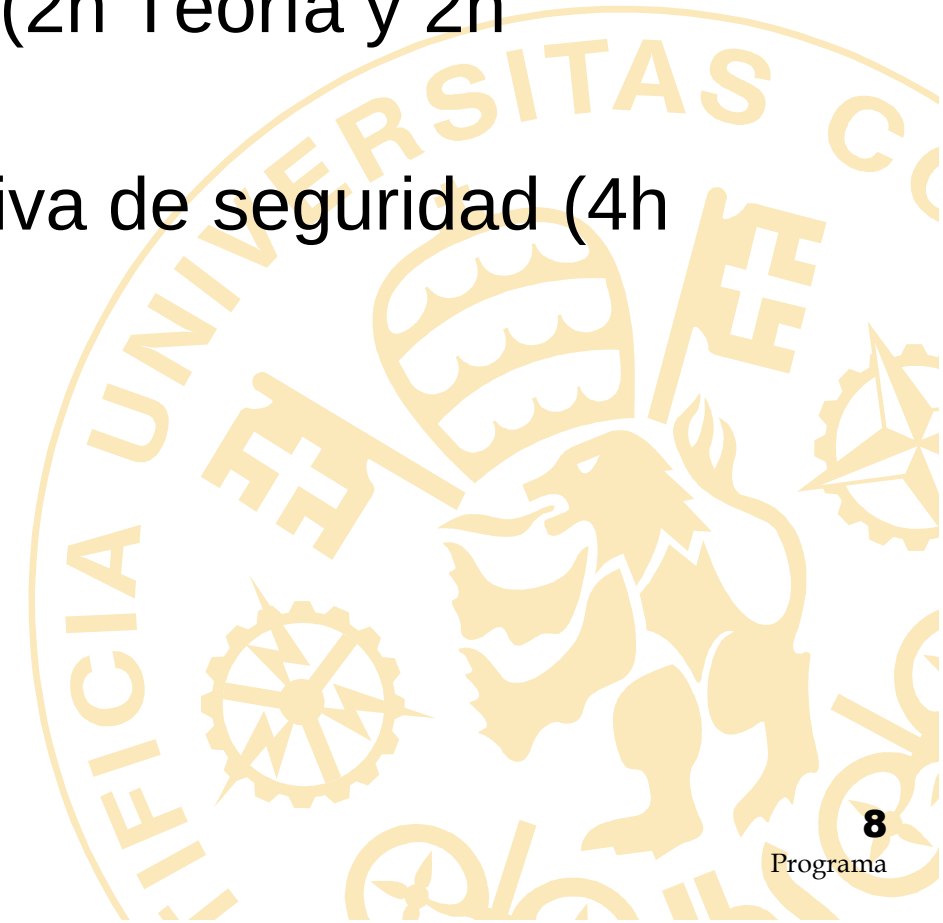
- La **terminología** utilizada en las técnicas y métodos existentes para protección y recuperación de la información
- Los **conceptos básicos** relacionados con la seguridad informática
- **Herramientas** y procedimientos principales relacionados con la seguridad informática
- Métodos y técnicas de diseño que le lleven a la realización de **proyectos de seguridad** de la información
- **Certificados electrónicos** para establecer conexiones seguras por internet, y correo electrónico firmado o cifrado.

Programa



Parte 1: Teoría sobre seguridad

- 1. Introducción y conceptos básicos. (4h teoría)
- 2. Análisis de Riesgos. (2h Teoría y 2h Prácticas)
- 3. Legislación y normativa de seguridad (4h teoría + 4h prácticas)



Parte 2: Criptografía

- 4. Criptografía simétrica (2h teoría + 2h prácticas)
- 5. Criptografía de clave pública (2h teoría + 2h prácticas)
- 6. Cifrado irreversible, funciones de resumen y aleatoriedad (2h teoría + 2h prácticas)
- 7. Algoritmos de firma digital (4h teoría + 4h prácticas)

Parte 3: Aplicaciones

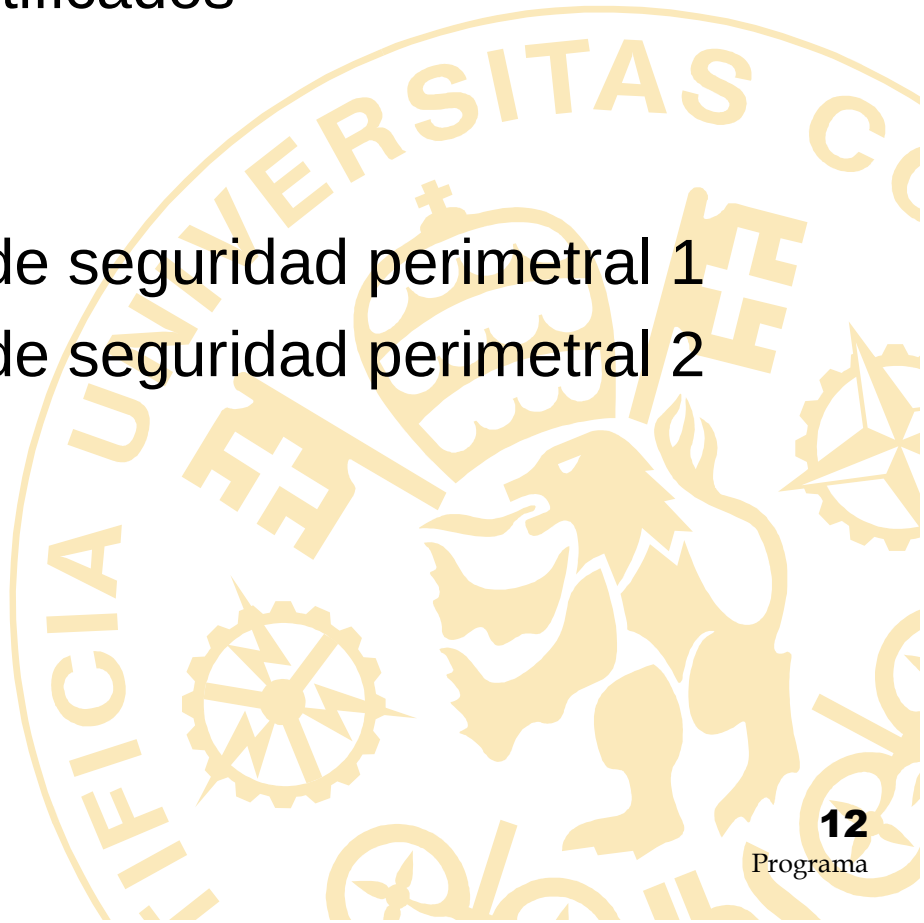
- 7. Algoritmos de firma digital (4h teoría + 4h prácticas)
- 8. Infraestructuras de Clave Pública (PKI). (4h teoría + 4h prácticas)
- 9. Virus y sistemas antivirus. (4h teoría + 4h prácticas)
- 10. Seguridad perimetral. (4h teoría + 4h prácticas)

Prácticas

- 1. Práctica: Gestión de la seguridad con herramientas públicas
- 2. Práctica: Legislación y normativa 1: LOPD
- 3. Práctica: Legislación y normativa 2
- 4. Práctica: Criptografía simétrica
- 5. Práctica: Criptografía asimétrica: generación de claves, cifrado y descifrado
- 6. Práctica: Aleatoriedad
- 7. Práctica: Firma electrónica de datos

Prácticas

- 8. Práctica: Firma electrónica de formularios
- 9. Práctica: Utilización de certificados en Internet
- 10. Práctica: Emisión de certificados
- 11. Práctica: Virus
- 12. Práctica: Spyware
- 13. Práctica: Herramientas de seguridad perimetral 1
- 14. Práctica: Herramientas de seguridad perimetral 2



Sistema de evaluación

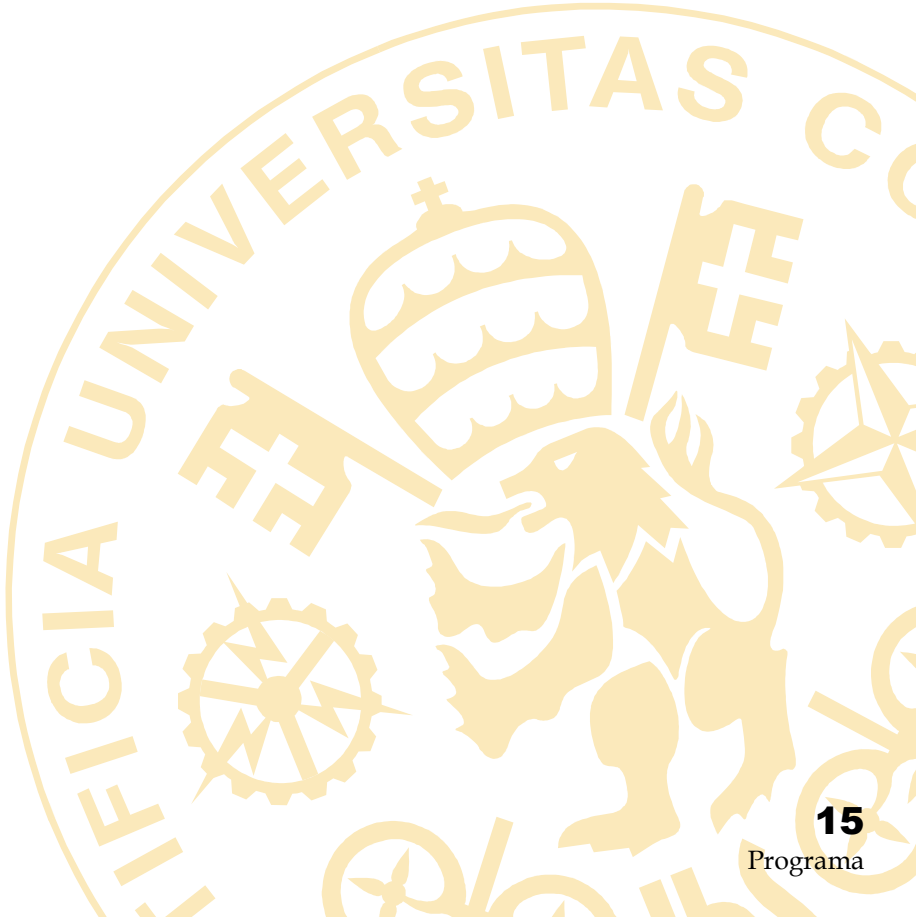
Sistema de Evaluación

- La **asistencia** a clase es obligatoria, según las normas de la Escuela
- A lo largo del curso se realizarán **prácticas** en ordenador y pequeños problemas, cuya entrega es obligatoria
- La nota final se basa fundamentalmente en los exámenes. (tipo test/preguntas cortas)

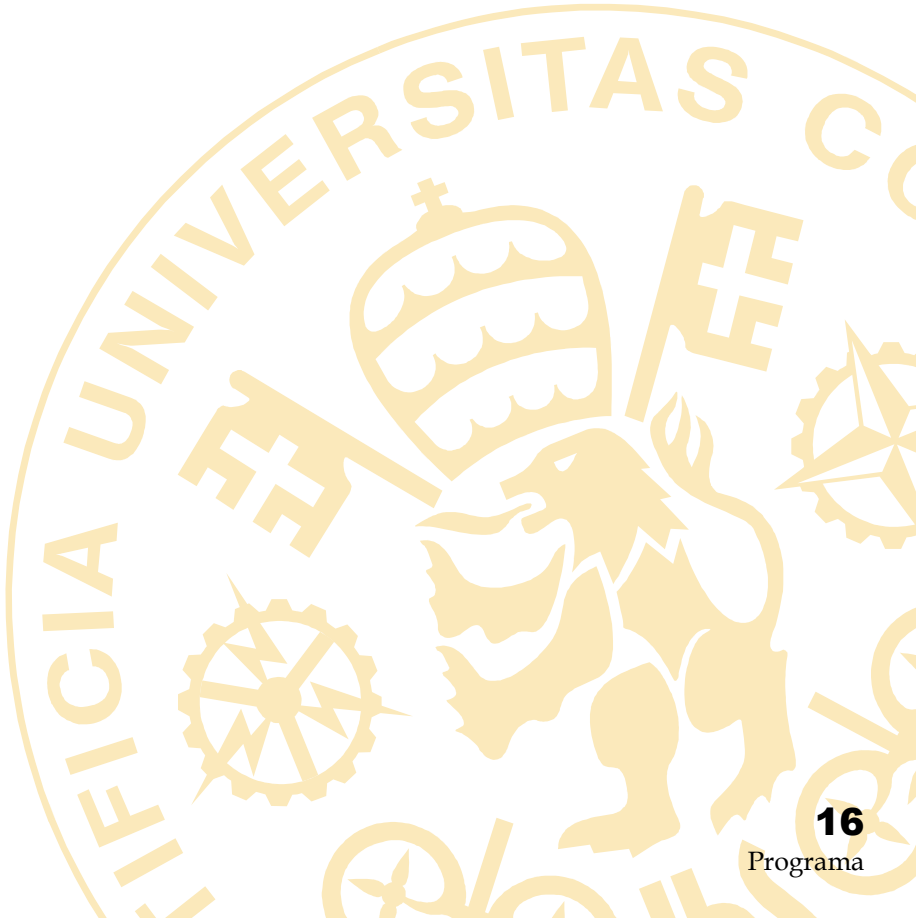
  Otros aspectos:
  - Participación en clase
  - Noticias sobre incidentes de seguridad

Sistema de Evaluación

- Exámenes:
  - Examen intercuatrimestral
    - Semana del 21 de abril
    - 20% de la nota
    - Temas 1 al 5
  - Examen final:
    - Semanas 16/jun – 4/jul
    - 80% de la nota
    - Todos los temas



Bibliografía



Bibliografía

- Bruce Schneier. **Applied Cryptography**. John Wiley & Sons., 1996
- William Stallings. **Cryptography and Network Security: Principles and Practice** (Third edition).. Prentice Hall, 2002
- Amparo Fúster y otros. **Técnicas Criptográficas de protección de datos**.. Ra-Ma, 2000
- Rolf Oppliger. **Security Technologies for the World Wide Web**, (Second Edition).. Artech House Publishers in the Computer Security Series, 2002
- Charles P. Pfleeger, Shari Lawrence Pfleeger. **Security in Computing** (Third edition). Prentice Hall, 2002
- Scott Barman. **Writing Information Security Policies**.. SAMS, 2001
- W.Cheswick & S. Bellovin. **Firewalls and Internet Security**. Addison-Wesley, 1994
- **Norma UNE-ISO/IEC 17799**. Information technology. Code of practice for information security management. Aenor, 2000

Objetivo global de la asignatura

Objetivo global de la asignatura

"I've never been more secure and felt more insecure"

Leonard Schranch, CEO SWIFT*

World Economic Forum in Davos, Jan/2003

* SWIFT es una compañía de servicios de red con base en Bruselas utilizada por 7000 instituciones financieras del mundo. Procesa 1500 millones de mensajes al año y mueve 6.000.000 millones de dólares al día.