Guía docente

Identificación de la asignatura

Asignatura / Grupo	22370 - Seguridad en Redes Telemáticas / 4
Titulación	Doble titulación: Grado en Matemáticas y Grado en Ingeniería Telemática - Quinto curso Grado en Ingeniería Telemática - Tercer curso
Créditos	6
Período de impartición	Segundo semestre
Idioma de impartición	Castellano

Profesores

Profesor/a	Horario de atención a los alumnos					
	Hora de inicio	Hora de fin	Día	Fecha inicial	Fecha final	Despacho / Edificio
María Francisca Hinarejos Campos *Responsable* xisca.hinarejos@uib.es	15:00	17:00	Viernes	02/09/2019	24/01/2020	D-136
	10:00	12:00	Lunes	02/09/2019	24/01/2020	D-136
José Luis Ferrer Gomila jlferrer@uib.es	11:30	13:30	Jueves	02/09/2019	31/07/2020	D-117
	11:30	13:30	Lunes	02/09/2019	31/07/2020	D-117

Contextualización

Seguridad en Redes Telemáticas es una asignatura que forma parte del módulo obligatorio del plan de estudios del Grado en Ingeniería Telemática (tercer curso) y de la doble titulación (quinto curso): Grado de Matemáticas y Grado en Ingeniería Telemática.

En esta asignatura se explican los principios de la criptografía para poder proporcionar los servicios de seguridad necesarios a las redes de comunicación. La firma digital y los certificados de clave pública, el control de acceso, los ataques y las contramedidas son elementos de esta asignatura. Además se estudiará cómo se implantan las medidas de seguridad en las distintas capas de la pila de protocolos TCP/IP. Por este motivo, es necesario que se tengan los conocimientos sobre redes de comunicación de datos (proporcionados en otras asignaturas del grado; ver apartado de requisitos).

Para tener una visión gráfica de la relación de esta asignatura con las del resto de asignaturas del grado, puede visitarse la siguiente URL: http://eps.uib.es/mapa/

La primera parte de la asignatura (Bloque 1) se imparte en catalán, y la segunda parte (Bloque 2) en castellano.

Requisitos

Fecha de publicación: 19/07/2019

Para que el alumno pueda realizar un buen aprovechamiento de la asignatura, es recomendable haber cursado (o estar cursando) tres tipos de asignaturas:

1 Asignaturas de redes: necesarias para entender el motivo por el que se aplica un determinado tipo de medida de seguridad.
2 Asignaturas de programación: necesarias para realizar prácticas de laboratorio.
3 Asignaturas de matemáticas: muchos de los algoritmos criptográficos se basan en operaciones matemáticas.

Recomendables

Para ver con detalle las asignaturas recomendables, ir a la siguiente URL: **http://eps.uib.es/mapa/**

Competencias

Específicas

* (CT2) Capacidad para aplicar las técnicas en las que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento, 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

Genéricas

* (CG3) Creatividad, innovación, y visión de futuro: capacidad para crear e innovar productos y servicios
* (CG4) Habilidad de adaptación a la rápida evolución de las tecnologías y los mercados de las TIC
* (CG5) Escrita: habilidad en la redacción de proyectos y documentación técnica

Básicas

* Se pueden consultar las competencias básicas que el estudiante tiene que haber adquirido al finalizar el grado en la siguiente dirección: http://estudis.uib.cat/es/grau/comp_basiques/

Contenidos

Contenidos temáticos

Bloque 0. Introducción

Bloque 1. Conceptos generales de criptografía

- Tema 1. Criptografía de clave secreta
- Tema 2. Criptografía de clave pública
- Tema 3. Integridad y autenticación
- Tema 4. Firma digital y certificación de clave pública

Bloque 2. Protocolos de seguridad

- Tema 1. Seguridad en la capa de transporte
- Tema 2. Correo electrónico certificado

Fecha de publicación: 19/07/2019

Tema 3. Seguridad a nivel IP

Metodología docente

Actividades de trabajo presencial (2,4 créditos, 60 horas)

Modalidad	Nombre	Tip. agr.	Descripción	Horas
Clases teóricas	Clases magistrales	Grupo grande (G)	Utilizando este método expositivo, se introducirán los conceptos básicos en los que se fundamenta la seguridad en redes. Se trabajarán las competencias CG4, CT2	40
Clases prácticas	Trabajo de análisis o desarrollo	Grupo mediano 2 (X)	Durante la segunda parte del curso, se llevará a cabo un proyecto (de análisis o desarrollo) en el que se utilizarán algunos de los mecanismos de seguridad vistos en la primera parte del curso. De esta manera, se reforzarán los conocimientos explicados en las clases magistrales y adquiridos en las prácticas de laboratorio. Este proyecto de análisis o de desarrollo se llevará a cabo en grupo. Se trabajarán las competencias CG3, CG4,CG5, CT2	10
Clases de laboratorio	Prácticas de laboratorio	Grupo mediano (M)	Las prácticas de laboratorio sirven tanto para poner en práctica algunos de los conocimientos teóricos explicados en las clases magistrales como para adquirir nuevos conocimientos. Estas prácticas se realizarán en grupos pequeños de alumnos. Se trabajarán y evaluarán las competencias CG3, CG4,CG5	8
Evaluación	Controles parciales	Grupo grande (G)	La materia de la asignatura se dividirá en dos partes, y a lo largo del semestre el alumno realizará dos controles parciales (uno durante el periodo lectivo y un segundo control el día de la convocatoria oficial de junio). Esta evaluación permite validar los resultados obtenidos a través del resto de métodos de evaluación. Se volverán a realizar dos controles en el periodo de recuperación. Se evaluarán las competencias CT2 y CG3	2

Al inicio del semestre estará a disposición de los estudiantes el cronograma de la asignatura a través de la plataforma UIBdigital. Este cronograma incluirá al menos las fechas en las que se realizarán las pruebas de evaluación continua y las fechas de entrega de los trabajos. Asimismo, el profesor o la profesora informará a los estudiantes si el plan de trabajo de la asignatura se realizará a través del cronograma o mediante otra vía, incluida la plataforma Aula Digital.

Actividades de trabajo no presencial (3,6 créditos, 90 horas)

Fecha de publicación: 19/07/2019

Modalidad	Nombre	Descripción	Horas
Estudio y trabajo autónomo individual	Trabajo autónomo	El estudio individual (o en grupo) le servirá al alumno tanto para obtener o consolidar los contenidos teóricos de la asignatura, como para preparar o finalizar las sesiones de prácticas de laboratorio, y realizar el análisis del proyecto a desarrollar. Se profundizará en las competencias CG3, CG4, CG5, CG13, CG14, CT2	90

Riesgos específicos y medidas de protección

Las actividades de aprendizaje de esta asignatura no conllevan riesgos específicos para la seguridad y salud de los alumnos y, por tanto, no es necesario adoptar medidas de protección especiales.

Evaluación del aprendizaje del estudiante

La evaluación de la asignatura se basa principalmente en dos controles parciales (45% el primer control y 30% el segundo control), pero también se deberá realizar un proyecto del que se tendrá que entregar un informe y llevar a cabo la defensa del mismo. Hay que tener en cuenta que la realización tanto del proyecto como de las prácticas de laboratorio ayudan al alumno a asimilar y ampliar los conceptos teóricos estudiados en clase.

Los controles parciales consistirán en preguntas de teoría a ser desarrolladas, preguntas tipo test, de desarrollo y/o problemas numéricos. Aunque los controles liberen materia, los conocimientos, habilidades o destrezas adquiridos son acumulativos.

El alumno obtendrá una calificación numérica entre 0 y 10 en cada una de las actividades evaluativas, la cual será ponderada según su peso a fin de obtener la calificación final de la asignatura. Para poder superar la asignatura el alumno ha de obtener un mínimo de 5 puntos sobre 10 mediante la suma ponderada de todas las actividades realizadas.

El método de evaluación planteado no requiere de un itinerario específico para los estudiantes a tiempo parcial (el itinerario A es válido para todos los estudiantes).

Convocatoria Anticipada

En esta asignatura no se permite la convocatoria anticipada.

Fraude en elementos de evaluación

De acuerdo con el artículo 33 del Reglamento Académico, "con independencia del procedimiento disciplinario que se pueda seguir contra el estudiante infractor, la realización demostrablemente fraudulenta de alguno de los elementos de evaluación incluidos en guías docentes de las asignaturas comportará, a criterio del profesor, una minusvaloración en su calificación que puede suponer la calificación de «suspenso 0» en la evaluación anual de la asignatura".

Fecha de publicación: 19/07/2019

Trabajo de análisis o desarrollo

Modalidad	Clases prácticas
Técnica	Trabajos y proyectos **(no recuperable)**
Descripción	Durante la segunda parte del curso, se llevará a cabo un proyecto (de análisis o desarrollo) en el que se utilizarán algunos de los mecanismos de seguridad vistos en la primera parte del curso. De esta manera, se reforzarán los conocimientos explicados en las clases magistrales y adquiridos en las prácticas de laboratorio. Este proyecto de análisis o de desarrollo se llevará a cabo en grupo. Se trabajarán las competencias CG3, CG4,CG5, CT2
Criterios de evaluación	Se valorará tanto la solución desarrollada, como el informe y defensa del proyecto realizado. No es necesario la obtención de una nota mínima.

Porcentaje de la calificación final: 25%

Controles parciales

Modalidad	Evaluación
Técnica	Pruebas de respuesta larga, de desarrollo **(recuperable)**
Descripción	La materia de la asignatura se dividirá en dos partes, y a lo largo del semestre el alumno realizará dos controles parciales (uno durante el periodo lectivo y un segundo control el día de la convocatoria oficial de junio). Esta evaluación permite validar los resultados obtenidos a través del resto de métodos de evaluación. Se volverán a realizar dos controles en el periodo de recuperación. Se evaluarán las competencias CT2 y CG3
Criterios de evaluación	Para que los controles puedan hacer media en la obtención de la nota final de la asignatura, se deberá obtener una nota igual o superior a 5 en cada uno de ellos, de manera independiente.

Porcentaje de la calificación final: 75% con calificación mínima 5

Recursos, bibliografía y documentación complementaria

Bibliografía básica

"Cryptography and Network Security: Principles and Practice". W. Stallings. Ed. Prentice Hall
“Applied Cryptography”. B. Schneier. Ed. John Willey & Sons

Bibliografía complementaria

A través de la página web de la asignatura en Aula Digital, se podrán obtener otros recursos, como notas de clase, enlaces a páginas web con información complementaria, material para las prácticas de laboratorio, bibliografía complementaria, etc.

Fecha de publicación: 19/07/2019