

## Seguridad en Redes

### Carreras/Planes para los que se ofrece:

- Ingeniería en Informática – Plan 2006 implementación 2010.
- Se dicta en el 1° semestre.

### Objetivos del curso

La materia tiene como propósito el presentar, implementar y mejorar las defensas de una infraestructura de procesamiento de datos, y medir la efectividad de las contramedidas implementadas, con el objetivo de impedir el secuestro de información, el acceso de terceros a recursos digitales no autorizados, la apropiación indebida de valores y la sustitución de identidad. Presenta al estudiante los conceptos, terminología, tipos de amenazas y vías a través de las cuales un ataque puede comprometer la operación o el contenido de una red corporativa. A su vez, introduce los paradigmas que permiten construir soluciones empresariales robustas y seguras, de alta demanda.

### Temario del curso

1. Repaso protocolo TCP/IP
  - 1.1. Modelo de capas
  - 1.2. Interacción y servicios de capas del modelo
  - 1.3. ARP/IP/TCP-UDP/aplicaciones
2. Problemas de Seguridad protocolo (redes) TCP/IP
  - 2.1. Autenticación del origen (IP spoofing)
  - 2.2. Interacción IP/MAC, ARP spoofing
  - 2.3. Ataques a protocolo de ruteo, ICMP
  - 2.4. TCP session Hijacking, SYN Flooding
  - 2.5. Capa de Aplicación: Servicio DNS
  - 2.6. VLAN
3. Redes inalámbricas (WiFi®).
  - 3.1. Requerimientos
  - 3.2. WEP, WPA, WPA2, EAP, 802.1X
  - 3.3. Integración con redes existentes
4. Seguridad IP (IPSec)
  - 4.1. Asociaciones de Seguridad (SA)
  - 4.2. Modos de funcionamiento (túnel y transporte)
  - 4.3. Protocolo AH y ESP (encabezados y servicios que ofrecen)
  - 4.4. IPSec Key Management (IKE)
  - 4.5. IPsec y filtrado
5. VPN
  - 5.1. ¿Qué es una VPN? VPN sobre Internet
  - 5.2. Implementación de VPN

## 6. Firewalls

- 6.1. Definición. Qué puede hacer y que NO un Firewall
- 6.2. Filtrado de paquetes, con y sin estados. Generando reglas de filtrado
- 6.3. Logging
- 6.4. Arquitecturas de Firewall
- 6.5. Tipos de Firewall
- 6.6. Servicios Proxy y NAT

## 7. IDS/IPS

- 7.1. Definición
- 7.2. Clasificación y Formas de Detección
- 7.3. Falsos positivos y negativos
- 7.4. ¿Acciones automáticas? Donde monitorizar (sensar)

## 8. Otro tipo de sensores. Honeypots

## 9. Diseño de un perímetro seguro

- 9.1. Identificación de activos a proteger
- 9.2. Identificación de fronteras
- 9.3. Separación e Identificación de zonas de seguridad

### **Evaluación y aprobación**

- Mínimo de asistencia requerido: 50% del total de clases.
- Una prueba escrita individual (obligatoria) con un mínimo de aprobación de 50/100.
- Trabajo obligatorio, con un mínimo de aprobación de 50/100.
- La prueba escrita representa el 50% de la nota final del curso.
- El trabajo obligatorio representa el 50% de la nota final del curso.
- Cumplidos los mínimos del régimen de evaluación, se aprueba la asignatura con una nota final en la escala de 6 a 12.
- En caso de reprobación de la asignatura, se podrá rendir examen en los períodos ordinarios (por el lapso de un año) siempre que se haya alcanzado el mínimo de asistencia requerido.

### **Docente**

- Ing. Andrés Moll