GUÍA DOCENTE ABREVIADA DE LA ASIGNATURA

G1828 - System and Network Security and Assurance

Grado en Ingeniería Informática

Curso Académico 2022-2023

1. DATOS IDENTIFICATIVOS				
Título/s	Grado en Ingeniería Informática		Tipología y Curso	Optativa. Curso 4
Centro	Facultad de Ciencias			
Módulo / materia	MATERIA INGENIERÍA DE COMPUTADORES MENCIÓN EN INGENIERÍA DE COMPUTADORES			
Código y denominación	G1828 - System and Network Security and Assurance			
Créditos ECTS	6	Cuatrimestre	Cuatrimestral (2)	
Web				
Idioma de impartición	Inglés		Forma de impartición	Presencial

Departamento	DPTO. INGENIERÍA INFORMÁTICA Y ELECTRÓNICA
Profesor responsable	ESTEBAN STAFFORD FERNANDEZ
E-mail	esteban.stafford@gestion.unican.es
Número despacho	Facultad de Ciencias. Planta: + 3. DESPACHO - COORDINACION NUEVO PLAN ESTUDIOS FAC. C (3017)
Otros profesores	

3.1 RESULTADOS DE APRENDIZAJE
- Conocer las técnicas básicas de protección y seguridad de que consta el sistema operativo.
- Conocer los aspectos fundamentales de garantía y seguridad en entornos computacionales distinguiendo las vulnerabilidades y ataques más comunes.
- Conocer los aspectos de seguridad a nivel de sistema y red, así como los mecanismos necesarios para cubrirlos: control de usuarios y accesos, permisos, firewalls, seguridad criptográfica, virus, etc.
- Saber manejar las herramientas adecuadas para configurar una red segura.
- Ser capaces de comunicar de forma efectiva, tanto por escrito como oralmente conocimientos, técnicas, resultados e ideas relacionados con el contenido de la materia estudiada.

4. OBJETIVOS

La sociedad actual depende cada vez más en los sistemas de información. Esta dependencia hace que los efectos de un fallo en estos sistemas pueda desencadenar consecuencias muy graves. Es por ello que un Ingeniero Informático debe conocer la manera de asegurar el funcionamiento de los sistemas a su cargo. Para ello debe cuidar tanto su diseño como su puesta en funcionamiento y explotación.

En el transcurso de la asignatura, el alumno deberá alcanzar los siguientes objetivos:

- Conocer las herramientas criptográficas de uso común en seguridad de computadores. Encriptación simiétrica, asimétrica y funciones de resumen (hash).
- Entender los mecanismos de control de acceso y autenticación. Saber evaluar los riesgos de tales mecanismos y proponer medios paliativos.
- Comprender y saber evaluar los riesgos de seguridad más habituales en sistemas informáticos, tanto a nivel de aplicación, sistema o red.
- Saber aplicar medios que mejoren la seguridad en sistemas y redes informáticos. Seleccionando contramedidas de proteccion, detección, contención y recuperación.

6. ORGANIZACIÓN DOCENTE

CONTENIDOS	
1	Bloque 1: Conceptos Generales 1.1 Introducción 1.2 Herramientas criptográficas 1.3 Autenticación 1.4 Control de Acceso
2	Bloque 2: Seguridad en Software 2.1 Código malintencionado 2.2 Denegación de Servicio 2.3 Desbordamiento de Pila 2.4 Programación segura
3	Bloque 3: Seguridad en Red 3.1 Detección de Intrusión 3.2 Prevención de intrusion y cortafuegos

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Test sobre los contenidos de la asignatura	Examen escrito	No	Sí	80,00
Evaluación de los ejercicios prácticos realizados en el laboratorio	Evaluación en laboratorio	No	Sí	20,00
TOTAL				100,00

Observaciones

Criterios de evaluación para estudiantes a tiempo parcial

Los alumnos matriculados a tiempo parcial realizarán únicamente un examen final con el 100% de la nota.

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA

Computer Security: Principles and Practice, 2nd ed. W. Stallings, L Brown. Pearson Education Limited, 2011.

Esta es la Guía Docente abreviada de la asignatura. Tienes también publicada en la Web la información más detallada de la asignatura en la Guía Docente Completa.