Adenda Docente de la asignatura de Seguridad Informática

Asignatura	Seguridad Informática		
Materia	Planificación y Explotación de Sistemas Informáticos		
Módulo			
Titulación	Grado en Ingeniería Informática de Servicios y Aplicaciones		
Plan	413	**Código**	40823
Periodo de impartición	Semestre 4	**Tipo/Carácter**	OB
Nivel/Ciclo	Grado	**Curso**	2
Créditos ECTS	6 ECTS		
Lengua en que se imparte	Español		
Profesor/es responsable/s	Juan José Álvarez Sánchez		
Datos de contacto (E-mail, teléfono…)	Tel.: +34 921 112430 Fax: +34 921 112401 e-mail: jjalvarez@infor.uva.es		
Departamento	Informática (ATC, CCIA, LSI)		

Contenidos reducidos fundamentales

Bloque 1: Redes de computadoras e Internet. Principios de Criptografía

a. Contextualización y justificación

Introducción del vocabulario y los términos específicos para el estudio pormenorizado de la seguridad en los niveles OSI y TCP/IP.

b. Objetivos de aprendizaje

- Internet y sus protocolos
- Arquitecturas cliente-servidor.
- Conceptos básicos de criptografía

c. Contenidos

1.1 ¿Qué es Internet?
1.1.1 Descripción de los componentes esenciales
1.1.2 Descripción de los servicios
1.1.3 ¿Qué es un protocolo?
1.2 La frontera de la red
1.2.1 Programas cliente y servidor
1.2.2 Redes de acceso

1.2.3 Medios físicos

1.3 Capas de protocolos y sus modelos de servicio
1.3.1 Arquitectura en capas
1.3.2 Mensajes, segmentos, datagramas y tramas

1.4 Fundamentos de criptografía
1.4.1 Criptografía de clave privada
1.4.2 Criptografía de clave pública

Bloque 2: La capa de aplicación

a. Contextualización y justificación

Esta es la capa con la que se encuentra el usuario y por tanto es muy importante conocer de primera mano sus funcionalidades para dar un servicio apropiado de seguridad en la red.

b. Objetivos de aprendizaje

- Dominar los protocolos de seguridad de los servicios HTTP, Correo electrónico y aplicaciones P2P.

c. Contenidos

2.1 La Web y HTTP
2.1.1 Introducción a HTTP
2.1.2 Conexiones persistentes y no persistentes
2.1.3 Formato de los mensajes HTTP
2.1.4 Interacción usuario-servidor: cookies
2.1.5 Almacenamiento en caché web
2.1.6 GET condicional

2.2 Transferencia de archivos: FTP
2.2.1 Comandos y respuestas de FTP

2.3 Correo electrónico en Internet
2.3.1 SMTP
2.3.2 Comparación con HTTP
2.3.3 Formatos de los mensajes de correo
2.3.4 Protocolos de acceso para correo electrónico

2.4 DNS: servicio de directorio de Internet
2.4.1 Servicios proporcionados por DNS
2.4.2 Cómo funciona DNS
2.4.3 Registros y mensajes DNS

2.5 Seguridad en la capa de aplicación

Bloque 3: Seguridad en la capa de transporte

a. Contextualización y justificación

Esta capa gestiona los protocolos más usados para las comunicaciones síncronas y asíncronas en Internet; de ahí la importacia del estudio de la seguridad en este ámbito.

b. Objetivos de aprendizaje

- Entender los procesos de cifrado SSL.
- Manejarse con el entorno Openssl

c. Contenidos

3.1 Transporte sin conexión: UDP
3.1.1 Estructura de los segmentos UDP
3.1.2 Suma de comprobación de UDP

3.2 Transporte orientado a la conexión: TCP
3.2.1 La conexión TCP
3.2.2 Estructura del segmento TCP
3.2.3 Estimación del tiempo de ida y vuelta y fin de temporización
3.2.6 Gestión de la conexión TCP

3.3 Seguridad en el protocolo TCP: SSL

Trabajos: Lista de Trabajos propuestos para la evaluación de la asignatura

A continuación se propone una lista de trabajos de donde los alumnos tendrán que elegir uno. Se entregará vía email y no tendrá una extensión superior a las 2000 palabras:

1. Descifrando Enigma
2. Protocolo de seguridad SSL
3. Ataques de ramsonware en tiempos del COVID-19
4. Principios de la Criptografía cuántica
5. Redes Virtuales Privadas (VPN)
6. Curvas Elípticas y su aplicación a la seguridad informática
7. Seguridad en el protocolo IPv6
8. Seguridad Wireless; situación actual
9. Descifrando Tor; análisis de su arquitectura
10. Criptografía de clave pública: algoritmo de Diffie-Hellman y RSA

Principios Metodológicos No Presenciales

1. Redacción, por parte del alumnado, de trabajos sobre problemas típicos como aplicación a los conceptos fundamentales de la asignatura. Todo el material del curso está a disposición del alumnado en el escritorio virtual de la asignatura.
2. Entrega de trabajos (obligatorio)

Resolución de dudas y entrega de los mismos a través de procesos telemáticos asíncronos o síncronos dependiendo de la contectividad de alumn@ y profesor.

Horas de dedicación a la asignatura

+ Estudio personal de los contenidos del Campus Virtual: 50 horas
+ Realización individual de los ejercicios de consolidación del Campus Virtual: 30 horas
+ Tutorías individuales o en grupo con el profesor: 10 horas
+ Actividades de evaluación: 10 horas
TOTAL: 100 horas

Criterios y sistemas de evaluación

- La comprensión de contenidos y su aplicación mediante la redacción de trabajos escritos, serán evaluados mediante la entrega de los mismos a través de procesos telemáticos.

- Esta se complementará con una evaluación personalizada mediante el uso de cuestionarios a través de procesos telemáticos.

- La evaluación de la **convocatoria extraordinaria** se realizará mediante la misma metodología y criterios que la convocatoria ordinaria.

. Tabla resumen del procedimiento de evaluación/calificación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Calificación del trabajo enviado al profesor por medios telemáticos (preferiblemente e-mail)	60%	El trabajo de se realizará con una fuente de tamaño 12 y un interlineado de 1,5. El formato del documento será en PDF
Cuestionario personalizado de cinco preguntas sobre el mencionado trabajo.	40%	El cuestionario personalizado se realizará en la fecha determinada por el profesor para cada trabajo y puede ser asíncrono u oral, según las posibilidades conectivas del profesor y el alumno.