Plan 512 GRADO EN INGENIERÍA DE TECNOLOGÍAS ESPECÍFICAS DE TELECOMUNICACIÓN

Asignatura 46667 SEGURIDAD EN REDES DE COMUNICACIONES

Tipo de asignatura (básica, obligatoria u optativa)

OPTATIVA (OBLIGATORIA DE LA MENCIÓN)

Créditos ECTS

6 ECTS

Competencias que contribuye a desarrollar

2.1
Generales

· GBE1. Conocimiento, comprensión y capacidad para aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico de Telecomunicación y facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento
· GBE3. Capacidad para resolver problemas con iniciativa, creatividad y razonamiento crítico.
· GBE4. Capacidad para diseñar y llevar a cabo experimentos, así como analizar e interpretar datos.
· GBE5. Capacidad para elaborar informes basados en el análisis crítico de la bibliografía técnica y de la realidad en el campo de su especialidad.
· GE3. Capacidad para desarrollar metodologías y destrezas de aprendizaje autónomo eficiente para la adaptación y actualización de nuevos conocimientos y avances científicos.
· GE6. Capacidad, y compromiso ético en la elaboración de soluciones de ingeniería y en las diversas situaciones de gestión de recursos humanos y de gestión económica, así como capacidad para comprender el impacto de las soluciones de Ingeniería en un contexto social global.
· GC1. Capacidad de organización, planificación y gestión del tiempo.
· GC2. Capacidad para comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con las telecomunicaciones y la electrónica.

2.2
Específicas

· TEL1. 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.
· TEL2. 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.
· TEL3. Capacidad de construir, explotar y gestionar servicios telemáticos, utilizando herramientas analíticas de planificación, de dimensionado y de análisis.

Objetivos/Resultados de aprendizaje

Al finalizar la asignatura el alumno deberá ser capaz de:
GENERALESAl finalizar la asignatura el alumno deberá ser capaz de:
GENERALES
· Comprender los principales tipo de vulnerabilidades en el funcionamiento de las redes y sistemas telemáticos y conocer las principales técnicas para solucionarlas.

· Determinar los procedimientos a aplicar y las herramientas a utilizar para incrementar el nivel de seguridad de una red telemática y de la información manejada por la misma
· Conocer, interpretar y aplicar legislación, normativa y metodologías del ámbito de la seguridad telemática y de la protección de datos
· Encontrar y analizar información técnica relacionada con la seguridad telemática y realizar informes técnicos con dicha información.
Trabajar en equipo en problemas multidisciplinares relacionados con el diseño de redes seguras, así como presentar los resultados obtenidos.

Contenidos

Bloque 1:
La seguridad: amenazas y ataques. Servicios y mecanismos de seguridad. Gestión de Riesgos. Legislación.

c.
Contenidos

TEMA 1: Introducción y conceptos básicos.
1.1 Introducción
1.2 Seguridad del entorno.
1.3 Seguridad del sistema.
1.4 Seguridad de la red.
TEMA 2: Gestión de la Seguridad. Análisis y gestión de riesgos
2.1 Introducción
2.2 Análisis de riesgos y amenazas.
2.3 Políticas de Seguridad.
2.4 Seguridad y análisis de Riesgos.
TEMA 3: Legislación y normativa de seguridad
3.1 Introducción
3.2 LOPD y su reglamento
3.3 Metodologías ISO 27000
Bloque 2:
Criptografía. Tipos de cifrado. Infraestructura de clave pública.

c.
Contenidos

TEMA 4: Criptografía.
4.1 Introducción a la Criptografía.
4.2 Cifrado clásico
4.3 Técnicas de Sustitución y de Permutación...
Tema 5: Criptografía simétrica.
5.1 Introducción al cifrado en flujo. RC4,A5
5.2 Introducción al cifrado en bloque.
5.3 Algoritmos simétricos Cifrado Bloque. DES y 3DES,AES
5.4 Distribución de claves
Tema 6: Teoría de Números.
6.1 Congruencia.CCR Conjunto Completo de restos
6.2 Inversos dentro de un cuerpo n
6.3 CRR Conjunto Reducido de restos
6.4 Función de Euler
Tema 7: Criptografía Asimétrica.
7.1 Introducción Criptografía Asimétrica.
7.2 Algoritmos asimétricos. RSA.
7.3 Curvas elípticas
7.4 Diffie-Hellman.
Tema 8: Autentificación. Hash. Firmas Digitales.
8.1 Introducción
8.2 Funciones MAC
8.3 Funciones HASH. MD5, SHA
8.4 HMAC

8.5 Firma digital
Tema 9: Certificados digitales y PKI.
9.1 Introducción
9.2 Certificados digitales.
9.3 Autoridades de certificación.
9.4 PKI (Infraestructura de Clave Pública)
Bloque 3:
Arquitecturas de seguridad en redes. Dispositivos y protocolos de seguridad.

c.
Contenidos

Tema 10: Protocolos de Seguridad a nivel de transporte
10.1 Introducción
10.2 Protocolo Secure Socket Layer (SSL)
10.3 Protocolo Transport Layer Security (TLS)
Tema 11: Seguridad a nivel de red: IPSEC.
11.1 Introducción
11.2 Arquitectura IPSEC
11.3 Protocolo AH
11.4 Protocolo ESP
11.5 Protocolo IKE
Tema 12: Seguridad a nivel de aplicación.
12.1 HTTS,
12.2 SSH,
12.3 Sistema Kerberos,
12.4 Seguridad en el correo electrónico PGP, S/MIME.
Tema 13: Seguridad a nivel de Enlace: EAP, 801.1x, Seguridad WIFI
13.1 Protocolo EAP.
13.2 Arquitectura 802.1x. Servidor Radius.
13.3 Seguridad WIFI. WEP.WPA.WPA-2..RSN
Tema 14: Sistemas de Defensa Perimetral.
14.1 Tipos
14.2 Cortafuegos.
14.3 Sistemas de Detección de Intrusos.
14.4 Señuelos (Honeypots)
14.5 Redes Privadas Virtuales
Tema 15. Malware
15.1 Virus y otras amenazas.
15.2 Análisis de Malware
15.3 Auditoría de vulnerabilidades.

Principios Metodológicos/Métodos Docentes

Se empleará:
- Clase magistral participativa
- Seminario
- Aprendizaje colaborativo
- Experimentación en prácticas de laboratorio

Criterios y sistemas de evaluación

BLOQUE
INSTRUMENTO/PROCEDIMIENTO

PESO EN LA NOTA FINAL
OBSERVACIONES
EXA
Examen final escrito – parte de teoría y problemas
60%
Es condición necesaria (pero no suficiente) para superar la asignatura alcanzar una calificación igual o superior a 3 puntos sobre la calificación global de la asignatura (10 puntos).
LAB
Informes de las sesiones de laboratorio
30%

Es condición necesaria (pero no suficiente) para superar la asignatura entregar todos los informes de laboratorio y que la suma de las calificaciones del bloque (LAB) alcance 2 puntos sobre la calificación global de la asignatura (10 puntos).
Test del laboratorio.
10%
Es condición necesaria (pero no suficiente) para superar la asignatura y que la suma de las calificaciones del bloque (LAB) alcance 2 puntos sobre la calificación global de la asignatura (10 puntos).

Los alumnos que no alcancen la mínima calificación exigida en cada una de las partes (LAB y EXA) tendrán una calificación global (sobre 10 puntos) igual a la de la menor calificación de las partes de la asignatura en las que no alcanzan el mínimo exigido.

Convocatoria extraordinaria
Para superar la asignatura en la convocatoria ordinaria los alumnos deben superar:
(EXA) El examen escrito (problemas + teoría).
(LAB) La evaluación del laboratorio (informes + test).

Los alumnos que han superado (LAB) pero no (EXA):
· Salvo petición expresa en sentido contrario, indicada el día de la revisión de la convocatoria ordinaria, mantienen la nota alcanzada en (LAB) y deben realizar de nuevo (EXA).
· Si el día de la revisión de la convocatoria ordinaria lo solicitan expresamente, pueden repetir de nuevo la parte de (LAB) en las condiciones que se indican a continuación. Además deben realizar de nuevo (EXA).

Los alumnos que han superado (EXA) pero no (LAB):
· Salvo petición expresa en sentido contrario, indicada el día de la revisión de la convocatoria ordinaria, mantienen la nota alcanzada en (EXA) y deben repetir la parte de (LAB) en las condiciones que se indican a continuación.
· Si el día de la revisión de la convocatoria ordinaria lo solicitan expresamente, pueden repetir de nuevo la parte de (EXA), además de repetir obligatoriamente la parte de (LAB).

Los alumnos no han superado ni (EXA) ni (LAB):
· Deben repetir ambas partes.

Todos los alumnos que tengan que recuperar la parte de (LAB) en la convocatoria extraordinaria deben realizar el test de laboratorio. Además, la realización de nuevos informes de laboratorio será obligatoria o voluntaria según las siguientes condiciones:
· Los alumnos que no hayan presentado alguno de los informes de laboratorio en la convocatoria ordinaria deben presentarlo en la extraordinaria.
· Los alumnos que hayan suspendido algún informe (han obtenido menos de la mitad de la nota máxima en ese informe) pueden presentarlo de nuevo (sin necesidad de asistir al laboratorio), de acuerdo con el enunciado de la convocatoria ordinaria. La nueva nota sustituirá a la anterior, sea mejor o peor. La fecha límite para esta entrega es el día del examen extraordinario, justo antes de comenzarlo.
· Los alumnos que habiendo aprobado los informes en la primera convocatoria deseen mejorar su nota de esta parte deben repetir todos los informes según el procedimiento que hará público el profesor tras el cierre de actas de la convocatoria ordinaria. Las nuevas notas sustituirán a las anteriores, sean mejores o peores.

Recursos de aprendizaje y apoyo tutorial

Véase Tutorías en
http://www.uva.es/export/sites/uva/2.docencia/2.01.grados/2.01.02.ofertaformativagrados/2.01.02.01.alfabetica/Grado-en-Ingenieria-de-Tecnologias-Especificas-de-Telecomunicacion/

Calendario y horario

Calendario Académico:
http://www.uva.es/export/sites/uva/7.comunidaduniversitaria/7.06.calendarioacademico/_documentos/Calendario-17-18.pdf
https://www.tel.uva.es/bin/horarios1718/DistribucionActividaddocenteETSIT2017-18.pdf
Horarios:
https://www.tel.uva.es/bin/horarios1718/Grado_3_4_TEL.pdf
Examenes:
https://www.tel.uva.es/bin/horarios1718/34gradoTelematica2cuatrimestre.pdf
https://www.tel.uva.es/bin/horarios1617/examenes_16-17.pdf

Tabla de Dedicación del Estudiante a la Asignatura/Plan de Trabajo

ACTIVIDADES PRESENCIALES
HORAS
ACTIVIDADES NO PRESENCIALES

HORAS
Clases teórico-prácticas (T/M)
25
Estudio y trabajo autónomo individual
60
Clases prácticas de aula (A)
0
Estudio y trabajo autónomo grupal
30
Laboratorios (L)
25

Prácticas externas, clínicas o de campo
0

Seminarios (S)
10

Tutorías grupales (TG)
0

Evaluación (fuera del periodo oficial de exámenes)

Total presencial
60
Total no presencial
90

Responsable de la docencia (recomendable que se incluya información de contacto y breve CV en el que aparezcan sus lineas de investigación y alguna publicación relevante)

Francisco Javier Merino Caminero (framer@tel.uva.es)

Idioma en que se imparte

Castellano