



DATOS IDENTIFICATIVOS

Seguridad

Asignatura	Seguridad			
Código	V05G300V01543			
Titulación	Grado en Ingeniería de Tecnologías de Telecomunicación			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OP	3	1c
Lengua	Castellano			
Impartición				
Departamento	Ingeniería telemática			
Coordinador/a	Fernández Masaguer, Francisco			
Profesorado	Fernández Masaguer, Francisco			
Correo-e	francisco.fernandez@det.uvigo.es			
Web	http://faitic.uvigo.es			

Descripción general En esta asignatura se estudian, de una manera unificada, los principales problemas o amenazas de seguridad en las redes y servicios telemáticos, y se presentan distintas técnicas para protegerlos.

Primero se aborda el tema desde un punto de vista general, de forma que los conceptos, servicios y técnicas de seguridad que se estudian, sean aplicables a cualquier tipo de red, servicio telemático o sistema de información a securizar. Este bloque lo forman los temas 1 al 4. Esto lleva a tratar con detalle los tres temas centrales de la seguridad: la parte algorítmica (cifrado, firma digital e integridad), los protocolos de autenticación, y los procedimientos de gestión y negociación de claves. El objetivo es que el alumno adquiera una sólida base que le capacite para facilitar su comprensión de las técnicas particulares que cada aplicación requiera así como para aplicarlo a otros ámbitos que tenga que afrontar.

Luego se trata el tema de una forma algo más particular, revisando los problemas, técnicas y estándares de seguridad en algunos de los entornos de comunicación de más prevalencia en la actualidad. Así se dedica un tema a la seguridad a nivel IP, protocolo central en la arquitectura Internet, y otro tema a la seguridad en la Web, dada la vigencia actual de este medio de intercomunicación telemática, donde el alumno asimilará los conceptos teóricos y prácticos del protocolo SSL, central para la seguridad de las transacciones a través de la Web. Dada la utilización cada vez mayor de las comunicaciones por medio inalámbrico y sus particulares problemas de seguridad, se dedica también un tema a ellos. Se cierra el curso con una introducción a otros dos temas de trascendencia creciente: las redes y software malicioso y el análisis forense de sistemas de información.

Competencias

Código	
B3	CG3 Conocimiento de materias básicas y tecnologías que capaciten al alumnado para el aprendizaje de nuevos métodos y tecnologías, así como que le dote de una gran versatilidad para adaptarse a nuevas situaciones.
B4	CG4 Capacidad para resolver problemas con iniciativa, para la toma de decisiones, la creatividad, y para comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico de Telecomunicación.
B6	CG6 Facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
C28	CE28/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.
D2	CT2 Concebir la Ingeniería en un marco de desarrollo sostenible.
D3	CT3 Tomar conciencia de la necesidad de una formación y mejora continua de calidad, mostrando una actitud flexible, abierta y ética ante opiniones o situaciones diversas, en particular en materia de no discriminación por sexo, raza o religión, respeto a los derechos fundamentales, accesibilidad, etc.

Resultados de aprendizaje

Resultados previstos en la materia	Resultados de Formación y Aprendizaje		
Comprender los fundamentos de la ciencia criptográfica.	B3		
Adquirir los conocimientos necesarios para asegurar la seguridad de un sistema informático o telemático.	B3		
Adquirir habilidades sobre el proceso de análisis de los ataques que puede sufrir una red y los principales mecanismos de defensa contra ellos.	B4	C28	D3
Conocer las principales arquitecturas de seguridad aplicables a los sistemas informáticos y telemáticos.	B4	C28	D3
Conocer las principales ideas de las normas y estándares más importantes en materia de seguridad en sistemas informáticos y en redes de comunicación.	B6	C28	D2

Contenidos

Tema	
1 Fundamentos matemáticos de la seguridad.	<ul style="list-style-type: none">- Nociones de Teoría de la Complejidad- Nociones básicas de Teoría de Números.
2. Algoritmos de cifrado, firma digital y hash	<ul style="list-style-type: none">- Tipos de criptosistemas y algoritmos.- Integridad y Algoritmos de Hash.- Criptosistemas de clave simétrica. Algoritmos de Mac. Cifrado simétrico. Principios de cifrado de Shannon. Cifrado en flujo y cifrado en bloque. Algoritmos DES y AES. Modos de trabajo de los cifradores en bloque.- Criptosistemas de clave pública. RSA y DSA.
3. Certificación y PKIs.	<ul style="list-style-type: none">- Problemática de seguridad en la criptografía asimétrica. Certificación y formatos de certificados.- Modelos de confianza. Confianza plana y modelo PGP. Confianza en terceros y autoridades de certificación.- Infraestructuras de certificación. Ruta de certificación. Revocación de certificados.
4. Protocolos de autenticación y convenio de clave.	<ul style="list-style-type: none">- Métodos de autenticación.- Amenazas a un protocolo de autenticación. Contramedidas.- Requisitos de un protocolo de convenio de clave. Protocolo D-H.- Autenticación en criptosistemas simétricos. Casos de estudio: Autenticación en GSM, Protocolo Kerberos.- Autenticación en criptosistemas asimétricos. Casos de estudio: autenticación X509 y SSL.- Protocolos basados en contraseñas: SRP.
5. Seguridad en el nivel de Red	<ul style="list-style-type: none">- Análisis de amenazas en el nivel de red.- Arquitectura de seguridad en IP.- Protocolo IPsec. Túneles IPsec. IPsec y NAT.- Protocolos para gestión de claves: IKE, ISAKMP y OAKLEY.
6. Seguridad en la Web	<ul style="list-style-type: none">- Problemas de seguridad en la Web.- Protocolos SSL y TLS.- Certificación en la Web.
7. Seguridad en entornos inalámbricos y protocolos AAA.	<ul style="list-style-type: none">- Amenazas a la seguridad en entornos inalámbricos.- Wireless Application Protocol (WAP).- WTLS. Protocolos WEP, WPA, WPA2 (802.11i).- Protocolos AAA: RADIUS.
8. Seguridad de Sistemas.	<ul style="list-style-type: none">- Cortafuegos y sistemas contra intrusiones.- Software y redes maliciosas. Botnets.- Análisis Forense de Sistemas.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Sesión magistral	21	38	59
Resolución de problemas y/o ejercicios de forma autónoma	0	10	10
Trabajos tutelados	6	28	34
Prácticas de laboratorio	11	22	33
Pruebas prácticas, de ejecución de tareas reales y/o simuladas.	1	0	1
Trabajos y proyectos	1	0	1
Pruebas de respuesta larga, de desarrollo	1	5	6
Pruebas de respuesta larga, de desarrollo	1	5	6

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías	
	Descripción
Sesión magistral	Exposición mediante presentación en powerpoint y pizarra de los contenidos teóricos de la asignatura. Se desarrollarán los temas teóricos de la materia que no queden cubiertos por las otras metodologías empleadas. En aquellos temas que se considere imprescindible, se plantearán y resolverán algunos ejercicios que sirvan de ayuda para la realización de otros similares por el alumno de forma autónoma. Con esta metodología el alumno adquirirá parte de las competencias CG3 y CE28.
Resolución de problemas y/o ejercicios de forma autónoma	El grupo resolverá de forma autónoma los ejercicios del boletín no realizados en las horas presenciales. Las diversas soluciones que surjan al abordar cada problema, serán puestas en común para consensuar la mejor forma de resolución. Las dudas surgidas se consensuarán y podrán exponerse al tutor en las horas normales de tutoría. Esta metodología esta orientada a las competencias CG4 y CE28.
Trabajos tutelados	Se presentarán varios trabajos prácticos a desarrollar, entre los cuales cada grupo deberá elegir uno. En las clase tipo C, se expondrá a cada grupo los objetivos del trabajo, herramientas hardware y software a usar, forma de acometerlo y se realizará un seguimiento a cada grupo. Esta metodología esta orientada a la adquisición de las competencias CG4, CG6 y CE28, CT2 y CT3.
Prácticas de laboratorio	El alumno desarrollará una práctica en el laboratorio, enfocada tanto a madurar y llevar a la practica los conceptos teóricos, como a mejorar su capacidad para el desarrollo y/o implantación de redes y servicios seguros. Esta metodología esta orientada a las competencias CG6, CE28, CT2 y CT3.

Atención personalizada

Metodologías	Descripción
Prácticas de laboratorio	Seguimiento individualizado del trabajo de cada grupo. Comentarios de forma conjunta con diversas recomendaciones y estrategias para la buena realización del proyecto. Se revisa con cada grupo el nivel de comprensión y avance del proyecto, dudas particulares que puedan surgir, errores de diseño y codificación Java. Ayuda para la comprensión de los paquetes JCA/JCE y JSSE. Ayuda individualizada para la instalación de la herramienta de gestión de almacenes de claves y del código Java básico de la práctica.
Trabajos tutelados	Seguimiento individualizado del trabajo de cada alumno y de cada grupo. Comentarios de forma conjunta de diversas recomendaciones y estrategias para la buena realización del proyecto. Se revisa con cada grupo el nivel de comprensión y avance del proyecto, dudas particulares que puedan surgir, errores de diseño o planteamiento y opciones de mejora.
Resolución de problemas y/o ejercicios de forma autónoma	Revisión y comentarios de los diversos ejercicios propuestos. El alumno podrá disponer en Fatic de la solución a varios de los ejercicios que se propongan.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje		
Pruebas prácticas, de ejecución de tareas reales y/o simuladas.	Prueba de grupo en la que el profesor valorará la practica de laboratorio, revisando su funcionamiento con los integrantes del grupo presentes. Esta prueba se realizara en la semana del 9 al 13 de Enero. Todos los integrantes del grupo deben estar presentes en el momento de la presentación. Se realizara una entrevista de autoria de la que se determinara el nivel de participacion de cada alumno y de la que, junto con el correcto funcionamiento, se deducira la nota individual.	25	B6	C28	D3
Trabajos y proyectos	Prueba de grupo. Valoración del proyecto o trabajo tutelado realizado por el grupo (tipo C). El grupo hara una demostración al profesor del proyecto o trabajo realizado y resultados obtenidos. Esta prueba se realizara en la semana del 9 al 13 de Enero. Todos los integrantes del grupo deben estar presentes en el momento de la presentación. Se realizara una entrevista de autoria de la que se determinara el nivel de participacion de cada alumno en el proyecto y de la que, junto con el correcto funcionamiento, se deducira la nota individual.	25	B4 B6	C28	D2 D3
Pruebas de respuesta larga, de desarrollo	Examen final de la asignatura. Este examen constara de un conjunto de ejercicios/cuestiones sobre los contenidos dados en el curso.	25	B3 B4	C28	
Pruebas de respuesta larga, de desarrollo	Examen parcial de la asignatura, obligatorio para los alumnos que vayan por EC. Este examen constara de un conjunto de ejercicios/cuestiones sobre los contenidos dados hasta (inclusive) la semana 6 del curso teorico.	25	B3 B4	C28	

- ELECCION DE EVALUACION CONTINUA.

Por defecto se considerará que el alumno va por evaluación continua. Si un alumno desea ir por no continua deberá comunicarlo al profesor antes de la semana 4 del curso académico. La comunicación sera por correo electrónico.

- PRIMERA CONVOCATORIA.

Evaluación continua. La evaluación continua estará formada por:

1. Trabajo B de laboratorio, representando un 25% de la nota. Este trabajo debera ser entregado via Faitic antes del día 8 de Enero.
2. Proyecto C, representando un 25% de la nota. Este proyecto deberá ser entregado via Faitic antes del día 8 de Enero.
3. Examen parcial de los contenidos dados hasta la 6 semana inclusive, representando el 25% de la nota. Este examen promediara con el examen final si el alumno saca un minimo de 1/3 del total de la nota. Si el alumno saca una nota inferior a esta, deberá volver a evaluarse de esta parte en el examen final. Este examen se realizará en la semana 7 del curso académico.
4. Examen final, en la fecha acordada en Junta de Escuela. Habrá dos casos:
 - Alumnos que hayan superado la nota mínima del examen parcial. En este examen entrarán los temas dados desde la semana 7 hasta el final. Representará un 25% de la nota total. Para poder superar la asignatura el alumno deberá obtener en este examen una nota mínima de 3,33 puntos sobre 10.
 - Alumnos que no hayan superada la nota mínima del examen parcial. En este examen entrarán todos los temas dados en el curso teórico. Representará un 50% de la nota total. Para poder superar la asignatura el alumno debera obtener en este examen una nota mínima de 3,33 puntos sobre 10.

Evaluación no continua. Los alumnos que no elijan EC realizarán un examen teórico final por el 80% de la nota, junto con las prácticas de laboratorio que completara el otro 20%. Sera necesario sacar un mínimo de 1/3 del examen teórico para poder superar la asignatura.

El examen final será el mismo para todos los alumnos, tantos para los que opten por evaluación continua como para los que no.

- CONVOCATORIA DE JULIO

Para los alumnos que hayan optado en la primera convocatoria por evaluación no continua, se realizará un examen final con un valor del 80%, junto con el laboratorio que representara el 20%. Se guarda la nota del laboratorio de la primera convocatoria.

Los alumnos que hayan optado durante el cuatrimestre por EC, podrán seguir optando en Julio por EC o bien cambiar a solo evaluación final. Los alumnos que así lo hagan deberán comunicarlo explícitamente al profesor por correo electrónico:

- En el primer caso, es decir de que sigan por EC en Julio, se guarda, de la primera convocatoria, las notas del examen parcial y final (siempre que hayan superado la nota minima) de la práctica de laboratorio y del proyecto tutelado. Deberán presentarse al examen final de la convocatoria todos los alumnos que no hayan superado la nota mínima teórica de la primera convocatoria.
- En el segundo caso, es decir de que se cambie de EC a ET en Julio, realizarán un examen final por el 80% de la nota y las prácticas de laboratorio por el 20%. Se conservará la nota del laboratorio de la

primera convocatoria, adecuadamente porcentuada.

- OTRAS OBSERVACIONES.

- *Nota mínima en teoría.* Se opte o no por EC e independientemente de la convocatoria, será obligatorio sacar un mínimo de 1/3 de la nota máxima (3,33 puntos sobre 10 para EC y 3,75 sobre 10 para ET) en el examen teórico, para poder aprobar la asignatura.
- Se considerará a un alumno como "no presentado" si no ha seguido la evaluación continua y no se ha presentado al examen final. Igualmente, si un alumno va por EC y no se presenta a ningún examen (A,B o C) se le considerará como "no presentado".
- Las calificaciones obtenidas en las prácticas B de laboratorio y proyecto C solamente serán válidas durante el curso académico en que se realicen.
- Si la nota total es igual o superior a 5 pero no se ha alcanzado la nota mínima en alguna parte, la nota final será 4.5 puntos (suspenseo).

Fuentes de información

Bibliografía Básica

F. Fernandez Masaguer, **Seguridad en Redes y Sistemas de Informacion**, 1ª ed., 2016

William Stallings, **Cryptography and Network Security. Principles and practice.**, 6ª ed., Pearson, 2014

Bibliografía Complementaria

R.Perlman, C. Kaufman, M.Speciner, **Network Security: Private communications on a public world**, 2ª ed., Prentice Hall, 2002

Joseph Migga Kizza, **Guide to Computer Network Security**, 2ª ed.,

Douglas R. Stinson, **Cryptography. Theory and Practice.**, 3ª ed.,

M. Laurent Maknavicius, **Wireless and Mobile Network Security**, 1ª, Wiley, 2009

Enisa, **Botnets: Detection; Measurement, Disinfection & Defence**, Enisa, 2011

Recomendaciones

Asignaturas que se recomienda cursar simultáneamente

Arquitecturas y servicios telemáticos/V05G300V01645

Servicios de internet/V05G300V01501

Asignaturas que se recomienda haber cursado previamente

Matemáticas: Álgebra lineal/V05G300V01104

Redes de ordenadores/V05G300V01403