Formulario de Aprobación Curso de Actualización 2011

Asignatura: Seguridad en Aplicaciones

Profesor de la asignatura [1]:
MSc. Ing. Felipe Zipitría, Profesor Adjunto, Instituto de Computación
Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación

Profesor Responsable Local [1]:
Otros docentes de la Facultad:
(título, nombre, grado, Instituto)

Docentes fuera de Facultad:
Ing. Rodrigo Martínez, Ayudante (Gr. 1) del InCo.

Instituto ó Unidad: Computación
Departamento ó Area: Programación, Grupo de Seguridad Informática
[1] Agregar CV si el curso se dicta por primera vez.
(Si el profesor de la asignatura no es docente de la Facultad se deberá designar un responsable local)

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

Horas Presenciales: 30

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:

Introducir a los participantes en los principales conceptos y metodologías asociadas a la seguridad en el desarrollo de aplicaciones. Comprender qué hitos tener en cuenta a la hora de construir aplicaciones seguras en el proceso de desarrollo, y entender los errores más comunes que se presentan en la codificación de las aplicaciones mediante una taxonomía. Finalmente, complementar los conceptos con el desarrollo de las aplicaciones Web y sus diferencias, si las hay, con las aplicaciones tradicionales.

Conocimientos previos exigidos: Profesionales informáticos vinculados al desarrollo de aplicaciones.

Conocimientos previos recomendados:

Metodología de enseñanza:

El curso se dictará en clases de 2 horas, 3 veces por semana, durante 5 semanas. El curso estará dividido en un 80% de exposiciones teóricas y el otro 20% de trabajos de laboratorio en el que se aplicarán los conceptos teóricos introducidos.

Se estima una dedicación aproximada del estudiante de 1 horas de estudio por cada hora dictada
Los totales de horas se computan de la siguiente forma:

Horas teórico-practicas: 60
Horas de preparación del trabajo y estudio asitido: 10
Horas de evaluación: 5
Total horas: 75

Forma de evaluación:

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

Temario:

1. Introducción.
   a. Presentación, revisión de conceptos.
   b. Un framework para el manejo de riesgos

2. Siete hitos para la seguridad en el software
   a. Code review
   b. Análisis de riesgos en la arquitectura
   c. Tests de penetración
   d. Test de seguridad basado en los riesgos
   e. Casos de abuso
   f. Requerimientos de seguridad
   g. Operaciones de seguridad
   h. Análisis externo

3. Taxonomía de errores de codificación
   a. Validación de la entrada y codificación
   b. Abusos de API
   c. Funcionalidad de seguridad
   d. Tiempo y estado
   e. Manejo de errores
   f. Calidad del código
   g. Encapsulación
   h. Entorno

4. Aplicaciones Web
   a. Autenticación/autorización
   b. Manejo de sesiones
   c. OWASP Top Ten, mapeo en la taxonomía

Bibliografía:

Software Security: Building Security In, Gary McGraw, Addison-Wesly Software Security Series, ISBN: 0-321-35670-5.

OWASP, Open Web Application Security Project, http://www.owasp.org