Formulario de aprobación de curso de posgrado/educación permanente

Asignatura:
Centro de Ensayos de Software: Seguridad Informática y Testing

Modalidad: (posgrado, educación permanente o ambas)

Posgrado	☐
Educación permanente	X

Profesor de la asignatura [1]: Ing. Federico Orihuela, Consultor en Seguridad y Performance, Centro de Ensayos de Software
(título, nombre, grado o cargo, instituto o institución)

Profesor Responsable Local [1]: Lic. Mónica Wodzislawski, Grado 3, Instituto de Computación
(título, nombre, grado, instituto)

Otros docentes de la Facultad:
(título, nombre, grado, instituto)

Docentes fuera de Facultad:
(título, nombre, grado, instituto)

[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)

Instituto o unidad: Centro de Ensayos de Software

Departamento o área:

Horas Presenciales: 12 hs (a distancia, sincrónicas)
(se deberán discriminar las horas en el ítem Metodología de enseñanza)

Nº de Créditos: no corresponde
[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:

- Desarrolladores de software
- Testers de software
- Especialistas en seguridad

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 incorporar herramientas para detectar amenazas y sugerir buenas prácticas en proyectos de desarrollo y mantenimiento de software.

Mediante distintas actividades se plantean interrogantes y se trabaja asimilando los fundamentos de la seguridad informática y de la información.

Conocimientos previos exigidos:
Conocimientos sobre programación y arquitecturas o redes.

Otros requisitos:

- Disponer de 15 a 20 horas semanales para participar en la formación.
- Tener acceso a un PC con Internet y disponer de parlantes y micrófono.
- Requerimientos de hardware / software:
  - PC con 4 GB RAM (mínimo), 6 GB RAM (recomendado).
- Sistemas operativos compatibles:
  - Microsoft Windows, Mac OS X, Linux, Gnome o KDE.

Conocimientos previos recomendados:
No aplica

Metodología de enseñanza:
El curso se dicta en modalidad en línea. Se describe la metodología de enseñanza y las horas dedicadas por el estudiante a la asignatura, distribuidas en horas de participación en videoconferencias y horas dedicadas por el estudiante al trabajo dedicación del estudiante tanto al estudio del material teórico como a la resolución de las actividades planteadas, incluyendo consultas en los foros. (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:
La metodología de enseñanza conjuga elementos de aprendizaje tradicional y de aprendizaje basado en problemas (ABP). El aprendizaje es un proceso constructivo y no receptivo por lo que se plantean problemas que llevan al alumno a comprender mejor el marco teórico para tratar de resolverlos.

El material teórico, que consiste de lecciones previamente preparadas y bibliografía adicional, se pone a disposición del estudiante para su estudio individual. Posteriormente se dictan clases sobre cada tema con el objetivo de aclarar las dudas y/o profundizar sobre aspectos particulares que se considere pertinentes.

El curso tiene un fuerte componente práctico. En cada tema se presentan actividades que permiten a los estudiantes plantear interrogantes, investigar y trabajar en equipo para aplicar el conocimiento teórico y aprender. Estas actividades pueden ser individuales o grupales. Las actividades son corregidas y evaluadas por el docente que devuelve al alumno los comentarios correspondientes para mejorar su rendimiento.

El objetivo de la evaluación es verificar que los estudiantes asimilaron y son capaces de aplicar lo aprendido a problemas reales y no que salven la Prueba final repitiendo información aprendida de memoria.

Detalle de horas:

- Horas de clase (teórico): 5 (videoconferencia, sincrónicas)
- Horas de clase (práctico): 5 (videoconferencia, sincrónicas)
- Horas de clase (laboratorio): 0
- Horas de consulta: 0
- Horas de evaluación: 2
  - Subtotal de horas presenciales: 12 horas sincrónicas (videoconferencia).
- Horas de estudio: 8 horas

- Horas de resolución de ejercicios/prácticos: 40 horas (incluyen horas de consultas en foros)
- Horas proyecto final/monografía: 0
    - Total de horas de dedicación del estudiante: 60 horas

Forma de evaluación:
La evaluación se realizará mediante actividades obligatorias y una prueba final.

Aprobación
Para aprobar el curso se deberá:
- Entregar y participar de toda actividad obligatoria y obtener en promedio un 60% de los puntos de las actividades obligatorias,
- Obtener al menos 60% de los puntos de la prueba final

La nota de cada curso se calcula con el siguiente criterio:
- 50% nota de prueba final,
- 40% nota promedio de todas las actividades del curso,
- 10% rendimiento individual evaluado por el docente, que incluye responsabilidad, motivación, interés, prolijidad, participación de actividades opcionales, foros, videoconferencias (participación sincrónica o asincrónica).

Temario:
- Introducción y objetivos
- Comprobación del sistema de autenticación
- Comprobación del manejo de identidad
- Pruebas de gestión de configuración de la infraestructura
- Recopilación de información
- Guía de pruebas de OWASP
- Seguridad de aplicaciones
- Nociones de tecnologías web Criptografía
- Seguridad informática y seguridad de la información
- Fundamentos de la seguridad informática

Bibliografía:

2011, Dafydd Stuttard . “The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws“
2014, Georgia Weidman. “Penetration Testing: A Hands-On Introduction to Hacking”
2016, William Stallings, “Cryptography and Network Security”
2022, Owasp https://owasp.org/ - consultado el 04/03/2021

Datos del curso

Fecha de inicio y finalización: **A DEFINIR – julio 2022**

Horario y Salón:
No aplica
Arancel: $19.000 (diecinueve mil pesos uruguayos)
[Si la modalidad no corresponde indique “no corresponde”. Si el curso contempla otorgar becas, indíquelo]

Arancel para estudiantes inscriptos en la modalidad posgrado: no corresponde
Arancel para estudiantes inscriptos en la modalidad educación permanente: $19.000