97/11

Facultad de Ingeniería
Comisión Académica de Posgrado

Formulario de Aprobación Curso de Actualización 2011

Asignatura: Seguridad de Sistemas Informáticos

Profesor de la asignatura [1]**:**
Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación
Ing. Alejandro Blanco, Profesor Adjunto, Instituto de Computación

Profesor Responsable Local [1]**:**
(título, nombre, grado, Instituto)

Otros docentes de la Facultad:
Ing. Marcelo Rodríguez, Asistente, Instituto de Computación

Docentes fuera de Facultad:
(título, nombre, cargo, Institución, país)

Instituto ó Unidad: **Computación**
Departamento ó Area: **Programación, Grupo de Seguridad Informática**

1

Fecha de inicio y finalización: a confirmar
Horario y Salón: a confirmar

Horas Presenciales: 36
Se deberán discriminar las mismas en el ítem Metodología de enseñanza.

Arancel: $8,500

Público objetivo y Cupos: Máximo 30 personas, mínimo 10
(si corresponde, se indicará el número de plazas, mínimo y máximo y los criterios de selección. Si no existe indicación particular para el cupo máximo, el criterio general será el orden de inscripción en el Depto. de Posgrado, hasta completar el cupo asignado)

Objetivos:

El objetivo de este curso es introducir al estudiante en los conceptos básicos de la seguridad informática. El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas, con el objetivo de desarrollar, ampliar o mejorar las plataformas de computación. Al finalizar el curso el alumno habrá adquirido los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir un sistema informático y establecer los mecanismos de protección adecuados que garanticen la seguridad del mismo.

Conocimientos previos exigidos: Profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información

Conocimientos previos recomendados:

Facultad de Ingeniería
Comisión Académica de Posgrado

Metodología de enseñanza:
El curso consiste de un 75% de exposiciones teóricas (24hs) y el otro 25% (8hs) de trabajos prácticos en grupos, que son realizados usando la infraestructura del LaSI (Laboratorio de Seguridad Informática).
El cuso se dictará en 8 clases téoricas de 3 horas, 2 clase por semana, durante 4 semanas y 2 sesiones de laboratorio de 4 horas.

Forma de evaluación:
Se evaluarán los trabajos de laboratorio y un examen final. La realización de las prácticas de laboratorio es **obligatoria**.

Temario:

1. Bases y Motivación
   a) Introducción.
   b) Motivación, definiciones y objetivos de la seguridad informática.
   c) Principios de seguridad informática.

2. Seguridad de Sistemas
   a) Identificación, Autenticación
   b) Métodos de Autenticación
   c) Algoritmos y protocolos de autenticación.

3. Políticas de seguridad y mecanismos de control de acceso. Estructuras de control. Seguridad Multinivel.

4. Modelos de control de acceso
   a) Bell-La Padula,
   b) Chinese wall
   c) RBAC

5. Seguridad en Windows.
   a) Arquitectura Windows, Registry, Servicio de Directorio.
   b) Implementación de principals, sujetos y objetos en windows.
   c) Control de Acceso en Windows.
      Tokens, Access Control Lists, Autenticación, etc
   d) Gestión de la Seguridad
      Group Policies, Built-in Accounts, Auditoria, etc

6. Seguridad en Unix
   a) Principals y sujetos y objetos en Unix
   b) Principios generales de seguridad:
   c) programas suid, chroot
   d) variables de ambiente, search path
   e) inetd, wrappers
   f) Auditoria de Logs
   g) Como implementar Seguridad multinivel o RBAC en Unix.
      SELinux, sudo
   h) Hardening

Bibliografía:

R. Anderson, *Security Engineering – A Guide to Building Dependable Distributed Systems,* Wiley, Third edition, 2008.

D. Gollmann, *Computer Security*, Wiley, 2006.

R. Morris, K. Thompson, *Password Security: A Case History*, Comm. ACM, vol. 22, 1979.

D. Klein, *"Foiling the Cracker": A Survey of, and Improvements to, Password Security*, Proc. USENIX Security Workshop, 1990.

R.S. Sandhu, *Lattice-Based Access Control Models*, IEEE Computer, 1993.

D. Denning, *A Lattice Model of Secure Information Flow*, Comm. ACM, vol 19, 1976.

Michael M Swift et al, Improving the granularity of access control for Windows 2000, ACM Trans Inf Syst Secur, 2002

Microsoft, Microsoft Windows 2000 Security: Technical Reference, Microsoft Press, 2000

S. Garfinkel, G. Spafford & A. Schwartz, Practical Unix & Internet Security (3rd Edition), O'Reilly, 2003