Guía docente de la asignatura

Seguridad en Redes de Comunicación (Especialidad Telemática) (221113C)

EUR-ACE®

Fecha de aprobación: **21/06/2022**

Grado	Grado en Ingeniería de Tecnologías de Telecomunicación	**Rama**	Ingeniería y Arquitectura
Módulo	Telemática	**Materia**	Servicios y Aplicaciones Telemáticos

Curso	3º	**Semestre**	2º	**Créditos**	6	**Tipo**	Obligatoria

PRERREQUISITOS Y/O RECOMENDACIONES

Los alumnos no precisan tener materias o asignaturas aprobadas como requisito indispensable para superar esta materia. No obstante, sí se recomienda tener aprobados los contenidos y adquiridas las competencias de semestres precedentes.

BREVE DESCRIPCIÓN DE CONTENIDOS (Según memoria de verificación del Grado)

Servicios de seguridad. Protocolos de seguridad. Comunicaciones seguras. Técnicas criptográficas. Vulnerabilidades y ataques. Control de acceso a servicios. Auditorías y políticas de seguridad. Protección de contenidos.

(Security services. Security protocols. Secure Communications. Cryptographic techniques. Vulnerabilities and attacks. Service access control. Audits and security policies. Content protection)

COMPETENCIAS ASOCIADAS A MATERIA/ASIGNATURA

COMPETENCIAS ESPECÍFICAS

- CE21 - 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.
- 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.
- CE24 - Capacidad de describir, programar, validar y optimizar protocolos e interfaces de comunicación en los diferentes niveles de una arquitectura de redes.
- CE27 - Capacidad de programación de servicios y aplicaciones telemáticas, en red y distribuidas.

COMPETENCIAS TRANSVERSALES

- CT01 - Capacidad de análisis y síntesis: Encontrar, analizar, criticar (razonamiento crítico), relacionar, estructurar y sintetizar información proveniente de diversas fuentes, así como integrar ideas y conocimientos.
- CT02 - Capacidad de organización y planificación así como capacidad de gestión de la Información.
- CT03 - Capacidad de comunicación oral y escrita en el ámbito académico y profesional con especial énfasis, en la redacción de documentación técnica.
- CT04 - Capacidad para la resolución de problemas.
- CT05 - Capacidad para tomar decisiones basadas en criterios objetivos (datos experimentales, científicos o de simulación disponibles) así como capacidad de argumentar y justificar lógicamente dichas decisiones, sabiendo aceptar otros puntos de vista.
- CT06 - Capacidad para el uso y aplicación de las TIC en el ámbito académico y profesional.
- CT07 - Capacidad de comunicación en lengua extranjera, particularmente en inglés.
- CT08 - Capacidad de trabajo en equipo.
- CT09 - Capacidad para el aprendizaje autónomo así como iniciativa y espíritu emprendedor.
- CT10 - Motivación por la calidad y la mejora continua, actuando con rigor, responsabilidad y ética profesional.
- CT11 - Capacidad para adaptarse a las tecnologías y a los futuros entornos actualizando las competencias profesionales.
- CT12 - Capacidad para innovar y generar nuevas ideas.
- CT13 - Sensibilidad hacia temas medioambientales.
- CT14 - Respeto a los derechos fundamentales y de igualdad entre hombres y mujeres.
- CT15 - Capacidad para proyectar los conocimientos, habilidades y destrezas adquiridos para promover una sociedad basada en los valores de la libertad, la justicia, la igualdad y el pluralismo.

RESULTADOS DE APRENDIZAJE (Objetivos)

- Conocer y comprender los aspectos involucrados en la seguridad de entornos de red, tomando conciencia de las limitaciones y riesgos que implica la interconexión de equipos y usuarios.
- Comprender el impacto y relevancia de los incidentes de seguridad en las tecnologías de la información y las comunicaciones.
- Conocer las vulnerabilidades, los componentes y los mecanismos de seguridad en los sistemas de comunicación y las redes.
- Conocer la metodología y los tipos de ataques a la seguridad de los sistemas y servicios.
- Capacidad de diseño y administración de la seguridad de un entorno de comunicaciones, establecida ésta en niveles de profundidad.

- Comprender y usar herramientas hardware y software específicas para el control y administración de la seguridad de los sistemas.
- Conocer y usar las principales tecnologías de seguridad relacionadas con la confidencialidad, autenticación, no repudio, disponibilidad y control de accesos.
- Conocer los fundamentos de los protocolos involucrados en las comunicaciones seguras.
- Conocer y aplicar los nuevos esquemas y sistemas involucrados en firma digital y servicios electrónicos.
- Desplegar y hacer uso de políticas de seguridad, definiendo los principios básicos que las sustentan.
- Conocer y seguir actuaciones e iniciativas relacionadas con la seguridad electrónica, tanto nacionales como internacionales.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

Bloque I. Fundamentos de seguridad (6 horas)

- Tema 1. Introducción (2h):
  - 1.1. Conceptos básicos.
  - 1.2. Vulnerabilidades.
  - 1.3. Modelos de seguridad.
  - 1.4. Estándares.
- Tema 2. Criptografía (4h):
  - 2.1. Fundamentos.
  - 2.2. Cifrado simétrico y asimétrico.
  - 2.3. Autenticación de mensajes.
  - 2.4. Firma digital.
  - 2.5. Distribución de claves.

Bloque II. Protocolos para comunicaciones seguras (14 horas)

- Tema 3. Seguridad de redes en capas (9h):
  - 3.1. Seguridad inalámbrica.
  - 3.2. IPsec.
  - 3.3. SSL/TLS.
  - 3.4. HTTPS.
  - 3.5. SSH.
  - 3.6. Correo seguro.
  - 3.7. DNS seguro.
- Tema 4. Control de accesos (5h):
  - 4.1. Acceso remoto.
  - 4.2. Cortafuegos.
  - 4.3. VPN.

Bloque III. Seguridad de sistemas en red (10 horas)

- Tema 5. Software malicioso (6h):
  - 5.1. Virus.
  - 5.2. Gusanos.
  - 5.3. Troyanos.
  - 5.4. Ataques DoS.

- 5.5. Intrusiones.
- Tema 6. Aspectos legales y éticos (4h):
  - 6.1. Propiedad intelectual.
  - 6.2. Protección de contenidos.
  - 6.3. Políticas.
  - 6.4. Cibercrimen.

Tutorías (5 horas):

Adicionalmente, se prevén impartir un total de 1 sesión de tutoría individual, de 1 hora de duración, y 2 sesiones de tutorías colectivas, de 2 horas de duración cada una de ellas. De estas últimas, la primera será al inicio del cuatrimestre y la segunda al final de este, antes del inicio de los exámenes. Por su parte, las tutorías individuales serán a libre elección del alumno a lo largo del semestre.

PRÁCTICO

Prácticas laboratorio (15 horas):

- Práctica 1. Análisis de seguridad de redes (2h).
- Práctica 2. Despliegue de PKI y servicios SSL/TLS con openSSL (4h).
- Práctica 3. Aplicaciones de correo electrónico y web seguras (2h).
- Práctica 4. Cortafuegos (3h).
- Práctica 5. Tunneling y redes privadas virtuales (2h).
- Práctica 6. Sistemas IDS (2h).

Seminarios (10 horas):

- Seminario 1. Herramientas de monitorización y análisis (2h).
- Seminario 2. Infraestructura de clave pública (PKI) y servicios de seguridad en capas (2h).
- Seminario 3. Servicios de usuario seguros (2h).
- Seminario 4. Seguridad perimetral y VPN (2h).
- Seminario 5. Acciones maliciosas (2h).

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- Pedro García Teodoro, Gabriel Maciá Fernández:"Seguridad en Redes y Sistemas de Comunicación. Teoría y Práctica". Kindle Direct Publishing, 2020.
- William Stallings: "Network Security Essentials: Applications and Standards". Prentice Hall, 4ª Ed., 2011.
- Robin P. Bryant (Editor): "Investigating Digital Crime". John Wiley & Sons, 1ª Ed., 2008.

BIBLIOGRAFÍA COMPLEMENTARIA

- Raymon Panko: "Corporate Computer and Network Security". Prentice Hall, 2ª Ed., 2010.
- Houston Carr, Charles Snyder, Bliss Bailey: "Management of Network Security". Prentice Hall, 1ª Ed., 2010.
- Randy Boyle: "Applied Information Security". Prentice Hall, 1ª Ed., 2010.

- Michael Goodrich, Roberto Tamassia: "Introduction to Computer Security". Addison-Wesley, 1ª Ed., 2011.

ENLACES RECOMENDADOS

- Plataforma Prado de la UGR.
- Web de la asignatura.

METODOLOGÍA DOCENTE

- MD01 - Lección magistral
- MD02 - Actividades prácticas
- MD03 - Seminarios
- MD04 - Actividades no presenciales
- MD05 - Tutorías académicas

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

Con objeto de evaluar la adquisición de los contenidos y competencias a desarrollar en la materia, se utilizará un sistema de evaluación diversificado, seleccionando las técnicas de evaluación más adecuadas en cada momento. Se utilizará alguna o algunas de entre las siguientes:

- Para la parte teórica se realizará examen escrito final, además de entregas de trabajos, ejercicios y sesiones de evaluación sobre el desarrollo y los resultados de las actividades propuestas. La ponderación de este bloque será del 60%.
- Para la parte práctica se realizarán sesiones de laboratorio, sobre las que, además de considerar la asistencia de los estudiantes, se realizarán ejercicios de control y seguimiento del aprovechamiento para evaluar los conocimientos adquiridos. El peso asociado a la calificación de esta parte será el 30%.
- La parte de seminarios se evaluará teniendo en cuenta la asistencia a éstos, los problemas/ejercicios propuestos que hayan sido resueltos y entregados por los alumnos y la presentación oral de los trabajos desarrollados. La ponderación de esta parte será del 10%, teniéndose en cuenta para ello la capacidad demostrada por el alumno en la búsqueda de fuentes bibliográficas y el autoaprendizaje.

La calificación global de la asignatura corresponderá a la suma de las calificaciones correspondientes a la parte teórica, la parte práctica y la correspondiente a los seminarios, de manera que la superación oficial de la materia precisará la concurrencia de dos hechos:

1. La calificación de la parte teórica deberá ser igual o superior al 40% del máximo de esta parte, esto es, >=2,4 puntos sobre 6.
2. La calificación global deberá ser igual o superior a 5 puntos sobre 10.

Para los estudiantes que se acojan a la evaluación única final, no se guardarán posibles calificaciones parciales de clase y deberá realizarse examen escrito de cada una de las partes en

que se organiza la asignatura: teoría, seminarios y prácticas.

Todo lo relativo a la evaluación se regirá por la Normativa de evaluación y calificación de los estudiantes vigente en la Universidad de Granada

Régimen de asistencia:

La asistencia a las clases teóricas o prácticas no es obligatoria, requiriéndose en cambio la asistencia a al menos el 50% de las sesiones programadas de seminarios y prácticas. En caso de incumplimiento se calificará con 0 puntos la parte correspondiente.

EVALUACIÓN EXTRAORDINARIA

Examen escrito de cada una de las partes componentes de la materia, Teoría, Seminarios y Prácticas, con los pesos asociados correspondientes (60%, 30% y 10%, respectivamente).

EVALUACIÓN ÚNICA FINAL

Examen escrito de cada una de las partes componentes de la materia, Teoría, Seminarios y Prácticas, con los pesos asociados correspondientes (60%, 30% y 10%, respectivamente).

INFORMACIÓN ADICIONAL

Disposición de recursos:

- A través de PRADO se dispondrán enlaces y recursos para la realización de prácticas de laboratorio.
- Asimismo, en la web del Dpto para la asignatura se aclarará cualquier cambio a realizar en la evaluación.
- También en dichas webs se dispondrán recursos y documentación adicional para la adaptación de la evaluación del curso.