

Formulario de aprobación de curso de posgrado/educación permanente

Asignatura: Gestión de la Seguridad de la Información

(Si el nombre contiene siglas deberán ser aclaradas)

Modalidad:

(posgrado, educación permanente o ambas)

Posgrado

Educación permanente

Profesor de la asignatura ¹: Mag. Ing. María Eugenia Corti, Profesor Adjunto, Instituto de Computación
Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación, Mag. Ing. María Fernanda Molina, Asistente,
Instituto de Computación

Profesor Responsable Local ¹:

(título, nombre, grado, instituto)

Otros docentes de la Facultad:

(título, nombre, grado, instituto)

Docentes fuera de Facultad: Mag. Ing. Gustavo Pallas.

(título, nombre, cargo, institución, país)

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)

[Si es curso de posgrado]

Programa(s) de posgrado: Diploma de Especialización Seguridad en Informática, Maestría en Seguridad Informática

Instituto o unidad: Instituto de Computación

Departamento o área: Seguridad Informática

Horas Presenciales: 77

(se deberán discriminar las horas en el ítem Metodología de enseñanza)

Nº de Créditos: 10

[Exclusivamente para curso de posgrado]

(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 enseñanza)

Público objetivo: Profesionales y estudiantes interesados en Seguridad Informática, en particular, profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información.

Cupos: No tiene

(si corresponde, se indicará el número de plazas, mínimo y máximo y los criterios de selección. Asimismo, se adjuntará en nota aparte los fundamentos de los cupos propuestos. Si no existe indicación particular para el cupo máximo, el criterio general será el orden de inscripción, hasta completar el cupo asignado)

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 la metodología de enseñanza y de las horas dedicadas por el estudiante a la asignatura, distribuidas en horas presenciales -de clase práctica, teórico, laboratorio, consulta, etc.- y no presenciales de trabajo personal del estudiante)

Descripción de la metodología:
[Obligatorio]

Detalle de horas:

- 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
 - 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

(título del libro-nombre del autor-editorial-ISBN-fecha de edición)



Facultad de Ingeniería Comisión Académica de Posgrado

Datos del curso

Fecha de inicio y finalización: 11 de agosto al 29 de setiembre de 2025

Horario y Salón: Lunes, miércoles y viernes de 18 a 21 hs.

Arancel: \$50.000

[Si la modalidad no corresponde indique "no corresponde". Si el curso contempla otorgar becas, indíquelo]

Arancel para estudiantes inscriptos en la modalidad posgrado: \$50.000

Arancel para estudiantes inscriptos en la modalidad educación permanente: \$50.000
