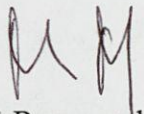


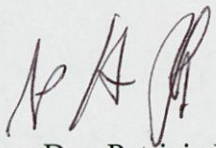
Comp 2000  
18

**UNIVERSIDAD DE BUENOS AIRES**  
**FACULTAD DE CIENCIAS EXACTAS Y NATURALES**

1. DEPARTAMENTO: Computación
2. CUATRIMESTRE: Segundo de 2000
3. ASIGNATURA: Seguridad informática en nuevas instalaciones
4. CARRERA: Licenciatura en Ciencias de la Computación
5. CARACTER DE LA MATERIA: optativa
6. NUMERO DE CODIGO DE CARRERA: 18
7. NUMERO DE CODIGO DE MATERIA: C
8. PUNTAJE: 1
9. PLAN DE ESTUDIOS AÑO: (1993) (1987)
10. DURACION DE LA MATERIA: una semana
11. HORAS DE CLASE SEMANAL:
  - a) TEORICA/PRACTICA: 15hs
  - b) LABORATORIO: ---
  - c) PRACTICAS: -----
  - d) SEMINARIOS: ---
12. CARGA HORARIA TOTAL: 15 hs semanales
13. ASIGNATURAS CORRELATIVAS: conocimientos básicos de informática
14. FORMA DE EVALUACION: prácticos y final
15. PROGRAMA Y BIBLIOGRAFIA: adjuntos a esta hoja

Fecha: 29 de junio 2000

  
Prof. Responsable  
Dr. Manuel Medina

  
Directora Dra. Patricia Borensztejn

## N1 - " Seguridad Informática en nuevas instalaciones"

**Horario: 19 a 22 hs.**

El Dr. Manuel Medina Llinás es catedrático de la Universidad Politécnica de Cataluña, España, en el Departamento de Arquitectura de Computadores y es director del es-CERT (Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas) y del Centro de Investigación CANet, Centro de Aplicaciones Internet. Ha dirigido proyectos de investigación y desarrollo y ha actuado de asesor en temas relacionados con la seguridad informática y firma electrónica para varias organizaciones públicas y privadas. Sus cursos reflejan la experiencia adquirida en colaboraciones en proyectos, generalmente financiados por la Comisión Europea, con empresas españolas y europeas.

### **Objetivos:**

- \* Presentar los fundamentos y las técnicas utilizadas para la protección de la información en sistemas informáticos.
- \* Impartir los conocimientos necesarios para aplicar métodos de análisis y evaluación del riesgo.
- \* Proporcionar los conocimientos básicos necesarios para aplicar técnicas criptográficas adecuadas en criptosistemas de clave pública y de clave privada.
- \* Introducir la problemática de la protección de la información en medios electrónicos de intercambio de mensajes como es el caso de INTERNET.
- \* Presentar la seguridad desde los distintos puntos de vista de una instalación informática: Red, Hardware, Sistema Operativo, Aplicaciones, Operadores/Administradores, Personal, Usuarios externos, Entorno.
- \* Introducir los conceptos de seguridad lógica y física, y herramientas fundamentales disponibles para mejorarlas. Brindar una definición de una política de seguridad adecuada.

### **Programa:**

1. Conceptos básicos, terminología y criptografía.
2. Estrategias fundamentales de la seguridad: análisis y gestión del riesgo.
3. Seguridad física.
4. Seguridad personal y Legislación.
5. Seguridad de los equipos (hardware)
6. Seguridad de los programas (software): Seguridad de los SO, aplicaciones distribuidas seguras (correo y comercio electrónicos), Virus.
7. Seguridad en la red: servicios de Seguridad, mecanismos de Seguridad.
8. Gestión de la Seguridad: criterios básicos de la evaluación de la Seguridad de los ordenadores, estudio de casos (criterios éticos, económicos y legales).
9. Políticas de seguridad.

### **Prerrequisitos**

Conocimientos básicos de Informática.

**ESTE CURSO SE DICTARA EN CASTELLANO**

