
Formulario de aprobación de curso de posgrado/educación permanente

Asignatura: Metodologías para el análisis forense informático

(Si el nombre contiene siglas deberán ser aclaradas)

Modalidad:

(posgrado, educación permanente o ambas)

Posgrado

Educación permanente

Profesor de la asignatura ¹: Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación
(título, nombre, grado o cargo, instituto o institución)

Profesor Responsable Local ¹: Ing. Marcelo Rodríguez, Asistente, Instituto de Computación
(título, nombre, grado, instituto)

Otros docentes de la Facultad:

(título, nombre, grado, instituto)

Docentes fuera de Facultad:

(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: Computación

Departamento o área: Programación, Grupo de Seguridad Informática

Horas Presenciales: 38

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

Nº de Créditos: 5

[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: Estudiantes de posgrado y/o profesionales en áreas afines interesados en Seguridad Informática, y en particular, profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información para el aseguramiento de las organizaciones.

Cupos: Sin cupo

(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 al estudiante en los conceptos básicos del análisis forense informático. El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas. Al finalizar el curso el alumno habrá adquirido los conceptos técnicos básicos necesarios en lo que respecta a las metodologías de análisis y el tratamiento y/o adquisición de la evidencia digital.

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

Conocimientos previos recomendados: Redes de computadores, seguridad en redes, sistemas y aplicaciones

Metodología de enseñanza:

(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]

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 curso se dictará en 8 clases teóricas 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:

[Indique la forma de evaluación para estudiantes de posgrado, si corresponde]

[Indique la forma de evaluación para estudiantes de educación permanente, si corresponde]

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

Temario:

- 1 Bases y Motivación
 - 1.1 Introducción.
 - 1.2 Motivación, definiciones y objetivos del análisis forense informático
 - 1.3 Principios de análisis forense
 - 1.4 Usos del análisis informático forense

 - 2 Evidencia digital
 - 2.1 Tipos de evidencia
 - 2.1.1 Volátil
 - 2.1.2 Persistente
 - 2.1.3 Física
 - 2.1.4 Lógica
 - 2.2 Propiedades (Admisible, autentica, completa, confiable, creíble)
 - 2.3 Fuentes de obtención de evidencias
 - 2.4 Cadena de custodia

 - 3 Tipos de análisis forense
 - 3.1 Análisis post-mortem
 - 3.2 Live análisis
 - 3.3 Análisis On-Site
 - 3.4 Análisis en el laboratorio

 - 4
 - 5 Metodologías para el análisis forense
 - 5.1 Identificación
 - 5.2 Preservación
 - 5.3 Análisis
 - 5.4 Presentación

 - 6
 - 7 Herramientas de soporte a la metodología
 - 7.1 Herramientas de identificación
 - 7.2 Herramientas de preservación
 - 7.3 Herramientas de análisis
 - 7.4 Herramientas de presentación

 - 8 Anti-forense
 - 8.1 Problemáticas y desafíos del análisis forense informático
 - 8.2 Técnicas anti-forenses
 - 8.3 Clasificación de métodos anti-forenses
 - 8.3.1 Destrucción de la evidencia
 - 8.3.2 Ocultar la evidencia
 - 8.3.3 Eliminación de las fuentes de la evidencia.
 - 8.3.4 Falsificación de la evidencia
 - 8.4 Herramientas anti-forenses
-

Bibliografía:

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

Libros

The Basics of Digital Forensics. The Primer for Getting Started in Digital Forensics. Autor: John Sammons, Publisher: Syngress, ISBN-10: 1597496618.

File System Forensic Analysis, Autor: Brian Carrier, Publisher: Addison-Wesley Professional, ISBN-10: 0-321-26817-2.

Handbook of Digital Forensics and Investigation, Autor: Eoghan Casey, Publisher: Academic Press, ISBN-10: 0123742676.

Digital Evidence And Computer Crime, Autor: Eoghan Casey, Publisher: Academic Press, ISBN-10: 0-12-163104-4.

Computación Forense. Descubriendo los rastros informáticos, Autor: Jeimy Cano, Editorial: Alfaomega, ISBN: 978-958-682-767-6.

Artículos

Manual de Peritaje Informático, Autor: Maricarmen Pascale (Coordinadora), Fundación de Cultura Universitaria, 2007.
