

Formulario de aprobación de curso de posgrado/educación permanente

Asignatura: Seguridad de Redes TCP/IP

(Si el nombre contiene siglas deberán ser aclaradas)

Modalidad:
(posgrado, educación permanente o ambas)

Posgrado

Educación permanente

Profesor de la asignatura ¹: Ing. Alejandro Blanco, Profesor Adjunto, Instituto de Computación, Ing. Leonardo Vidal, Asistente, Instituto de Computación,
Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación

Profesor Responsable Local ¹:

(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 Seguridad en Informática

Instituto o unidad: Instituto de Computación

Departamento o área: Seguridad Informática

Horas Presenciales: 45

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

Nº de Créditos: 6

[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 informática en redes de datos TCP/IP.

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 de la seguridad informática de redes de datos TCP/IP. El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas, con el objetivo de desarrollar, ampliar o mejorar las plataformas de comunicación de datos. Al finalizar el curso el estudiante habrá adquirido los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir una red de datos TCP/IP y establecer los mecanismos de protección adecuados.

Conocimientos previos exigidos: Ninguno

Conocimientos previos recomendados: Conocimientos de informática

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]

- Horas clase (teórico): 30
 - Horas clase (práctico): 0
 - Horas clase (laboratorio): 9
 - Horas consulta: 3
 - Horas evaluación: 3
 - Subtotal horas presenciales: 45
 - Horas estudio: 45
 - Horas resolución ejercicios/prácticos: 0
 - Horas proyecto final/monografía: 0
- Total de horas de dedicación del estudiante: 90

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

- * trabajos de laboratorio.
- * un examen final.

La realización de las prácticas de laboratorio es obligatoria.

Temario:

- 1 Repaso protocolo TCP/IP
 - 1.1 modelo de capas
 - 1.2 interacción y servicios de capas del modelo
 - 1.3 ARP/IP/TCP-UDP/aplicaciones
- 2 Problemas de Seguridad protocolo (redes) TCP/IP
 - 2.1 Autenticación del origen (*IP spoofing*)
 - 2.2 Interacción IP/MAC, *ARP spoofing*
 - 2.3 Ataques a protocolo de ruteo, ICMP.

- 2.4 TCP session Hijacking, SYN Flooding
- 2.5 Capa de Aplicación: Servicio DNS
- 2.6 VLAN
- 3 Redes inalámbricas (WiFi®).
 - 3.1 Requerimientos
 - 3.2 WEP, WPA, WPA2, EAP, 802.1X
 - 3.3 Integración con redes existentes
- 4 Seguridad IP (IPSec)
 - 4.1 Asociaciones de Seguridad (SA)
 - 4.2 Modos de funcionamiento (túnel y transporte)
 - 4.3 Protocolo AH y ESP (encabezados y servicios que ofrecen)
 - 4.4 IPSec Key Management (IKE)
 - 4.5 IPsec y filtrado
- 5 VPN
 - 5.1 ¿Qué es una VPN? VPN sobre Internet
 - 5.2 Implementación de VPN.
- 6 Firewalls
 - 6.1 Definición. Qué puede hacer y que NO un Firewall.
 - 6.2 Filtrado de paquetes, con y sin estados. Generando reglas de filtrado.
 - 6.3 Logging
 - 6.4 Arquitecturas de Firewall.
 - 6.5 Tipos de Firewall.
 - 6.6 Servicios Proxy y NAT.
- 7 IDS/IPS
 - 7.1 Definición.
 - 7.2 Clasificación y Formas de Detección.
 - 7.3 Falsos positivos y negativos
 - 7.4 ¿Acciones automáticas? Donde monitorizar (sensar).
- 8 Otro tipo de sensores. Honeypots
- 9 Diseño de un perímetro seguro
 - 9.1 Identificación de activos a proteger.
 - 9.2 Identificación de fronteras
 - 9.3 Separación e Identificación de zonas de seguridad.

Bibliografía:

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

R. Anderson - Wiley - *Security Engineering – A Guide to Building Dependable Distributed Systems*, ISBN-10: 0470068523 | ISBN-13: 978-0470068526 – 2nd Edition, 2008

D. Gollmann – Wiley, *Computer Security* – ISBN-10: 0470862939 | ISBN-13: 978-0470862933 – 2nd Edition, 2006

E. D. Zwicky, S. Cooper, & B. Chapman - Ed. O'Reilly, *Building Internet Firewalls*, ISBN-10: 1565928717 | ISBN-13: 978-1565928718 - 2nd Edition, 2000.

R. Ziegler, Ed. New Riders, *Linux Firewalls* - 2nd Edition.

Charlie Kaufman, Radia Perlman & Mike Speciner - Prentice Hall, *Network Security: Private Communication in a Public World*, ISBN-10: 0130460192 | ISBN-13: 978-0130460196 - 2nd Edition, 2002.

W. Stallings - Prentice Hall, *Network Security Essentials: Applications and Standards*, ISBN-10: 0136108059 | ISBN-13: 978-0136108054 - 4th Edition, 2010

J. Edney, W. A. Arbaugh - Addison-Wesley Professional, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, ISBN-10: 0321136209 | ISBN-13: 978-0321136206 – 1st Edition, 2003.

Datos del curso

Fecha de inicio y finalización: Desde el 1 de junio al 27 de julio de 2021

Horario y Salón: Martes y jueves de 18 a 21 hs. Laboratorios: 3 (a confirmar fechas) de 18 a 21 hs.

Arancel: \$23.400

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

Arancel para estudiantes inscriptos en la modalidad posgrado: \$23.400

Arancel para estudiantes inscriptos en la modalidad educación permanente: \$23.400
