



20
Jek

Facultad de Ingeniería Comisión Académica de Posgrado

Formulario de Aprobación Curso de Posgrado 2015

Asignatura: Gestión de la Seguridad de la Información

Profesor de la asignatura:

Mag. Ing. María Eugenia Corti, Profesor Asistente, Instituto de Computación
Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación

Profesor Responsable Local¹:

(título, nombre, grado, Instituto)

Otros docentes de la Facultad:

(título, nombre, grado, Instituto)

Docentes fuera de Facultad:

MSc. Ing. Eduardo Carozo.
Mag. Ing. Gustavo Pallas.

Instituto ó Unidad: Instituto de Computación
Departamento ó Area: Seguridad Informática

Fecha de inicio y finalización: Del 28 de setiembre al 13 de noviembre

Horario y Salón: Lunes, Miércoles y Viernes de 18:00 a 21:00 hs. Salón a confirmar.

Horas Presenciales: 77

Nº de Créditos: 10

(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 a los estudiantes en los principales conceptos y metodologías asociadas a la gestión de seguridad de la información, y en el marco normativo internacional y nacional existente. Llevar a la práctica una metodología de rápida aplicación para la implementación de un Sistema de Gestión de Seguridad de la Información. Presentar metodologías concretas para la gestión de riesgos y gestión de incidentes. Se abarcarán las principales conceptos entorno a la familia de normas ISO/IEC 27000.

Conocimientos previos exigidos: Ninguno

Conocimientos previos recomendados: Conocimientos de informática

Metodología de enseñanza:

El curso se dictará en clases de 3 horas, 3 veces por semana, durante 7 semanas. El curso estará dividido en un 50% de exposiciones teóricas y el otro 50% de trabajos prácticos, en grupos, en los que se aplicarán los conceptos teóricos introducidos. Cada trabajo práctico realizado en clase formará parte de un trabajo final que deberá ser entregado y presentado por el grupo al finalizar el curso.
(comprende una descripción de las horas de clase asignadas y su distribución en horas de práctico, horas de teórico, horas de laboratorio, etc. si corresponde)

- Horas clase (teórico): 30
- Horas clase (práctico): 24
- Horas clase (laboratorio): 0
- Horas consulta: 20
- Horas evaluación: 3
 - Subtotal horas presenciales: 77
- Horas estudio: 43
- Horas resolución ejercicios/prácticos: 30
- Horas proyecto final/monografía: 0
 - Total de horas de dedicación del estudiante: 150

Forma de evaluación: El curso se evaluará a partir de:

- trabajos en clase
- un trabajo final y la presentación del mismo
- un examen final.

Temario:

1. Introducción.
 - 1.1 Definiciones y conceptos de gestión de seguridad de la información
 - 1.2 Confidencialidad, Integridad y Disponibilidad
 - 1.3 Marco normativo nacional e internacional
2. Sistema de Gestión de Seguridad de la Información
 - 2.1 Metodologías de implantación
 - 2.2 Principales desafíos a enfrentar
 - 2.3 Herramientas disponibles que faciliten la implantación
3. Gestión de Riesgos
 - 3.1 Introducción al proceso de gestión
 - 3.2 Metodologías de análisis de riesgo
 - 3.3 Tratamiento de riesgos
4. Gestión de incidentes
 - 4.1 Definición de incidentes
 - 4.2 Procesos de clasificación, análisis, tratamiento, resolución y cierre
 - 4.3 Control de flujos de información y procesos.
 - 4.4 Modelos organizacionales de Centros de Respuesta y su relación con el SGSI
5. Gestión de la continuidad del negocio
 - 5.1 Componentes del negocio
 - 5.2 Tipos de desastres que deben considerarse
 - 5.3 Análisis de Impacto del Negocio



Herrera

Facultad de Ingeniería Comisión Académica de Posgrado

-
- 5.4 Desarrollo de estrategias de mitigación
 - 5.5 Plan de continuidad del negocio/ Plan de recuperación
 - 5.6 Entrenamiento, testeo y auditoría del Plan de Continuidad del Negocio.

Bibliografía:

Susan Snedaker, Business Continuity & Disaster Recovery for IT professionals, ISBN: 978-1-59749-172-3.

Gonzalo Alvarez Marañón y otro, Seguridad Informática para Empresas y Particulares, ISBN: 84-481-4008-7

C. Alberts y A. Dorofee, Managing Information Security Risks, ISBN: 0-321-11886-3
