Universitat de Lleida

GUÍA DOCENTE

SEGURIDAD DE APLICACIONES Y COMUNICACIONES

Coordinación: OJEDA CONTRERAS, JESUS

Año académico 2022-23

SEGURIDAD DE APLICACIONES Y COMUNICACIONES 2022-23

Información general de la asignatura

<table>
<tr><td>Denominación</td><td>SEGURIDAD DE APLICACIONES Y COMUNICACIONES</td></tr>
<tr><td>Código</td><td>102380</td></tr>
<tr><td>Semestre de impartición</td><td>1R Q(SEMESTRE) EVALUACIÓN CONTINUADA</td></tr>
<tr><td>Carácter</td><td>
<table>
<tr><th>Grado/Máster</th><th>Curso</th><th>Carácter</th><th>Modalidad</th></tr>
<tr><td>Grado en Técnicas de Interacción Digital y de Computación</td><td>3</td><td>OBLIGATORIA</td><td>Presencial</td></tr>
</table>
</td></tr>
<tr><td>Número de créditos de la asignatura (ECTS)</td><td>6</td></tr>
<tr><td>Tipo de actividad, créditos y grupos</td><td>
<table>
<tr><th>Tipo de actividad</th><td>PRALAB</td><td>TEORIA</td></tr>
<tr><th>Número de créditos</th><td>3</td><td>3</td></tr>
<tr><th>Número de grupos</th><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordinación</td><td>OJEDA CONTRERAS, JESUS</td></tr>
<tr><td>Departamento/s</td><td>INFORMATICA E INGENIERIA INDUSTRIAL</td></tr>
<tr><td>Distribución carga docente entre la clase presencial y el trabajo autónomo del estudiante</td><td>6 ECTS = 25x6 = 150 horas de trabajo
40% -> 60 horas presenciales
60% -> 90 horas trabajo autónomo del estudiante</td></tr>
<tr><td>Información importante sobre tratamiento de datos</td><td>Consulte este enlace para obtener más información.</td></tr>
<tr><td>Idioma/es de impartición</td><td>Castellano / Catalán</td></tr>
</table>

SEGURIDAD DE APLICACIONES Y COMUNICACIONES 2022-23

Profesor/a (es/as)	Dirección electrónica\nprofesor/a (es/as)	Créditos impartidos por el profesorado	Horario de tutoría/lugar
OJEDA CONTRERAS, JESUS	jesus.ojedacontreras@udl.cat	6	

Información complementaria de la asignatura

Para cualquier duda y/o cuestión, podéis enviar un correo electrónico al profesor de la asignatura.

Objetivos académicos de la asignatura

- Entender los conceptos, problemas y procedimientos de seguridad informática
- Entender los conceptos y mecanismos principales de la criptografía
- Entender y ser capaces de hacer un análisis de riesgos
- Diseñar y configurar esquemas de cortafuegos

Competencias

- CT3. Implementar nuevas tecnologías y tecnologías de la información y la comunicación.
- CG2. Capacidad para diseñar, desarrollar, evaluar y garantizar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas informáticos.
- CG3. Capacidad para utilizar plataformas de hardware y software adecuadas para el desarrollo y ejecución de aplicaciones digitales interactivas.
- CE7. Conocer, administrar y mantener sistemas, servicios y aplicaciones informáticas interactivas.
- CE12. Conocer y saber aplicar las características, funcionalidad y estructura de las redes de ordenadores e internet, y diseñar e implementar aplicaciones interactivas basadas en ellas.

Contenidos fundamentales de la asignatura

1. Fundamentos de seguridad de la información
2. Criptografía
    - Funciones Hash (MD5, SHA)
    - Criptografía simétrica (DES, AES)
    - Criptografía asimétrica (RSA, ElGamal)
3. Seguridad del sistema operativo
    - Sandboxing (chroot)
    - Firewalls (iptables)
4. Riesgos, vulnerabilidades y ataques

Ejes metodológicos de la asignatura

Atendiendo al horario de la asignatura, cada semana el estudiante asiste a 2 horas de Teoria y a 2 horas de laboratorio (PRALAB).

En las sesiones de Teoria se presentan los temas que se pueden consultar en el apartado de contenidos. Incorporan ejemplos ilustrativos y propuestas de problemas para resolver en las clases de laboratorio.

Las sesiones PRALAB se imparten en el laboratorio y presentan problemas y se analizan las soluciones propuestas. También se pueden presentar las prácticas de las asignatura y se realiza el trabajo de laboratorio

correspondiente.

El trabajo autónomo del estudiante consiste en la resolución de los ejercicios propuestos y las tareas de prácticas cuando así se indique.

El lenguage de programación usado en las prácticas es Python. También se usaran máquinas virtuales como VirtualBox.

Plan de desarrollo de la asignatura

Sem	Descripción	Actividad Teoria	Actividad PRALAB	Trabajo autónomo
1	Fundamentos	T1: Fundamentos	Repaso Python	Consulta de bibliografía y programa, Repaso Python
2	Funciones Hash	T2: Criptografia	Python, Presentación P1	P1, Problemas T2
3	Funciones Hash	T2: Criptografia	Problemas T2	P1, Problemas T2
4	Cripto simétrica	T2: Criptografia	P1	P1, Problemas T2
5	Cripto simétrica	T2: Criptografia	Problemas T2	P1, Problemas T2
6	Cripto asimétrica	T2: Criptografia	P1	P1, Problemas T2
7	Cripto asimétrica	T2: Criptografia	P1 - Entrega P1	Problemas T2
8	Sandboxing	T3: Seguridad SO	Dudas T1	Problemas T3
9		1r Parcial		Estudiar
10	Sandboxing	T3: Seguridad SO	Presentación P2	P2, Problemas T3
11	Firewalls	T3: Seguridad SO	P2, Problemas T3	P2, Problemas T3
12	Firewalls	T3: Seguridad SO	P2	P2, Problemas T3
13	Riesgos y Ataques	T4: Riesgos y Ataques	P2, Problemas T4	P2, Problemas T4
14	Riesgos y Ataques	T4: Riesgos y Ataques	Entrega P2	Problemas T4
15	Riesgos y Ataques	T4: Riesgos y Ataques	Dudas T3 y T4	Problemas T4
16/17		2o Parcial		Estudiar
18				
19		Recuperación		Estudiar

Sistema de evaluación

Acr	Actividad de evaluación	Ponderación	Nota Mínima	En grupo	Obligatoria	Recuperable
PE1	Examen 1r Parcial	25%	-	No	No	Sí
PE2	Examen 2o Parcial	25%	-	No	No	Sí
P1	Práctica 1	25%	-	Sí (<=2)	No	No
P2	Práctica 2	25%	-	Sí (<=2)	No	No

Nota Final = 0.25 * PE1 + 0.25 * PE2 + 0.25 * P1 + 0.25 * P2

Recuperación de las pruebas escritas 1 y 2: Si la nota final obtenida en la asignatura es <5, entonces el estudiante puede optar a mejorar/recuperar el 50% que representen las pruebas escritas (el estudiante podrá elegir qué parte quiere recuperar, o elegir las dos partes).

Salvo nueva situación de excepcionalidad, las pruebas escritas serán presenciales.

Bibliografía y recursos de información

- William Stallings. Cryptography and Network Security. Prentice Hall. 2005.
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press. 1996.
- Adam Shostack. Threat modeling: designing for security. Wiley. 2014.
- Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams. Gray Hat Hacking: The Ethical Hackers Handbook. McGraw-Hill. 2011.