Formulario de Aprobación Curso de Actualización 2016

Asignatura: Seguridad de Sistemas Informáticos

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

Profesor Responsable Local:Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación
Ing. Alejandro Blanco, Profesor Adjunto, Instituto de Computación
(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: Instituto de Computación
Departamento ó Area: Seguridad Informática

Fecha de inicio y finalización: Desde el 15 de marzo al 26 de abril. Martes y Jueves
Horario y Salón: de 18:00 a 21:00 hs. Salón a confirmar

Horas Presenciales: 38
(se deberán discriminar las mismas en el ítem Metodología de enseñanza)

Arancel: $12.250
(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem metodología de la enseñanza)

Público objetivo y Cupos: Profesionales y estudiantes interesados en Seguridad Informática en particular, profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información
No tiene cupo

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 estudiante 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: Ninguno

Conocimientos previos recomendados: Conocimientos de informática

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.

- Horas clase (teórico):24
- Horas clase (práctico):0

- Horas clase (laboratorio):8
- Horas consulta:3
- Horas evaluación:3
    - Subtotal horas presenciales: 38
- Horas estudio: 37
- Horas resolución ejercicios/prácticos:
- Horas proyecto final/monografía:
    - Total de horas de dedicación del estudiante: 75

Forma de evaluación: El curso se evaluará a partir de

- trabajos de laboratorio
- un examen final.

La realización de las prácticas de laboratorio es **obligatoria**.

Temario:

1. Bases y Motivación
    1.1 Introducción.
    1.2 Motivación, definiciones y objetivos de la seguridad informática.
    1.3 Principios de seguridad informática.

2 Seguridad de Sistemas
    2.1 Identificación, Autenticación
    2.2 Métodos de Autenticación
    2.3 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
    4.1 Bell-La Padula,
    4.2 Chinese wall
    4.3 RBAC

5 Seguridad en Windows.
    5.1 Arquitectura Windows, Registry, Servicio de Directorio.
    5.2 Implementación de principals, sujetos y objetos en windows.
    5.3 Control de Acceso en Windows.
    Tokens, Access Control Lists, Autenticación, etc
    5.4 Gestión de la Seguridad
    Group Policies, Built-in Accounts, Auditoria, etc

6 Seguridad en Unix
    6.1 Principals y sujetos y objetos en Unix
    6.2 Principios generales de seguridad:
    6.3 programas suid, chroot
    6.4 variables de ambiente, search path
    6.5 inetd, wrappers
    6.6 Auditoria de Logs
    6.7 Como implementar Seguridad multinivel o RBAC en Unix.
    SELinux, sudo
    6.8 Hardening

Bibliografía:

Libros

Security Engineering – A Guide to Building Dependable Distributed Systems - R. Anderson – Wiley - ISBN-10: 0470068523 | ISBN-13: 978-0470068526 – 2nd Edition, 2008.

Computer Security - D. Gollmann – Wiley – ISBN-10: 0470862939 | ISBN-13: 978-0470862933 – 2nd Edition, 2006 .

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

Artículos

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