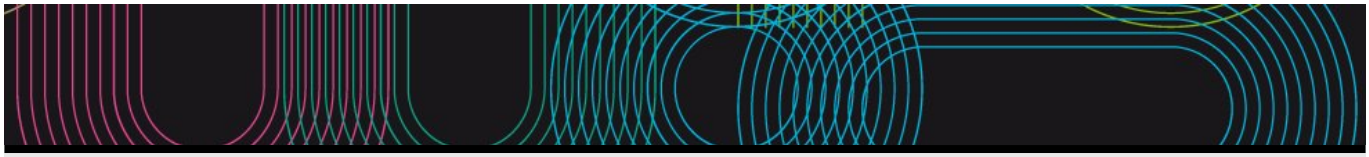

DATOS IDENTIFICATIVOS				
Seguridad				
Asignatura	Seguridad			
Código	V05G306V01305			
Titulacion	Grado en Ingeniería de Tecnologías de Telecomunicación (docencia en inglés)			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OP	3	1c
Lengua Impartición	Castellano			
Departamento	Ingeniería telemática			
Coordinador/a	Fernández Masaguer, Francisco Rodríguez Rubio, Raúl Fernando			
Profesorado	Fernández Masaguer, Francisco Rodríguez Rubio, Raúl Fernando			
Correo-e	francisco.fernandez@det.uvigo.es rrubio@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 asi como para aplicarlo a otros ámbitos que tenga que afrontar. Luego se trata el tema de una forma algo mas particular, revisando los problemas, técnicas y estandares de seguridad en algunos de los entornos de comunicación 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 telemática, donde el alumno asimilará los conceptos teóricos y prácticos del protocolo SSL, central para la seguridad de la 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.			

Resultados de Formación y Aprendizaje	
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 deuna 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 religion, respeto a los derechos fundamentales, accesibilidad, etc.

Resultados previstos en la materia

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.	- Nociones basicas de Teoría de la Complejidad - Nociones básicas de Teoría de Números.
2. Algoritmos de hash, cifrado y firma digital.	- Tipos de criptosistemas. - 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, DSA y curvas elípticas. - Influencia de la computacion cuantica en la criptografia.
3. Certificación e infraestructuras de certificación (PKIs)	- Problemática de seguridad en la criptografía asimétrica. Certificación. - Modelos de confianza. Confianza plana. Confianza en terceros y autoridades de certificación. - Infraestructuras de certificación. Ruta de certificación. - Revocación de certificados.
4. 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 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. - Single Sign On (SSO)
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/IKEv2, ISAKMP y OAKLEY.
6. Seguridad en la Web	- Problemas de seguridad en la Web. - Protocolos SSL y TLS. - Certificación en la Web.
7. Seguridad en entornos inalámbricos y protocolos AAA.	- Amenazas a la seguridad en entornos inalámbricos. - Wireless Aplication Protocol (WAP). WTLS. Protocolos WEP, WPA, WPA2 (802.11i). - Protocolos AAA: RADIUS.
8. Seguridad de Sistemas.	- Cortafuegos y sistemas contra intrusiones. - Software y redes maliciosas. - Análisis Forense de Sistemas.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	21	38	59
Resolución de problemas de forma autónoma	0	10	10
Trabajo tutelado	6	28	34
Prácticas de laboratorio	11	22	33
Práctica de laboratorio	1	0	1
Trabajo	1	0	1

Examen de preguntas de desarrollo	1	5	6
Examen de preguntas 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
Lección 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 de forma autónoma	El alumno resolverá de forma autónoma los ejercicios del boletín no realizados en las horas presenciales. 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.
Trabajo tutelado	Trabajo en grupo. 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	Trabajo en grupo. El grupo desarrollará una o dos prácticas en el laboratorio, enfocadas 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. 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.
Trabajo tutelado	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 de forma autónoma	Revisión y comentarios de los diversos ejercicios propuestos. El alumno podrá disponer en Faitic de la solución a varios de los ejercicios que se propongan.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje		
Práctica de laboratorio	Prueba de grupo en la que el profesor valorará las prácticas de laboratorio, revisando su funcionamiento con los integrantes del grupo presentes. Esta prueba se realizará en la ultima o penúltima semana del cuatrimestre, según publicará en Moovi en las primeras semanas del cuatrimestre. Todos los integrantes del grupo deben estar presentes en el momento de la presentación. Se realizará una entrevista de autoría de la que se determinará el nivel de participación de cada alumno y de la que, junto con el correcto funcionamiento, se deducirá la nota individual.	25	B6	C28	D3
Trabajo	Prueba de grupo. Valoración del proyecto o trabajo tutelado realizado por el grupo (tipo C). El grupo hará una demostración al profesor del proyecto o trabajo realizado y resultados obtenidos. Esta prueba se realizará en la ultima o penúltima semana del cuatrimestre, según publicará en Moovi en las primeras semanas del cuatrimestre. Todos los integrantes del grupo deben estar presentes en el momento de la presentación. Se realizará una entrevista de autoría de la que se determinará el nivel de participación de cada alumno en el proyecto y de la que, junto con la documentación y el correcto funcionamiento, se deducirá la nota individual.	25	B4 B6	C28	D2 D3

Examen de preguntas de desarrollo	Examen final de la asignatura. Este examen constará de un conjunto de ejercicios/cuestiones sobre los contenidos dados en el curso.	25	B3 B4	C28
Examen de preguntas de desarrollo	Examen parcial de la asignatura, obligatorio para los alumnos que vayan por EC. Este examen constará de un conjunto de ejercicios/cuestiones sobre los contenidos dados hasta aproximadamente la mitad del curso teórico.	25	B3 B4	C28

Otros comentarios sobre la Evaluación

- ELECCION DE EVALUACION CONTINUA.

  Por defecto se considerará que el alumnado va por evaluación continua. Si un alumno desea ir por evaluacion global deberá comunicarlo al profesorado antes de concluir la semana 5 del cuatrimestre. La comunicación será por correo electrónico.

- OPORTUNIDAD ORDINARIA.

  Evaluación continua. La evaluación continua (EC) estará formada por:

  1. Trabajo B de laboratorio, representando un 25% de la nota. Este trabajo deberá ser entregado via Moovi. La fecha concreta de entrega se publicará en Moovi en las primeras semanas del cuatrimestre, tras reunión de coordinación con el resto de materias.
  2. Proyecto C, representando un 25% de la nota. Este proyecto deberá ser entregado vía Moovi. La fecha concreta tope de entrega se publicará en Moovi en las primeras semanas del cuatrimestre, tras reunión de coordinación con el resto de materias.
  3. La planificación de las diferentes pruebas de evaluación intermedia se aprobará en una Comisión Académica de Grado (CAG) y estará disponible al principio del cuatrimestre'
  4. Examen parcial de los contenidos dados hasta aproximadamente la mitad del cuatrimestre, representando el 50% de la nota total de teoría. Este examen promediará con el examen final si el alumno saca un mínimo de 3.5 puntos sobre 10. Si el alumno saca una nota inferior a esta, deberá volver a evaluarse de esta parte en el examen final. La fecha de realización de esta prueba intermedia se aprobara en una Comisión Académica de Grado y estará disponible a principio del cuatrimestre.
  5. Examen final, en la fecha acordada en Junta de Escuela. Habrá dos casos:

     - Alumnado que haya superado la nota mínima del examen parcial. En este examen entrarán los temas dados desde aproximadamente la mitad del cuatrimestre 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 3,5 puntos sobre 10.
     - Alumnado que no haya superado 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 deberá obtener en este examen una nota mínima de 3,5 puntos sobre 10, con un mínimo de 3,5 puntos en cada una de las dos partes del examen.

  Evaluación global. El alumnado que opte por evaluación global (EG) realizará un examen teórico final por el 80% de la nota, junto con las prácticas de laboratorio B, que completará el otro 20%.

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

- OPORTUNIDAD EXTRAORDINARIA.

  Para el alumnado que haya optado en la oportunidad ordinaria por evaluación única, se realizará un examen final con un valor del 80%, junto con el trabajo B de laboratorio que representará el 20%. Se guarda la nota

del laboratorio de la convocatoria ordinaria.
El alumnado que haya optado durante el cuatrimestre por EC, podrá seguir por EC o bien cambiar a evaluación global (el alumnado os que así lo haga deberá comunicarlo explícitamente al profesorado por correo electrónico no mas tarde de una semana antes de la fecha del examen extraordinario):

- En el primer caso, es decir, de que sigan por EC en la oportunidad extraordinaria, la nota total constará, al igual que en la convocatoria ordinaria, del 50% de la parte teórica, 25% de las prácticas de laboratorio y 25% del proyecto tutelado. Se guarda, de la oportunidad ordinaria, las notas del examen parcial y final (siempre que hayan superado la nota mínima), de la práctica de laboratorio (representando un 25%) y del proyecto tutelado (25%). Deberá presentarse al examen teórico final de la convocatoria todo el alumnado que no hayan superado la nota mínima teórica, en alguna de las dos partes del examen, de la convocatoria ordinaria, pero solo sera necesario realizar el examen de la parte o partes de las que no se haya alcanzado ese minimo (3,5).
- En el segundo caso, es decir, de que se cambie de EC a EG, realizará un examen teórico final por el 80% de la nota y las prácticas de laboratorio por el 20%. Se conservará la nota del laboratorio de la convocatoria ordinaria, adecuadamente porcentuada.

El alumnado que cambie de EG a EC se le conserva la nota del laboratorio B, adecuadamente porcentuada.

- OTRAS OBSERVACIONES.
  - ***Nota mínima en teoría.*** Independientemente de la convocatoria, será obligatorio sacar un mínimo de 3,5 puntos sobre 10 para EC y 4 puntos sobre 10 para evaluacion global, en cada una de las dos partes del examen teórico, para poder aprobar la asignatura.
  - Se considerará a un alumno/a como "No Presentado" si no ha seguido la evaluación continua y no se ha presentado al examen teorico 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 4.9 puntos (suspenso).

- CONVOCATORIA DE FIN DE CARRERA.
  - La evaluación en la convocatoria de fin de carrera estará formada por:
    - Examen teórico (50%). Examen individual de los contenidos de la asignatura representando el 50% de la nota total. El alumnado deberá obtener una nota minima de 3,5 puntos (en cada una de las dos partes del examen) sobre 10 para aprobar la asignatura.
    - Trabajo B de laboratorio, representando un 25% de la nota.
    - Proyecto C, representando un 25% de la nota.

Fuentes de información

Bibliografía Básica

F. Fernandez Masaguer, **Apuntes de Seguridad en Redes y Sistemas de Informacion**, 1ª ed., Revisión 2023

William Stallings, **Cryptography and Network Security. Principles and practice.**, 8ª ed., Pearson, 2020

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/V05G301V01310
Servicios de internet/V05G301V01301

Asignaturas que se recomienda haber cursado previamente

Programación II/V05G301V01110