Universidad Rey Juan Carlos

GUÍA DOCENTE

SEGURIDAD EN REDES DE ORDENADORES

GRADO EN INGENIERIA EN TELEMATICA

CURSO 2017-18

Fecha de publicación: 14-07-2017

I.-Identificación de la Asignatura	
Tipo	OPTATIVA
Período de impartición	3 curso, 2Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

II.-Presentación

En esta asignatura se tratan los aspectos básicos de la seguridad en redes de ordenadores y sistemas de computación distribuidos y centralizados, cubriendo los conceptos teóricos básicos, el uso de herramientas criptográficas, protocolos de red seguros, protección ante ataques comunes y software dañino (malware), técnicas para el desarrollo de software seguro, y administración segura de servicios.
Los conocimientos previos necesarios para cursar esta asignatura son: programación imperativa, construcción de aplicaciones distribuidas, protocolos de red TCP/IP, y uso básico de sistemas operativos.

III.-Competencias

Competencias Generales

CG03. Conocimiento de materias básicas y tecnologías, que le capacite para el aprendizaje de nuevos métodos y tecnologías, así como que le dote de una gran versatilidad para adaptarse a nuevas situaciones.
CG04. Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad, y de comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico de Telecomunicación.

Competencias Específicas

CE22. Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos.

IV.-Contenido

IV.A.-Temario de la asignatura

- Tema 1. “Introducción y definiciones básicas”. Definiciones y conceptos básicos de seguridad a nivel de usuario. Identificación de riesgos. Identificación de activos. Análisis coste/beneficio.
- Tema 2. “Herramientas Criptográficas”. Confidencialidad, integridad, no-repudio. Uso de herramientas criptográficas simétricas y asimétricas. Cifrado en bloques y modos de operación. Resúmenes (hash). Firma digital. Generación, almacenamiento, e intercambio de claves. Generación de números pseudoaleatorios. Certificados X509. IPK. Web of Trust y PGP
- Tema 3. “Autenticación y control de acceso”. Estudio de la identificación, autenticación, autorización y control de acceso de usuarios y aplicaciones. Esquemas centralizados (UNIX) y distribuidos (Plan 9). ACLs. Capabilities. RBAC. Almacenamiento de secretos. Ataques clásicos.
- Tema 4. "Malware". Descripción de los distintos tipos de software dañino (malware). Virus. Troyanos. Gusanos. Exploits. Rootkits. Key-loggers. Spyware. Técnicas comunes de ataques a programas: vulnerabilidades de pila, de montón, etc.
- Tema 5. "Desarrollo de aplicaciones seguras". Técnicas de programación para la creación de programas seguros. Uso correcto de buffers. Tratamiento de cadenas de texto. Privilegio de ejecución. Protección de estructuras de datos. Protección de datos en memoria.
- Tema 6. “Protocolos red seguros y redes privadas virtuales”. Funcionamiento y uso de protocolos de red seguros (IPsec, OpenSSH, etc.). Configuración de redes privadas virtuales.
- Tema 7. "Seguridad perimetral". Cortafuegos. Tipos de filtrado. IDS. Test de penetración.
- Tema 8. "Criptomonedas y Blockchain". Fundamentos y funcionamiento de las criptomonedas. Tecnología Blockchain.

IV.B.-Actividades formativas

Tipo	Descripción
Laboratorios	Uso de herramientas de cifrado (openssl, GPG)
Laboratorios	Desarrollo de herramientas de seguridad con la biblioteca openssl (HMAC, firma digital)
Laboratorios	Prácticas de comunicaciones seguras en red (IPsec y OpenVPN)
Laboratorios	Prácticas de seguridad perimetral (snort, iptables y nmap)

V.-Tiempo de Trabajo	
Clases teóricas	26
Clases prácticas de resolución de problemas, casos, etc.	4
Prácticas en laboratorios tecnológicos, clínicos, etc.	26
Realización de pruebas	4
Tutorías académicas	16
Actividades relacionadas: jornadas, seminarios, etc.	2
Preparación de clases teóricas	20
Preparación de clases prácticas/problemas/casos	70
Preparación de pruebas	12
Total de horas de trabajo del estudiante	180

VI.-Metodología y plan de trabajo

Tipo	Periodo	Contenido
Laboratorios	Semana 3 a Semana 7	Desarrollo de herramientas de seguridad con la biblioteca openssl (HMAC, firma digital)
Clases Teóricas	Semana 10 a Semana 10	Teoría tema 7
Prácticas	Semana 9 a Semana 12	Prácticas de seguridad perimetral (snort, iptables y nmap)
Clases Teóricas	Semana 13 a Semana 13	Teoría tema 8
Laboratorios	Semana 12 a Semana 12	Prácticas con bitcoin
Laboratorios	Semana 7 a Semana 9	Prácticas de comunicaciones seguras en red (IPsec y OpenVPN)
Clases Teóricas	Semana 9 a Semana 9	Teoría tema 6
Clases Teóricas	Semana 1 a Semana 1	Teoría tema 1
Clases Teóricas	Semana 1 a Semana 3	Teoría tema 2
Clases Teóricas	Semana 3 a Semana 4	Teoría tema 3
Clases Teóricas	Semana 5 a Semana 6	Teoría tema 4
Clases Teóricas	Semana 6 a Semana 7	Teoría tema 5
Clases Teóricas	Semana 7 a Semana 9	Teoría tema 6

Clases Teóricas	Semana 9 a Semana 12	Teoría tema 7
Laboratorios	Semana 2 a Semana 3	Uso de herramientas de cifrado (openssl, GPG)

VII.-Métodos de evaluación

VII.A.-Ponderación para la evaluación

Evaluación Ordinaria: Si el profesorado considera que la asistencia es obligatoria deberá especificarse con precisión.
(Nota: para no admitir a una prueba a un estudiante por no cumplir con el mínimo de asistencia, se deberá poder justificar por el profesor utilizando un sistema probatorio, como por ejemplo, una hoja de firmas)
La distribución y características de las pruebas de evaluación son las que se describen a continuación. Atendiendo a las características específicas de cada grupo el profesor podrá, en las primeras semanas de curso, introducir cambios que considere oportunos comunicándolo al Vicerrectorado de Calidad.
Evaluación extraordinaria: Los alumnos que no consigan superar la evaluación ordinaria, o no se hayan presentado, serán objeto de la realización de una evaluación extraordinaria para verificar la adquisición de las competencias establecidas en la guía.

Descripción de las pruebas de evaluación y su ponderación

•Entrega de prácticas. Ponderación: 30%
•Prueba escrita sobre teoría. Ponderación: 40%
•Prueba escrita sobre las prácticas. Ponderación: 30%
Cada apartado se puntuará de 0 a 10, para superar la asignatura es necesario al menos 4 puntos en la prueba de teoría y una media ponderada de 5 puntos.

VII.B.-Evaluación de alumnos con dispensa académica

Para que un alumno pueda optar a esta evaluación, tendrá que obtener la 'Dispensa Académica' para la asignatura, que habrá solicitado al Decano/a o Director/a del Centro que imparte su titulación. La Dispensa Académica se podrá conceder siempre y cuando las peculiaridades propias de la asignatura lo permitan.

Asignatura con posibilidad de dispensa: Si

VII.C.-Revisión de las pruebas de evaluación

Conforme a la normativa de reclamación de exámenes de la Universidad Rey Juan Carlos.

VII.D.-Estudiantes con discapacidad o necesidades educativas especiales

Las adaptaciones curriculares para estudiantes con discapacidad o con necesidades educativas especiales, a fin de garantizar la igualdad de oportunidades, no discriminación, la accesibilidad universal y la mayor garantía de éxito académico serán pautadas por la Unidad de Atención a Personas con Discapacidad en virtud de la Normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.
Será requisito imprescindible para ello la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que los estudiantes con discapacidad o necesidades educativas especiales deberán contactar con ella, a fin de analizar conjuntamente las distintas alternativas.

VII.E.-Conducta Académica

Véase normativa de conducta académica

VIII.-Recursos y materiales didácticos
Bibliografía
Cryptography and Network Security: Principles and Practice. William Stallings. Ed. Prentice Hall
Data and Computer Communications. William Stallings. Ed. Prentice Hall
Computer Networking: A Top-Down Approach. James F. Kurose. Ed. Addison Wesley
T. S. Denis, Cryptography for Developers, Syngress Publishing, 2006.
D. Gollmann, Computer Security, John Wiley &Sons, 2011.
N. Daswani, C. Kern, A. Kesavan, Foundations on Security, Apress, 2007.
Applied Cryptography. Bruce Schneier. Ed. Wiley
Practical UNIX and Internet Security. Simson Garfinkel, Gene Spafford, Alan Schwartz. Ed. O'Reilly Media
Bibliografía de consulta
Building and Integrating Virtual Private Networks. Markus Feilner. Ed. Packt Publishing
The Art of Deception. Kevin Mitnik. Ed. Wiley
Beginning OpenVNP. Markus Feilner, Norbert Graf. Ed. Packt Publishing
Beyond Fear. Bruce Schneier. Ed. Springer
Security for Ubiquitous Computing. Frank Stajano. Ed. Wiley
D. Salomon, Foundations of computer security, 2005.
J. Viega, The myths of security, Oreilly, 2009.

IX.-Profesorado	
Nombre y apellidos	ENRIQUE SORIANO SALVADOR
Correo electrónico	enrique.soriano@urjc.es
Departamento	Teoría de la Señal y las Comunicaciones y Sistemas Telemáticos y Computación
Categoría	Profesor Contratado Doctor
Titulación académica	Doctor
Responsable Asignatura	Si
Horario de Tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/-a a través de correo electrónico
Nº de Quinquenios	2

Nº de Sexenios	2
Tramo Docentia	-
Nombre y apellidos	EVA MARIA CASTRO BARBERO
Correo electrónico	eva.castro@urjc.es
Departamento	Teoría de la Señal y las Comunicaciones y Sistemas Telemáticos y Computación
Categoría	Titular de Universidad interino
Titulación académica	Doctor
Responsable Asignatura	No
Horario de Tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/-a a través de correo electrónico
Nº de Quinquenios	2
Nº de Sexenios	0
Tramo Docentia	-