

Programa de Asignatura

Ingeniería en Computación - In.Co.

Nombre de la Asignatura	Fundamentos de la Seguridad Informática
Responsable	Gutavo Betarte
Créditos	10
Objetivo de la Asignatura	Capacitar al estudiante para: (1) Asimilar la seguridad informática como un conjunto de metodologías. (2) Analizar la seguridad de una red o sistema informático, identificando los puntos débiles de la misma para su protección. (3) Conocer los principales ataques de los que puede ser objeto un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión. (4) Entender el funcionamiento de diferentes protocolos criptográficos que se utilizan en la actualidad. (5) Conocer los sistemas de autenticación más importantes identificando sus características principales.
Metodología de enseñanza	CARGA TOTAL DE TRABAJO: 150 horas. Horas de aula semanales: 4 Horas de trabajo del estudiante semanales: 6 Se dictarán clases teóricas, prácticas y de laboratorio en máquinas.
Temario	<p><u>Módulo 1. Bases y motivación</u></p> <p>Introducción. Motivación, definiciones y objetivos de la seguridad informática. Motivación. Ejemplos históricos. Ejemplos actuales. Quién precisa seguridad informática. Definición de seguridad informática. Objetivos. Propiedades de seguridad: confidencialidad (secreto), disponibilidad, integridad, autenticación, no repudio. Motivación y herramientas del atacante. Principios de seguridad informática.</p> <p><u>Módulo 2. Criptografía Aplicada</u></p> <p>Introducción a la Criptografía. Definiciones. Criptografía moderna. Algoritmo público, clave secreta. Objetivos de un algoritmo. Tipos de ataques a los que debe ser inmune un algoritmo. Cifrado perfecto. "One time pads". Clasificaciones: Cifrados de clave simétrica, de clave pública, en bloque, en flujo. Encadenamiento de algoritmos en bloques. Otras funciones criptográficas. Hashes. Diffie-Hellman. Gestión de claves. Firma electrónica. Ejemplo de protocolos: SSL. Importancia de los números aleatorios en criptografía. Infraestructura de clave pública (PKI). Certificados digitales. Ejemplo: X.509. Protocolos criptográficos.</p> <p><u>Módulo 3. Seguridad de Sistemas</u></p> <p>Identificación, Autenticación: mecanismos tradicionalmente utilizados en los sistemas operativos comunes, y ganar una noción razonable de los nuevos mecanismos que ya se están implementando (y que se implementan hace tiempo</p>

en sistemas especializados en seguridad). Métodos de Autenticación. Algoritmos y protocolos de autenticación. Políticas de seguridad y mecanismos de control de acceso. Modelos de políticas de seguridad: Bell - La Padula. BIBA. Clark-Wilson. Chinese Wall. Modelos de control de acceso: IBAC (Identity Based Access Control). DAC (Discretionary Access Control). MAC (Mandatory Access Control). RBAC (Role Based Access Control). Mecanismos de control de acceso: ACL, Control de acceso centralizado (AAA), RADIUS, TACACS, Single Sign-On. Seguridad en Windows. Seguridad en Unix.

Módulo 4. Seguridad en Redes TCP/IP

Introducción a la seguridad en redes TCP/IP. Problemas en las distintas capas del modelo OSI simplificado. Seguridad por debajo de la capa 3. Seguridad física. Seguridad en los protocolos de capa 2 y capa MAC. Ataques a estos protocolos. Redes inalámbricas. (IN)Seguridad en capa 3 y 4. Ataques a los protocolos IP, TCP, UDP, ICMP. Qué nos dá IPsec y qué no. Seguridad en los protocolos de aplicación. Servicios de infraestructura críticos: DNS. Ataques a las aplicaciones. Seguridad de la infraestructura. Ataques a la infraestructura. (IN)Seguridad en los protocolos de ruteo. Herramientas para la seguridad en redes TCP/IP: Firewalls, VPNs, IDS, Honeypots. El estado de la seguridad en Internet: DDoS, Ataques "Man in the middle", Ataques a las aplicaciones. Botnets, Canales encubiertos, Ataques "sociales". El factor humano. Phishing, etc.

Módulo 5. Seguridad en las Aplicaciones

Errores en los programas y defensas: Ataques al Stack, Bugs en el formato de los strings, Ataques de Timing, Defensas contra estos ataques. Diseño de código seguro: Diseño modular, Herramientas para hacer código seguro, Verificadores de modelos. Manejando código inseguro: Sandboxing, Máquinas virtuales. Seguridad en los browsers: Cookies, Privacidad y multitudes, Java Script, Java Applets y ActiveX. Secure Coding.

Módulo 6. Seguridad en Bases de Datos

Bases de datos Relacionales: claves, reglas de integridad. Control de acceso: el modelo de seguridad de SQL, privilegios, vistas como control de acceso. Bases estadísticas: seguridad, agregación e inferencia, ataques, contramedidas. Integración con el SO. Privacidad.

Bibliografía y Material de Referencia

Computer Security, Dieter Gollman, Wiley Computing Publishing, 2nd. Edition, 2006.

Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J. Anderson, Wiley Computing Publishing, 2001. ISBN: 0-471-38922-6.

Practical Unix & Internet Security, S. Garfinkel, G. Spafford & A. Schuartz, Ed. O'Reilly, 3rd Edition.

National Security Agency, Central Security Service, <http://www.nsa.gov>.

SANS (SysAdmin, Audit, Network Security) Institute, <http://www.sans.org>.

Building Internet Firewalls, E. D. Zwicky, S. Cooper, & B. Chapman, Ed. O'Reilly, 2nd Edition.

Linux Firewalls, R. Ziegler, Ed. New Riders, 2nd Edition.

**Conocimientos
previos exigidos y
recomendados**

Exigidos: lógica, bases de datos, sistemas operativos y algoritmos y estructuras de datos
Recomendados: redes de computadoras y criptografía

Anexo:**• Cronograma tentativo**

semana 1: Módulo 1
semanas 2 a 4: Módulo 2
semanas 5 a 7: Módulo 3
semanas 7 a 10: Módulo 4
semanas 10 y 11: Módulo 5.
semana 12: Módulo 6.

• Modalidad del curso y procedimiento de evaluación.

La asignatura se evaluará por medio de dos parciales y trabajos de laboratorio. El nivel mínimo de suficiencia en los trabajos de laboratorio es eliminatorio. Por otra parte, dependiendo de las condiciones de dictado del curso, el trabajo de laboratorio se evalúa según las opciones aprobado/no aprobado, o con puntaje diferenciado en el caso de aprobación. En este último caso, el puntaje del laboratorio se integraría al puntaje total del curso, prorrateándose en los de las pruebas parciales.

En todos los casos de los resultados obtenidos surgen dos posibilidades:

- Exoneración del curso
- Insuficiencia en el curso; el estudiante reprueba el curso

Se presenta a continuación el esquema de evaluación del curso

Exoneración. El estudiante debe cumplir los siguientes requisitos :

- llegar al nivel mínimo en cada uno de los trabajos de laboratorio, y
- reunir al menos el 60% del puntaje de parciales, y
- obtener al menos el 25% en cada prueba parcial

Insuficiencia. El estudiante no obtiene los puntajes de alguna de las franjas anteriores.

• Materia.

Arquitectura, Sistemas Operativos y Redes de Computadoras

• Previaturas.

Plan 97

Para **cursar** esta asignatura se deben tener aprobado los **exámenes** de las siguientes asignaturas: fundamentos de bases de datos, sistemas operativos, programación 3 y lógica.

Plan 87

Para **cursar** esta asignatura se deben tener aprobados los **exámenes** de las siguientes asignaturas: Bases de Datos, sistemas operativos, programación III y lógica.

- **Cupo**

Máximo : 30, Mínimo : 15

15 estudiantes serán seleccionados según escolaridad en materias afines (Sistemas Operativos, Arquitectura de Sistemas y Programación 3 o 4 según el plan) y se tendrá en cuenta (no excluyente) Redes de Computadoras. Los restantes 15 estudiantes se seleccionarán mediante sorteo entre los asistentes a las dos primeras clases. El cupo se debe a la cantidad de máquinas disponibles para la realización de los trabajos prácticos y de laboratorio y del seguimiento requerido por parte de los docentes.