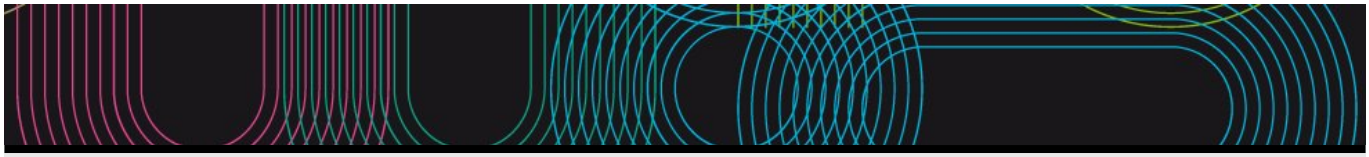

DATOS IDENTIFICATIVOS				
Seguridad				
Asignatura	Seguridad			
Código	V05G300V01543			
Titulacion	Grado en Ingeniería de Tecnologías de Telecomunicación			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OP	3	1c
Lengua Impartición	Castellano			
Departamento	Ingeniería telemática			
Coordinador/a	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 telematicos, y se presentan distintas tecnicas para protegerlos. Primero se aborda el tema desde un punto de vista general, de forma que los conceptos, servicios y tecnicas de seguridad que se estudian, sean aplicables a cualquier tipo de red, servicio telematico o sistema de informacion 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 algoritmica (cifrado, firma digital e integridad), los protocolos de autenticacion, y los procedimientos de gestion y negociacion de claves. El objetivo es que el alumno adquiera una solida base que le capacite para facilitar su comprension de las tecnicas particulares que cada aplicacion requiera asi como para aplicarlo a otros ambitos que tenga que afrontar. Luego se trata el tema de una forma algo mas particular, revisando los problemas, tecnicas y estandares de seguridad en algunos de los entornos de comunicacion de mas prevalencia en la actualidad. Asi 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 telematica. Se presentan los principales problemas de seguridad en el comercio electronico a traves de la Web y se estudia el funcionamiento del Paypal, uno de los metodos de pago mas utilizados en la Web. Dada la utilización cada vez mayor de las comunicaciones por medio inalambrico y sus particulares problemas de seguridad, se dedica tambien un tema a ellos. Se cierra el curso con una introduccion a otros dos temas de trascendencia creciente: las redes y software malicioso y el analisis forense de sistemas de informacion.			

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 teorias matemáticas en las que se sustenta la seguridad de los algoritmos y protocolos criptográficos usados para la protección de la información en 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 telematicos, sistemas de telecomunicación y sistemas de información.	A3
Conocimiento de los diferentes metodos, 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 matematicos de la seguridad.	- Nociones de Teoria 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 publica. Algoritmos de firma digital: RSA, ElGamal y DSA.
3. Certificacion y PKIs.	- Problematica de seguridad en la criptografia asimetrica. Certificacion 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.	- Metodos de autenticación. - Amenazas a un protocolo de autenticación. Contramedidas. - Requisitos de un protocolo de convenio de clave. Protocolo D-H. - Autenticación en criptosistemas simetricos. Casos de estudio: Autenticación en GSM, Protocolo Kerberos. - Autenticacion en criptosistemas asimetricos. Casos de estudio: autenticacion X509 y SSL. - Protocolos basados en contraseñas: SRP.
5. Seguridad en el nivel de Red	- Analisis de amenazas en el nivel de red. - Arquitectura de seguridad en IP. - Protocolo IPsec. Tuneles IPsec. IPsec y NAT. - Protocolos para gestion de claves: IKE, ISAKMP y OAKLEY.
6. Seguridad en la Web y comercio electronico	- Problemas de seguridad en la Web. - Protocolos SSL y TLS. - Certificacion en la Web. - Principios de comercio electrónico y protocolos de pago.
7. Seguridad en entornos inalambricos y protocolos AAA.	- Amenazas a la seguridad en entornos inalambricos. - Wireless Aplication 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. - Analisis 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
Trabajos y proyectos	1	0	1

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

Metodologías

	Descripción
Sesión magistral	Exposición mediante presentacion en powerpoint y pizarra de los contenidos teoricos de la asignatura. Se desarrollarán los temas teóricos de la materia que no queden cubiertos por las otras metodologias empleadas. Con esta metodología el alumno adquirirá parte de las competencias A3 y A37.
Resolución de problemas y/o ejercicios	Se resolverán algunos ejercicios del boletin, de forma que sirvan de guia para la resolución autonoma por el grupo del resto de ejercicios del boletín. Esta metodologia esta orientada a la competencia A4.
Resolución de problemas y/o ejercicios de forma autónoma	El grupo resolverá de forma autonoma los ejercicios del boletin no realizados en las horas presenciales. Las diversas soluciones que surjan al abordar cada problema, seran puestas en comun para consensuar la mejor forma de resolución. Las dudas surgidas se consensuarán y podrán exponerse al tutor en las horas normales de tutoria. Esta metodología esta orientada a la competencia A4.
Trabajos tutelados	Se presentaran varios trabajos teóricos y practicos a desarrollar, entre los cuales cada grupo debe 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 A4, A6 y A37.
Prácticas de laboratorio	El alumno desarrollara una practica en el laboratorio, enfocada tanto a madurar y llevar a la practica los conceptos teoricos, como a mejorar su capacidad para el desarrollo y/o implantacion de redes y servicios seguros. Esta metodología esta orientada a las competencias A6 y A37.

Atención personalizada

Metodologías	Descripción
Sesión magistral	El alumno podrá interactuar con el profesor en las horas de tutoria normales para: 1. Tutelar el trabajo o proyecto que elejido, tanto antes como durante como despues de su realización, validando su orientación, indice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientacion y realizacion de las practicas 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 tutoria normales para: 1. Tutelar el trabajo o proyecto que elejido, tanto antes como durante como despues de su realización, validando su orientación, indice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientacion y realizacion de las practicas 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 tutoria normales para: 1. Tutelar el trabajo o proyecto que elejido, tanto antes como durante como despues de su realización, validando su orientación, indice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientacion y realizacion de las practicas 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 tutoria normales para: 1. Tutelar el trabajo o proyecto que elejido, tanto antes como durante como despues de su realización, validando su orientación, indice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientacion y realizacion de las practicas 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 tutoria normales para: 1. Tutelar el trabajo o proyecto que elejido, tanto antes como durante como despues de su realización, validando su orientación, indice de contenidos, organización, parte descriptiva y ausencia de errores. 2. Resolver cualquier tipo de duda concerniente a la orientacion y realizacion de las practicas 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 boletin 1 antes de la semana 10 y el 2 antes de la semana 15. Con esta prueba se evaluaran parte de las competencias A3, A4 y A37	10
Pruebas de respuesta larga, de desarrollo	Examen final de la asignatura. Este examen constara de un conjunto de ejercicios/problemas/cuestiones sobre los contenidos dados en el curso. Con esta prueba se evaluara otra parte de las competencias A3 y A4 y A37	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. Con esta prueba se evaluara una parte de la competencias A6 y otra parte de la A37	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. Con esta prueba se evaluara otra parte de las competencias A4 y A6 y otra parte de la A37.	20

Otros comentarios sobre la Evaluación

- ELECCION DE EVALUACION CONTINUA.

  Los alumnos que opten por evaluación continua deberán comunicarlo explícitamente al profesor antes de la semana 4 del curso académico. Pasado este plazo se considerara que el alumno va por no continua. La comunicación sera por correo electrónico.

- CONVOCATORIA DE FIN DE CUATRIMESTRE

  La evaluacion continua esta formada por los ejercicios a realizar de forma autonoma, por el trabajo o proyecto y por las practicas de laboratorio, representando en total el 50% de la asignatura, segun se especifica encima en el apartado de evaluación. El otro 50% corresponde a un examen final.

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

  El examen final será 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 la primera convocatoria por evaluación 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 las notas del boletín de problemas, practica de laboratorio y proyecto tutelado. Aun asi, el alumno tiene la posibilidad de mejorar cualquiera de ellas hasta llegar a la puntuación máxima correspondiente.
  - En el segundo caso, es decir de que se cambie de EC a ET en Julio, realizaran un examen final por el 80% de la nota y las prácticas de laboratorio por el 20%.

- OTRAS OBSERVACIONES.

- *Nota mínima en teoría.* Se opte o no por EC e independientemente de la convocatoria, será obligatorio sacar un mínimo de 3,33 puntos sobre 10 (es decir, 1/3 de la nota maxima) en el examen teórico, para poder aprobar la asignatura.
- Se considerará a un alumno como "no presentado" si no ha seguido la evaluacion continua y no se ha presentado al examen final.
- Las calificaciones obtenidas en las practicas de laboratorio y proyecto en grupo solamente será válida durante el curso académico en que se realicen.

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