



## DATOS IDENTIFICATIVOS

### Seguridad

Asignatura	Seguridad			
Código	V05G300V01543			
Titulación	Grado en Ingeniería de Tecnologías de Telecomunicación			
Descriptor	Creditos ECTS	Selección	Curso	Cuatrimestre
	6	OB	3	1c
Lengua	Castellano			
Impartición				
Departamento	Ingeniería telemática			
Coordinador/a	Fernández Masaguer, Francisco			
Profesorado	Fernández Masaguer, Francisco			
Correo-e	f_masaguer@yahoo.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. Se presentan los principales problemas de seguridad en el comercio electrónico a través de la Web y se estudia el funcionamiento del Paypal, uno de los métodos de pago más utilizados en 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 de titulación

Código	
A3	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.
A4	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.
A6	CG6 Facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
A37	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.

## Competencias de materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
------------------------------------	---------------------------------------

Conocimiento de algunas de las teorías matemáticas en las que se sustenta la seguridad de los algoritmos y protocolos criptográficos usados para la protección de redes y servicios.	A3
Conocimiento de los principios y funcionamiento de los principales algoritmos de cifrado, firma digital y hash usados como soporte de los servicios de seguridad incorporados en las redes y servicios telemáticos, sistemas de telecomunicación y sistemas de información.	A3
Conocimiento de los diferentes métodos, técnicas y protocolos de autenticación, persona-persona, persona-máquina, máquina-máquina.	A3
Dotar al alumno de la capacidad de analizar los problemas de seguridad de un sistema de información, red o servicio telemático, evaluar los riesgos asociados y de implantar las técnicas apropiadas para garantizar un nivel adecuado de seguridad.	A4
Capacidad para aplicar las técnicas de seguridad en que se basan las redes, servicios y aplicaciones telemáticas, tales como protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos.	A37
Facilitar el manejo y conocimiento de especificaciones y normativas de seguridad	A6 A37

## Contenidos

Tema	
1 Fundamentos matemáticos de la seguridad.	- Nociones de Teoría de la Complejidad - Nociones básicas de Teoría de Números.
2. Algoritmos de cifrado, firma digital y hash	- Cifrado. Principios de cifrado de Shannon. Cifrado en flujo y cifrado en bloque. Algoritmos DES y AES. Modos de trabajo de los cifradores en bloque. - Integridad y Algoritmos de Hash. - Criptosistemas de clave pública. Algoritmos de firma digital: RSA, ElGamal y DSA.
3. Certificación y PKIs.	- 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.	- 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	- 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 y comercio electrónico	- Problemas de seguridad en la Web. - Protocolos SSL y TLS. - Certificación en la Web. - Principios de comercio electrónico y protocolos de pago. Sistema PayPal.
7. Seguridad en entornos inalámbricos y protocolos AAA.	- Amenazas a la seguridad en entornos inalámbricos. - Wireless Application Protocol (WAP). WTLS. Protocolos WEP, WPA, WPA2 (802.11i). - Protocolos AAA: RADIUS y DIAMETER.
8. Seguridad de Sistemas.	- 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	19	38	57
Resolución de problemas y/o ejercicios	2	0	2
Resolución de problemas y/o ejercicios de forma autónoma	0	10	10
Trabajos tutelados	6	28	34
Prácticas de laboratorio	11	22	33
Pruebas de respuesta larga, de desarrollo	2	10	12
Pruebas prácticas, de ejecución de tareas reales y/o simuladas.	1	0	1

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

<b>Metodologías</b>	
	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.
Resolución de problemas y/o ejercicios de forma autónoma	Se resolverán algunos ejercicios del boletín, de forma que sirvan de guía para la resolución autónoma por el grupo del resto de ejercicios del boletín.
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.
Trabajos tutelados	Se presentarán varios trabajos teóricos y prácticos a desarrollar, entre los cuales cada grupo debe elegir uno. En las clases 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.
Prácticas de laboratorio	El alumno desarrollará una práctica en el laboratorio, enfocada tanto a madurar y llevar a la práctica los conceptos teóricos, como a mejorar su capacidad para el desarrollo y/o implantación de redes y servicios seguros.

### **Atención personalizada**

<b>Metodologías</b>	<b>Descripción</b>
Sesión magistral	El alumno podrá interactuar con el profesor en las horas de tutoría normales para: 1. Tutelar el trabajo o proyecto que elija, tanto antes como durante como después de su realización, validando su orientación, índice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientación y realización de las prácticas de laboratorio. 3. Duda que se le planteen al alumno sobre la realización de los ejercicios del boletín y contenidos teóricos de la asignatura.
Prácticas de laboratorio	El alumno podrá interactuar con el profesor en las horas de tutoría normales para: 1. Tutelar el trabajo o proyecto que elija, tanto antes como durante como después de su realización, validando su orientación, índice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientación y realización de las prácticas de laboratorio. 3. Duda que se le planteen al alumno sobre la realización de los ejercicios del boletín y contenidos teóricos de la asignatura.
Resolución de problemas y/o ejercicios	El alumno podrá interactuar con el profesor en las horas de tutoría normales para: 1. Tutelar el trabajo o proyecto que elija, tanto antes como durante como después de su realización, validando su orientación, índice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientación y realización de las prácticas de laboratorio. 3. Duda que se le planteen al alumno sobre la realización de los ejercicios del boletín y contenidos teóricos de la asignatura.
Trabajos tutelados	El alumno podrá interactuar con el profesor en las horas de tutoría normales para: 1. Tutelar el trabajo o proyecto que elija, tanto antes como durante como después de su realización, validando su orientación, índice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientación y realización de las prácticas de laboratorio. 3. Duda que se le planteen al alumno sobre la realización de los ejercicios del boletín y contenidos teóricos de la asignatura.
Resolución de problemas y/o ejercicios de forma autónoma	El alumno podrá interactuar con el profesor en las horas de tutoría normales para: 1. Tutelar el trabajo o proyecto que elija, tanto antes como durante como después de su realización, validando su orientación, índice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientación y realización de las prácticas de laboratorio. 3. Duda que se le planteen al alumno sobre la realización de los ejercicios del boletín y contenidos teóricos de la asignatura.

### **Evaluación**

	Descripción	Calificación
Resolución de problemas y/o ejercicios de forma autónoma	Valoración de los dos boletines de problemas/ejercicios. El grupo deberá entregar el boletín 1 antes de la semana 10 y el 2 antes de la semana 15.	10
Pruebas de respuesta larga, de desarrollo	Examen final de la asignatura. Este examen constará de unos 8 a 10 ejercicios/problemas/cuestiones sobre los contenidos dados en el curso.	50

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 15.	20
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. El grupo debera entregar el trabajo antes de la semana 15. Todos los integrantes del grupo deben estar presentes en el momento de la presentación.	20

### Otros comentarios sobre la Evaluación

- ELECCION DE EVALUACION CONTINUA.

Los alumnos que opten por evaluacion continua deberan comunicarlo explicitamente al profesor antes de la semana 4 del curso academico. La comunicacion sera por correo electronico.

- CONVOCATORIA DE FIN DE CUATRIMESTRE

La evaluacion continua esta formada por los ejercicios a realizar de forma autonoma, por el trabajo y por las practicas de laboratorio, representando en total el 50% de la asignatura, segun se especifica encima en el descriptivo de pruebas.

Los alumnos que no elijan EC realizaran un examen final por el 80% de la nota, junto con la practica de laboratorio que completara el otro 20%.

El examen final sera el mismo para todos los alumnos, tantos para los que opten por evaluacion continua como para los que no. En el caso de los de evaluacion continua contara como el 50% de la nota, mientras que en los que no opten por evaluacion continua contara por el 80% de la nota.

- CONVOCATORIA DE JULIO

Para los alumnos que no hayan optado en Mayo por evaluacion continua, se realizara un examen final con un valor del 80% junto con el laboratorio que representara el 20%. Se guarda la nota del laboratorio de Mayo. Los alumnos que hayan optado durante el cuatrimestre por EC, podran seguir optando en Julio por EC o bien cambiar a solo evaluacion final. Los alumnos que asi lo hagan deberan comunicarlo explicitamente al profesor por correo electronico.

- En el primer caso, es decir de que sigan por EC en Julio, se guarda las notas del boletin de problemas, practica de laboratorio y trabajo tutelado. Aun asi, el alumno tiene la posibilidad de mejorar cualquiera de ellas hasta llegar a la puntuación máxima correspondiente.
- En el segundo caso, realizaran un examen final por el 80% de la nota y las practicas de laboratorio por el 20%.

La calificacion obtenida en las practicas de laboratorio y trabajos en grupo sera válida solamente durante el curso académico en que se realicen y en el siguiente.

Se considerará a un alumno como "no presentado" si no ha seguido la evaluacion continua y no se ha presentado al examen final.

### Fuentes de información

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

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

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

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

Benjamin M. Lail, **Broadband Network & Device Security**, 1ª ed.,

### 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

---