Guía docente
270123 - SI - Seguridad Informática

Última modificación: 30/01/2024

Unidad responsable: Facultad de Informática de Barcelona
Unidad que imparte: 701 - DAC - Departamento de Arquitectura de Computadores.

Titulación: GRADO EN INGENIERÍA INFORMÁTICA (Plan 2010). (Asignatura optativa).

Curso: 2023 **Créditos ECTS:** 6.0 **Idiomas:** Catalán, Castellano

PROFESORADO

Profesorado responsable: RENÉ SERRAL GRACIÀ

Otros:

Primer quadrimestre:
ROBERTO BARREDA ORENGA - 11, 13
DAVIDE CAREGLIO - 12
RENÉ SERRAL GRACIÀ - 11, 12, 13

Segon quadrimestre:
ROBERTO BARREDA ORENGA - 11, 12
MARC CATRISSE I PÉREZ - 11, 12

CAPACIDADES PREVIAS

Las obtenidas en las asignaturas Sistemas Operativos y Redes de Computadores.

Conocimientos de inglés técnico.

REQUISITOS

- Pre-Corequisito SO
- Pre-Corequisito XC

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
CT6.4. Demostrar conocimiento y capacidad de aplicación de las características, las funcionalidades y la estructura de los Sistemas Distribuidos, de las Redes de Computadores y de Internet que permita su uso y su administración, así como el diseño y la implementación de aplicaciones basadas en ellas.
CT7.1. Demostrar conocimiento de las métricas de calidad y saber utilizarlas.
CT7.2. Evaluar sistemas hardware/software en función de un criterio de calidad determinado.
CT7.3. Determinar los factores que inciden negativamente en la seguridad y la fiabilidad de un sistema hardware/software, y minimizar sus efectos.
CT8.1. Identificar tecnologías actuales y emergentes y evaluar si son aplicables, y en qué medida, para satisfacer las necesidades de los usuarios.
CTI1.1. Demostrar comprensión del entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.
CTI1.2. Seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.
CTI1.3. Seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización con los criterios de costo y calidad identificados.
CTI2.3. Demostrar comprensión, aplicar y gestionar la garantía y la seguridad de los sistemas informáticos (CEIC6).
CTI3.1. Concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación ubicua.

Genéricas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

METODOLOGÍAS DOCENTES

Esta asignatura ha de dar una visión global y lo más técnica posible de los problemas y soluciones de seguridad en los sistemas informáticos y las redes. Por esta razón, cubre muchos temas y debe tener una componente descriptiva grande.

Sin embargo, la metodología docente utilizará ejemplos y problemas para ir introduciendo los conceptos para que los estudiantes alcancen las competencias necesarias. Además, se intentará fomentar la interactividad con los estudiantes planteando en clase situaciones reales para discutir las soluciones posibles.

Por otra parte, las prácticas en el laboratorio irán completando las capacidades y los conocimientos adquiridos en clase de teoría / problemas.

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

1.Ser capaz de entender las amenazas y riesgos de seguridad de los sistemas informáticos.
2.Ser capaz de analizar malware, como virus, troyanos, etc.
3.Ser capaz de entender e identificar mecanismos de control de acceso de un sistema operativo.
4.Conocer las problemáticas de seguridad en las redes de computadores y ser capaz de encontrar soluciones para protegerlas.
5.Ser capaz de diseñar mecanismos de protección para las aplicaciones distribuidas.
6.Ser capaz de entender la necesidad y funcionamiento de mecanismos forenses a la seguridad informática.
7.Ser capaz de utilizar mecanismos criptográficos para la protección de recursos informáticos.
8.Ser capaz de entender, aplicar y diseñar infraestructuras de clave pública (PKI).
10.Ser capaz de entender los mecanismos de protección y las políticas de seguridad.
11.Ser capaz de gestionar la adquisición, estructuración, análisis y visualización de datos y de información del ámbito de la ingeniería informática, valorando de forma crítica los resultados de esta gestión.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo grande	45,0	30.00
Horas aprendizaje autónomo	84,0	56.00
Horas grupo pequeño	15,0	10.00
Horas actividades dirigidas	6,0	4.00

Dedicación total: 150 h

CONTENIDOS

Introducción

Descripción:
Amenazas, análisis de riesgos, mecanismos de protección, seguridad en las comunicaciones, seguridad forense, políticas, recuperación, aspectos legales, ...

Criptografía

Descripción:
Conceptos básicos de criptografía. Clave pública. Firma electrónica.

Infraestructura PKI

Descripción:
Certificados. Directorios. Protocolos.

Seguridad en las aplicaciones

Descripción:
Seguridad en la web. Protocolos seguros de aplicación.

Seguridad en los sistemas operativos

Descripción:
Analisis de las amenazas. Funcionamiento de los codigos maliciosos. Virus y gusanos. Protección. Antivirus. Estructura de un SO.

Análisis forense

Descripción:
Recopilación de evidencias. Análisis.

ACTIVIDADES

Desarrollo del tema 1. Introducción.

Descripción:
Aprendizaje de los conceptos y objetivos asociados a este tema.

Objetivos específicos:
1, 10

Dedicación: 5h
Grupo grande/Teoría: 1h
Aprendizaje autónomo: 4h

Desarrollo del tema 2. Criptografía.

Descripción:
Aprendizaje de los conceptos y objetivos asociados a este tema.

Objetivos específicos:
7

Dedicación: 18h
Grupo grande/Teoría: 6h
Grupo mediano/Prácticas: 4h
Aprendizaje autónomo: 8h

Desarrollo del tema 3. Infraestructura PKI.

Descripción:
Aprendizaje de los conceptos y objetivos asociados a este tema.

Objetivos específicos:
8

Dedicación: 9h
Grupo grande/Teoría: 3h
Grupo mediano/Prácticas: 1h
Aprendizaje autónomo: 5h

Lab 1. Uso de certificados digitales y apache (HTTPS)

Descripción:
Ser capaz de crear un certificado X.509 con openssl e instalarlo en un servidor web apache para configurar el protocolo HTTPS

Objetivos específicos:
8

Dedicación: 6h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 4h

Primer examen de teoría

Descripción:
Examen de teoría de los primeros temas de la asignatura: Introducción, Criptografía, Infraestructura PKI y seguridad en red

Objetivos específicos:
1, 4, 7, 8, 10

Dedicación: 7h 30m
Actividades dirigidas: 1h 30m
Aprendizaje autónomo: 6h

Desarrollo del tema 4. Seguridad en las aplicaciones.

Descripción:
Aprendizaje de los conceptos y objetivos asociados a este tema.

Objetivos específicos:
5

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 25h
Grupo grande/Teoría: 6h
Grupo mediano/Prácticas: 4h
Aprendizaje autónomo: 15h

Lab 2. Análisis de Vulnerabilidades web

Descripción:
Comprensión de las técnicas de programación seguras descritas en la sesión. Uso de las aplicaciones webscarab y WebGoat de la distribución de linux OWASP

Objetivos específicos:
1, 5

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 8h
Grupo pequeño/Laboratorio: 4h
Aprendizaje autónomo: 4h

Desarrollo del tema 5. Seguridad en los sistemas operativos.

Descripción:
Aprendizaje de los conceptos y objetivos asociados a este tema.

Objetivos específicos:
2, 3

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 23h
Grupo grande/Teoría: 6h
Grupo mediano/Prácticas: 4h
Aprendizaje autónomo: 13h

Lab 5. Análisis de código malicioso

Descripción:
Comprender las diferentes formas de análisis de código malicioso. Ser capaz de utilizar correctamente la herramienta de análisis IDAPro

Objetivos específicos:
1, 2

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 8h
Grupo pequeño/Laboratorio: 4h
Aprendizaje autónomo: 4h

Desarrollo tema 7. Seguridad forense.

Descripción:
Aprendizaje de los conceptos y objetivos asociados a este tema.

Objetivos específicos:
6

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 8h
Grupo grande/Teoría: 3h
Grupo mediano/Prácticas: 2h
Aprendizaje autónomo: 3h

Lab 6. Investigación de un caso forense

Descripción:
Los alumnos aprenderán los procedimientos y metodologías básicas que se deben tener en cuenta a la hora de realizar un análisis forense. También se espera que después del laboratorio aumente su comprensión de las herramientas y aplicaciones forenses necesarias para resolver la mayoría de los incidentes de seguridad en los que se involucra una evidencia digital.

Objetivos específicos:
6

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 6h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 4h

Lab CT. Uso solvente de los recursos bibliográficos

Descripción:
Gestionar la adquisición, estructuración, análisis y visualización de datos y de información del ámbito de la ingeniería informática, valorando de forma crítica los resultados de esta gestión.
- Planificar y utilizar la información necesaria para un trabajo académico (por ejemplo, para el trabajo de fin de grado) a partir de una reflexión crítica sobre los recursos de información utilizados.
- Gestionar la información de forma competente, independiente y autónoma.
- Evaluar la información encontrada e identificar sus lagunas.

Objetivos específicos:
11

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 4h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 2h

Cuestionario sobre el uso solvente de los recursos bibliográficos

Descripción:
Cuestionario sobre el uso solvente de los recursos bibliográficos

Objetivos específicos:
11

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 3h
Actividades dirigidas: 1h
Aprendizaje autónomo: 2h

Segundo examen de teoría

Descripción:
Examen de teoría de los temas de la asignatura: Seguridad en las aplicaciones, seguridad en los sistemas operativos y análisis forense.

Objetivos específicos:
2, 3, 5, 6

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 7h 30m
Actividades dirigidas: 1h 30m
Aprendizaje autónomo: 6h

Examen final de laboratorio

Descripción:
Examen sobre todas las prácticas de laboratorio realizadas a lo largo del curso.

Objetivos específicos:
2, 3, 4, 5, 7, 8

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 5h
Actividades dirigidas: 1h
Aprendizaje autónomo: 4h

Examen final

Descripción:
Examen exclusivo para los alumnos que se han presentado a los dos controles pero no han aprobado la asignatura. El examen es sobre todo el temario.

Objetivos específicos:
1, 2, 3, 4, 5, 6, 7, 8, 10

Competencias relacionadas:
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 7h
Actividades dirigidas: 1h
Aprendizaje autónomo: 6h

SISTEMA DE CALIFICACIÓN

1. Realización de un control (C1) a mitad del cuatrimestre y de un segundo control al final (C2) sobre la materia expuesta en las clases de teoría.
Teoría = 0,5 x C1 + 0,5 x C2

2. Realización de las prácticas:
2.1 Se evaluará a través de entregas y/o cuestionarios individuales por Atenea (NQ)
2.2 Se realizará un examen final de laboratorio (EL).
La nota del laboratorio será: Lab = 0,5 * NQ + 0,5 EL

3. Realización de una actividad individual dedicada a la competencia transversal (CT) propuesta por los profesores de teoría y/o laboratorio relacionada con "Uso solvente de recursos bibliográficos"

La nota final (NF) de la asignatura se calculará de la siguiente forma:
NF = 0,7 x Teoría + 0,25 x Lab + 0,05 x CT

No habrá un examen final, hay la posibilidad de repetir el primer parcial durante el segundo (que se hará en el horario de exámenes al final de curso)

El nivel de consecución de la competencia transversal se evalúa a partir de la CT y se calculará de la siguiente forma:
A si CT >= 8.5; B si CT >=7; C si CT >= 5; D si CT

BIBLIOGRAFÍA

Básica:
- Stallings, W. Network security essentials: applications and standards. 6th ed. Pearson Education, 2017. ISBN 9781292154916.
- Stallings, W. Cryptography and network security: principles and practice. 7th ed. Prentice Hall, 2017. ISBN 9781292158587.
- Stallings, W. Computer Security: Principles and Practice. 4th ed. Prentice Hall, 2018. ISBN 9781292220611.
- Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. Handbook of applied cryptography. CRC Press, 1997. ISBN 0-8493-8523-7.
- Adams, C.; Lloyd, S. Understanding PKI: concepts, standards, and deployment considerations. 2nd ed. Addison-Wesley, 2003. ISBN 0-672-32391-5.

Complementaria:
- Medina, M.; Molist, M. Cibercrimen : ¡protégete del Bit-Bang!, los ataques en el Ciberespacio a : tu ordenador, tu móvil, tu empresa... aprende de víctimas, expertos y CiberVigilantes. Barcelona: Tibidabo, 2015. ISBN 9788416204823.