Formulario de aprobación de curso de posgrado/educación permanente

Asignatura: Criptografía Aplicada
(Si el nombre contiene siglas deberán ser aclaradas)

Modalidad: (posgrado, educación permanente o ambas)	**Posgrado**	X
	Educación permanente	X

Profesor de la asignatura [1]: Esp. Ing. Germán Gustavo Bollmann. Universidad de la Defensa Nacional, Argentina
(título, nombre, grado o cargo, instituto o institución)

Profesor Responsable Local [1]: Dr. Ing. Gustavo Betarte, Profesor Titular, 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 en Seguridad Informática, Maestría en Seguridad Informática

Instituto o unidad: Computación

Departamento o área: Programación, Grupo de Seguridad Informática

Horas Presenciales: 36
(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: Profesionales y estudiantes 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: Mínimo 10 personas y máximo 30 personas
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 que los estudiantes conozcan los conceptos fundamentos de la criptografía, las principales primitivas criptográficas, así como algunas prácticas de uso que las hacen vulnerables.

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:
El curso consiste de un 66% de exposiciones teóricas (20hs) y el otro 34% (10hs) de trabajos prácticos que son realizados con soporte computacional.

El cuso se dictará en 8 clases teóricas de 2.5 horas cada una, durante 5 semanas y 4 sesiones de práctico de 2.5 horas cada una.

- Horas clase (teórico): 20
- Horas clase (práctico): 10
- Horas clase (laboratorio):
- Horas consulta:3
- Horas evaluación:3
  - Subtotal horas: 36
- Horas estudio: 20
- Horas resolución ejercicios/prácticos: 20
- Horas proyecto final/monografía:
  - Total de horas de dedicación del estudiante: 76

Forma de evaluación:
Se evaluarán los trabajos de práctico y un examen final. La realización de las prácticas es **obligatoria.**

Temario:

1. Introducción a la Seguridad de la información
   a) Definiciones
   b) Diferencias entre seguridad informática y Seguridad de la información
   c) Amenazas

2. Confidencialidad (criptología y criptografía simétrica)
   a) Criptografía y Criptoanálisis.
      i. Requerimientos de la criptografía.
      ii. Tipos de cifrados.
      iii. Cifrado Simétrico.
      iv. Algoritmos estándares.
   b) Funciones unidireccionales y problemas matemáticos

3. Integridad (Hashes criptográficos)
   a) Funciones unidireccionales
   b) Funciones hash.

c) Necesidad de las funciones hash.
d) Funciones estándares.
e) Integridad de los mensajes.

4. Criptografía Asimétrica
   a) Algoritmo de cifra RSA.
      i. Criterios de elección de primos para la cifra.
      ii. Cifrado de información por bloques y de números.
      iii. Debilidades del algoritmo RSA.
   b) Problemas de los algoritmos de clave pública/privada, o Cifrado Asimétrico.
   c) Ataques a RSA por factorización

5. Integridad y Autenticación
   a) Firma digital
   b) Infraestructura de Clave Pública

Bibliografía:

BIBLIOGRAFÍA GENERAL OBLIGATORIA

• Seguridad informática; Costas Santos, Jesus; RA-MA Editorial; 2014
• Schneier, Bruce. (1996). Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley.
• Alfred J. Menezes (2020) “Handbook Of Applied Cryptography", CRC Press, disponible en https://archive.org/details/handbookofappliedcryptographyalfredj.menezes/mode/2up”.

BIBLIOGRAFÍA GENERAL COMPLEMENTARIA

• Criptografía sin secretos con Python; Arboledas Brihuega, David RA-MA Editorial; 2019.
• Alexander, Alberto: (2007), “Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005”. Ed. Alfaomega. ISBN: 978-958-682-713-3.
• Héctor Jara y Federico Pacheco: (2012) “Ethical Hacking 2.0”, USERS Ediciones. ISBN: 978-987-1347-93-3.
• Stallings, William. (2005) “Criptography and Network Security”, 3rd. Ed. Prentice Hall.
• Cangallo Rosenberg, B. (2011). Handbook of financial cryptography and security. Boca Raton: Chapman & Hall/CRC.
• Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (1997). Security in Computing (5th ed.). Upper Saddle River, NJ: Prentice Hall.
• Manuel J. Lucena López (2022) Criptografía y Seguridad en Computadores, disponible en http://criptografiayseguridad.blogspot.com/p/criptografia-y-seguridad-en.html

Datos del curso

Fecha de inicio y finalización: 07 de octubre al 22 de noviembre de 2024

Horario y Salón:

Arancel: $ 24000
[Si la modalidad no corresponde indique “no corresponde”. Si el curso contempla otorgar becas, indíquelo]

Arancel para estudiantes inscriptos en la modalidad posgrado:
Arancel para estudiantes inscriptos en la modalidad educación permanente:

Actualizado por expediente n.º: 060165-000046-23