Seguridad en Sistemas y Redes de Telecomunicación

Guía de Aprendizaje – Información al estudiante

1. Datos Descriptivos

Asignatura	Seguridad en Sistemas y Redes de Telecomunicación
Materia	M10 – Tecnología Específica de Telemática
Departamento responsable	Ingeniería de Sistemas Telemáticos
Créditos ECTS	4,5
Carácter	Obligatoria
Titulación	Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación
Curso	Cuarto
Especialidad	Itinerario en Telemática

Curso académico	2014-2015
Semestre en que se imparte	Primero
Idioma en que se imparte	Castellano
Página Web	Sitio Moodle de la asignatura

2. Profesorado

NOMBRE Y APELLIDO	DESPACHO	Correo electrónico
Víctor A. Villagrá González (Coordinador)	B-217	villagra@dit.upm.es
José A. Mañas Argemí	C-219	pepe@dit.upm.es

3. Conocimientos previos requeridos para poder seguir con normalidad la asignatura

Asignaturas superadas	N/A
Otros resultados de aprendizaje necesarios	• Fundamentos de Telemática • Redes y Servicios de Telecomunicación • Redes de Ordenadores

4. Objetivos de Aprendizaje

COMPETENCIAS ASIGNADAS A LA ASIGNATURA Y SU NIVEL DE ADQUISICIÓN		
Código	Competencia	Nivel
CG1-13	Todas las asignaturas del Plan de Estudios contribuyen en mayor o menor medida a la consecución de las competencias generales del perfil de egreso.	2
CECT1	Capacidad para aprender de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo o la explotación de sistemas y servicios de telecomunicación.	1
CECT6	Capacidad de concebir, desplegar, organizar y gestionar redes, sistemas, servicios e infraestructuras de telecomunicación en contextos residenciales (hogar, ciudad y comunidades digitales), empresariales o institucionales responsabilizándose de su puesta en marcha y mejora continua, así como conocer su impacto económico y social	1
CE-TL1	Capacidad de construir, explotar y gestionar las redes, servicios, procesos y aplicaciones de telecomunicaciones, entendidas éstas como sistemas de captación, transporte, representación, procesado, almacenamiento, gestión y presentación de información multimedia, desde el punto de vista de los servicios telemáticos.	2
CE-TL2	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.	3
CE-TL3	Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis	1
CE-TL4	Capacidad de describir, programar, validar y optimizar protocolos e interfaces de comunicación en los diferentes niveles de una arquitectura de redes.	1
CE-TL5	Capacidad de seguir el progreso tecnológico de transmisión, conmutación y proceso para mejorar las redes y servicios telemáticos.	2
CE-TL6	Capacidad de diseñar arquitecturas de redes y servicios telemáticos.	2

LEYENDA: Nivel de adquisición 1: Básico
Nivel de adquisición 2: Medio
Nivel de adquisición 3: Avanzado

RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA			
Código	**Resultado de aprendizaje**	**Competencias asociadas**	**Nivel de adquisición**
RA1	Comprender la necesidad de introducir la seguridad en las redes y sistemas de telecomunicación como parte integral de su diseño y despliegue.	CECT6, CE-TL1, CE-TL2	3
RA2	Ser capaz de abordar correctamente una planificación de política y servicios de seguridad basándose en un análisis de riesgos.	CE-TL2, CE-TL3	2
RA3	Conocer las principales técnicas criptográficas simétricas y asimétricas y su aplicación a la seguridad de los sistemas y comunicaciones.	CE-CT1, CE-TL2, CE-TL4	1
RA4	Conocer el funcionamiento de las amenazas técnicas y humanas a la seguridad de las redes y sistemas de telecomunicación	CE-CT1, CE-TL2, CE-TL4, CE-TL5	2
RA5	Categorizar adecuadamente los distintos servicios de seguridad para redes y sistemas, en función de los activos que protegen.	CE-TL2, CE-TL4, CE-TL5, CE-TL6	3
RA6	Comprender los distintos mecanismos de seguridad basados en control de acceso: autenticación y defensa perimetral.	CE-TL2, CE-TL4, CE-TL6	3
RA7	Comprender y analizar distintos protocolos de seguridad, y cómo se aplican las técnicas criptográficas en las comunicaciones	CE-TL2, CE-TL4, CE-TL6	3

LEYENDA: Nivel de adquisición 1: Conocimiento
Nivel de adquisición 2: Comprensión y aplicación
Nivel de adquisición 3: Análisis y síntesis

5. Sistema de evaluación de la asignatura

INDICADORES DE LOGRO		
Ref	**Indicador**	**Relaciona-do con RA**
I1.1	Comprender la importancia de la seguridad en los sistemas y redes de telecomunicación y ser consciente de su papel clave en las fases de diseño y despliegue de redes y sistemas.	RA1
I2.1	Conocer y aplicar la planificación de servicios de seguridad usando el ciclo de seguridad de sistemas.	RA2
I2.2	Comprender los objetivos y las etapas del análisis de riesgos en entornos de telecomunicación y utilizar las herramientas que facilitan su aplicación.	RA2
I2.3	Ser capaz de realizar un análisis de riesgos de escenarios de redes y sistemas de telecomunicación.	RA2
I2.4	Conocer los distintos elementos de una estructura organizativa de la seguridad de telecomunicaciones en una organización, con sus distintos roles y funciones.	RA2
I2.5	Comprender y aplicar distintas métricas e indicadores globales de riesgo en un entorno de gestión de la seguridad en una organización	RA2
I3.1	Conocer la necesidad de los algoritmos criptográficos en la seguridad de redes y sistemas de telecomunicación. Conocer los principales algoritmos criptográficos simétricos a lo largo de la historia.	RA3
I3.2	Conocer la motivación y necesidad de los algoritmos asimétricos y las funciones resumen. Comprender el funcionamiento de los principales algoritmos asimétricos y de resumen existentes y sus aplicaciones a la seguridad de las comunicaciones.	RA3
I3.3	Conocer la problemática de los ataques a las claves públicas de los algoritmos asimétricos y su solución mediante certificación de claves públicas y la Infraestructura de Clave Pública.	RA3
I3.4	Comprender las funciones de la firma electrónica y sus implicaciones en distintos escenarios, como firmas de larga duración. Conocer los productos y sistemas certificados de firma electrónica.	RA3

INDICADORES DE LOGRO		
Ref	**Indicador**	**Relaciona-do con RA**
I4.1	Conocer las distintas amenazas actuales a sistemas y redes de telecomunicación, tanto desde el punto de vista de amenazas humanas como tecnológicas, comprendiendo el origen de las distintas vulnerabilidades tecnológicas existentes actualmente.	RA4
I4.2	Utilizar y comprender herramientas de escaneo de vulnerabilidades.	RA4
I5.1	Conocer la problemática de la autenticación y comprender los distintos sistemas de autenticación existentes y sus ventajas e inconvenientes.	RA5, RA6
I6.1	Comprender el problema de la autenticación en sistemas y redes inseguras y conocer los principales mecanismos de autenticación dinámica.	RA6
I6.2	Comprender la problemática la autenticación en múltiples sistemas y los principales sistemas de gestión de autenticación de Single Sign On.	RA6
I6.3	Comprender las bases de la defensa perimetral de sistemas y red, con las distintas tecnologías que se pueden utilizar para ello.	RA6
I6.4	Conocer los principios de diseño de políticas de reglas de seguridad de defensa perimetral. Diseñar políticas de reglas para distintos escenarios y requisitos. Utilizar herramientas para su diseño y despliegue.	RA6
I6.5	Conocer los principales sistemas que permiten complementar la figura del cortafuegos en un escenario de defensa perimetral.	RA6
I7.1	Analizar las distintas ventajas e inconvenientes de la aplicación de protocolos de seguridad en los distintos niveles de la torre de comunicaciones.	RA7
I7.2	Conocer los principales protocolos de seguridad en las comunicaciones a nivel de red, transporte y aplicación.	RA7

EVALUACION SUMATIVA			
Breve descripción de las actividades evaluables	**Momento**	**Lugar**	**Peso en la calif.**
Prueba parcial 1 de evaluación	Semana 8	Aula, Convocatoria de examen parcial	40%
Prueba parcial 2 de evaluación	Convocatoria oficial	Aula, Convocatoria oficial	40%
Realización y entrega de trabajos	Semanas 2 y 7	Moodle	10%
Realización y entrega de prácticas de laboratorio	Semanas 12 y 13	Aula, Moodle	10%
			Total: 100%

CRITERIOS DE CALIFICACIÓN

En convocatoria ordinaria, los alumnos serán evaluados mediante evaluación continua, según los criterios especificados más abajo. Los alumnos que lo deseen podrán, no obstante, ser evaluados en convocatoria ordinaria mediante una única prueba final siempre y cuando así lo expresen mediante escrito formalizado en el registro de la ETSI Telecomunicación y dirigido al Director del Departamento de Ingeniería de Sistemas Telemáticos no más tarde del 30 de septiembre. La presentación de este escrito supondrá la renuncia automática a la evaluación continua.

CONVOCATORIA ORDINARIA: MODALIDAD EVALUACIÓN CONTINUA

La asignatura se aprobará cuando se obtenga una calificación mayor o igual a 5 puntos sobre un total de 10, según las normas que se indican en este apartado.

La nota final se obtendrá mediante la suma de las calificaciones correspondientes a las diferentes actividades de evaluación, con los siguientes pesos:

- Prueba parcial 1: 40%
- Prueba parcial 2: 40%
- Realización y entrega de trabajos: 10%
- Realización y entrega de prácticas de laboratorio: 10%

En todos ellos se exige una nota mínima de 4 sobre 10.

La materia de los temas 1, 2, 3, 4 y 5 será evaluada mediante un examen parcial 1. En caso de obtener menos de 4 puntos o desear subir nota, el alumno deberá presentarse a la recuperación en la convocatoria oficial de examen, renunciando a la nota del primer parcial-

CONVOCATORIA ORDINARIA: EVALUACIÓN MEDIANTE UNA ÚNICA PRUEBA FINAL

El 100% de la calificación de los alumnos que presenten el escrito arriba referido se otorgará en función de una única prueba final a celebrar en la fecha que determine Jefatura de Estudios.

CONVOCATORIA EXTRAORDINARIA

La evaluación de la asignatura en su convocatoria extraordinaria se realizará mediante una única prueba final a celebrar en la fecha que determine Jefatura de Estudios, con independencia de la opción elegida en la convocatoria ordinaria.

6. Contenidos y Actividades de Aprendizaje

CONTENIDOS ESPECÍFICOS		
Bloque / Tema / Capítulo	**Apartado**	**Indicadores Relaciona-dos**
Tema 1: Introducción a la Seguridad	1.1 Seguridad en Redes y Sistemas de Telecomunicación	I1.1
	1.2 Motivación e importancia de la Gestión de la Seguridad	I1.1
Tema 2: Criptografía	2.1 Funciones Resumen.	I3.1
	2.2 Criptografía de Clave Simétrica	I3.1
	2.3 Criptografía de Clave Pública	I3.2
Tema 3: Firma Electrónica	3.1 Infraestructura de Clave Pública (PKI)	I3.2, I3.3
	3.2 Firmas de Larga Duración	I3.4
	3.3 Productos y Sistemas Certificados	I3.4
Tema 4: Gestión de Riesgos	4.1 Análisis de Riesgos.	I2.1, I2.2, I2.3
	4.2 Tratamiento de los Riesgos	I2.2, I2.3
	4.3 Marco Regulatorio de los Análisis de Riesgos	I2.2, I2.3
Tema 5: Gestión de la Seguridad	5.1 Roles y Funciones	I2.4
	5.2 Métricas e Indicadores de Seguridad	I2.5
Tema 6: Amenazas de Internet	6.1 Amenazas Humanas	I4.1
	6.2 Amenazas Tecnológicas	I4.1, I4.2
Tema 7: Servicios de Control de Acceso	Sistemas de Autenticación	I5.1
	Sistemas de Autenticación Dinámica	I6.1
	Gestión de Autenticación: Sistemas SSO	I6.2
	Defensa Perimetral de Sistemas	I6.3
	Funciones y Tipos de Cortafuegos de Red	I6.3
	Diseño de Políticas de Reglas de Cortafuegos	I6.4
	Características Avanzadas de Cortafuegos	I6.3
	Arquitectura de Seguridad en Red	I6.5

Tema 8: Servicios de Protección de la Comunicación	Seguridad en las Comunicaciones	I7.1
	Seguridad a nivel de red: IPSEC	I7.2
	Seguridad a nivel de transporte: SSL/TLS	I7.2
	Seguridad a nivel de aplicación	I7.2

7. Breve descripción de las modalidades organizativas utilizadas y de los métodos de enseñanza empleados

CLASES DE TEORÍA	Se exponen los conceptos, herramientas y ejemplos de los temas de Seguridad en Sistemas y Redes de Telecomunicación.
VISITAS	Dependiendo de su disponibilidad, se realizará una visita a un centro empresarial de gestión de la seguridad en una organización.
CONFERENCIAS	Se invitará a expertos del mundo empresarial a impartir conferencias a los alumnos en temas relacionados con la aplicación de los conceptos en el mundo empresarial.
TRABAJOS	A lo largo del curso se propondrán varios trabajos para que los alumnos los resuelvan individualmente. Estos trabajos serán evaluados.
PRÁCTICAS DE LABORATORIO	Se propondrán dos prácticas de laboratorio que permitan poner en práctica en entorno realista diversos conceptos de la asignatura
TUTORÍAS	Las tutorías se ajustarán a la normativa vigente.

8. Recursos didácticos

BIBLIOGRAFÍA	W. Stallings. “Cryptography and Network Security: Principles and Practice”. 6 Edition. Prentice Hall. 2013.
	B. Schneier. “Applied Cryptography”. John Wiley & Sons. 2ª ed. 1995. http://www.wiley.com/
	W. Chesswick, S. Bellovin & A. Rubin. “Firewalls and Internet Security”. Addison-Wesley, 2ª Edición 2003.
	“Criptografía y Seguridad en Computadores”. M. J. Lucena. 4 Edicion. Marzo 2010.
	Apuntes propios de la asignatura
RECURSOS WEB	Sitio Moodle de la asignatura
EQUIPAMIENTO	Aula
	Laboratorio
	Sala de trabajo en grupo

9. Cronograma de trabajo de la asignatura

Semana	Actividades en Aula	Actividades en Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades de Evaluación	Otros
Semana 1 (7 horas)	Tema 1: Introducción y Motivación. Tema 2: Funciones Resumen. Criptografía Simétrica. (3h)		• Estudio (2h) • Familiarización con herramientas (2h)			
Semana 2 (8 horas)	Tema 2: Criptografía de Clave Pública. Trabajo de Criptografía de Clave Pública (3h)		• Estudio (2h) • Realización del trabajo (3h)		Entrega del trabajo	
Semana 3 (6 horas)	Tema 3. Infraestructura de Clave Pública (PKI). Firmas de Larga Duración. Productos y Sistemas Certificados (3h)		• Estudio (3h)			
Semana 4 (9 horas)	Tema 4. Análisis de Riesgos. Tratamiento de los Riesgos. Marco Regulatorio. (3h)		• Estudio (4h) • Familiarización con herramientas (2h)			
Semana 5 (6 horas)	Trabajo de Gestión de Riesgos (3h)		• Realización del Trabajo (3h)			
Semana 6 (7 horas)	Trabajo de Gestión de Riesgos. Tema 5: Gestión de la Seguridad (3h)		• Estudio (2h) • Realización del Trabajo (2h)		Entrega del trabajo	
Semana 7 (9 horas)	Tema 5: Gestión de la Seguridad. Conferencia (3h)		• Estudio (2h) • Preparación Examen Parcial 1 (4h)			

Semana 8 (12 horas)	Tema 6: Amenazas de Internet Tema 7: Sistemas de Autenticación (3h)		• Estudio (2h) • Preparación Examen Parcial 1 (3h) • Búsqueda de Herramientas (2h)		Examen Parcial 1 (2h)	
Semana 9 (9 horas)	Tema 7: Sistemas de Autenticación. Autenticación Dinámica. Sistemas SSO. (3h)		• Estudio (4h) • Búsqueda de Herramientas (2h)			
Semana 10 (7 horas)	Tema 7: Sistemas SSO. Defensa Perimetral de Sistemas. Cortafuegos de Red. (3h)		• Estudio (3h) • Solución de Escenarios (1h)			
Semana 11 (7 horas)	Tema 7: Cortafuegos de Red. Reglas de Cortafuegos. Características Avanzadas. Arquitectura Seguridad en Red (3h)		• Estudio (3h) • Solución de Escenarios (1h)			
Semana 12 (5 horas)	Conferencia (1h)	Práctica de Explotación Vulnerabilidades (2h)	• Familiarización con herramientas y escenario de laboratorio (2h)		Entrega de Práctica	
Semana 13 (5 horas)		Práctica de Configuración Cortafuegos (3h)	• Familiarización con herramientas y escenario de laboratorio (2h)		Entrega de Práctica	
Semana 14 (6 horas)	Tema 8: Servicios de Protección de Comunicaciones (3h)		• Estudio (3h)			
Semana 15 (6 horas)	Visita a un Centro de Operación de Seguridad empresarial. (3h)		• Preparación del examen parcial 2 (3h)			
Periodo de exámenes (8h)			• Preparación del examen parcial 2 (6h)		Examen parcial 2 (2h)	

Nota: Para cada actividad se especifica la dedicación en horas que implica para el alumno.