



DATOS IDENTIFICATIVOS

Seguridade

Materia	Seguridade			
Código	V05G300V01543			
Titulación	Grao en Enxeñaría de Tecnoloxías de Telecomunicación			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OP	3	1c
Lingua de impartición	Castelán			
Departamento	Enxeñaría telemática			
Coordinador/a	Fernández Masaguer, Francisco			
Profesorado	Fernández Masaguer, Francisco			
Correo-e	francisco.fernandez@det.uvigo.es			
Web	http://faitic.uvigo.es			

Descrición xeral Nesta asignatura estúdanse, dun xeito unificado, os principais problemas ou ameazas de seguridade nas redes e servizos telemáticos, e preséntanse distintas técnicas para protexelos.

Primeiro abórdase o tema desde un punto de vista xeral, de forma que os conceptos, servizos e técnicas de seguridade que se estudan, sexan aplicables a calquera tipo de rede, servizo telemático ou sistema de información a securizar. Este bloque fórmalo os temas 1 ao 4. Isto leva a tratar con detalle os tres temas centrais da seguridade: a parte algorítmica (cifrado, firma dixital e integridade), os protocolos de autenticación, e os procedementos de xestión e negociación de claves. O obxectivo é que o alumno adquira unha adoitada base que lle capacite para facilitar a súa comprensión das técnicas particulares que cada aplicación requira así como para aplicalo a outros ámbitos que teña que afrontar.

Logo trátase o tema dunha forma algo máis particular, revisando os problemas, técnicas e estándares de seguridade nalgúns dos entornos de comunicación de máis prevalencia na actualidade. Así dedícase un tema á seguridade a nivel IP, protocolo central na arquitectura Internet, e outro tema á seguridade na Web, onde o alumno asimilará os conceptos teóricos e prácticos do protocolo SSL, central para a seguridade das transaccións a través da Web. Dada a utilización cada vez maior das comunicacións por medio inalámbrico e os seus particulares problemas de seguridade, dedícase tamén un tema a eles. Péchase o curso cunha introducción a outros dous temas de transcendencia crecente: as redes e software malicioso e o análise forense de sistemas de información.

Competencias

Código	
B3	CG3 Coñecemento de materias básicas e tecnoloxías que capaciten o alumnado para a aprendizaxe de novos métodos e tecnoloxías, así como para dotalo dunha gran versatilidade para adaptarse a novas situacións.
B4	CG4 Capacidade para resolver problemas con iniciativa, para a toma de decisións, a creatividade, e para comunicar e transmitir coñecementos, habilidades e destrezas, comprendendo a responsabilidade ética e profesional da actividade do Enxeñeiro Técnico de Telecomunicación.
B6	CG6 Facilitade para o manexo de especificacións, regulamentos e normas de obrigado cumprimento.
C28	CE28/TEL2 Capacidade para aplicar as técnicas en que se basean as redes, servizos e aplicacións telemáticas, tales como sistemas de xestión, sinalización e conmutación, encamiñamento e enrutamento, seguridade (protocolos criptográficos, tunelado, devasas, mecanismos de cobro, de autenticación e de protección de contidos), enxeñaría de tráfico (teoría de grafos, teoría de colas e teletráfico) tarificación e fiabilidade e calidade de servizo, tanto en contornas fixas, móbiles, persoais, locais ou a gran distancia, con diferentes anchos de banda, incluíndo telefonía e datos.
D2	CT2 Concibir a Enxeñaría no marco do desenvolvemento sostible.
D3	CT3 Tomar conciencia da necesidade dunha formación e mellora continua de calidade, amosando unha actitude flexible, aberta e ética ante opinión discriminación por sexo, raza ou relixión, respecto os dereitos fundamentais, acesibilidade, etc.

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe		
Comprender os fundamentos da ciencia criptográfica.	B3		
Adquirir os coñecementos necesarios para asegurar a seguridade dun sistema informático ou telemático.	B3		
Adquirir habilidades sobre o proceso de análise dos ataques que pode sufrir unha rede e os principais mecanismos de defensa contra eles.	B4	C28	D3
Coñecer as principais arquitecturas de seguridade aplicables aos sistemas informáticos e telemáticos.	B4	C28	D3
Coñecer as principais ideas das normas e estándares máis importantes en materia de seguridade en sistemas informáticos e en redes de comunicación.	B6	C28	D2

Contidos

Tema	
1 Fundamentos matemáticos da seguridade.	- Nocións de Teoría da Complexidade. - Revisión de Teoría de Números.
2. Algoritmos de cifrado, firma dixital e hash	- Tipos de criptosistemas e algoritmos. - Integridade e Algoritmos de Hash. - Ciptosistema de chave simétrica. Funciones Mac. Cifrado. Principios de cifrado de Shannon. Cifrado en fluxo e cifrado en bloque. Algoritmos DES e AES. Modos de traballo dos cifradores en bloque. - Ciptosistemas de chave pública. RSA e DSA.
3. Certificación e PKIs.	- Problemática da seguridade na criptografía asimétrica. Certificación e formatos de certificados. - Modelos de confianza. Confianza plana e modelo PGP. Confianza en terceiros e autoridades de certificación. - Infraestructuras de certificación. Ruta de Certificación. Revocación de certificados.
4. Protocolos de autenticación e convenio de clave.	- Métodos de autenticación. - Ameazas a un protocolo de autenticación. Contramedidas. - Requisitos dun protocolo de convenio de chave. Protocolo D-H. - Autenticación en criptosistemas simétricos. Casos de estudo: GSM y Kerberos. - Autenticación en criptosistemas asimétricos. Casos de estudo: autenticación X509 e SSL. - Protocolos baseados en contrasinais: SRP.
5. Seguridade no nivel de Rede	- Análise de ameazas no nivel de rede. - Arquitectura de seguridade en IP. - Protocolo IPsec. Tuneles IPsec. IPsec e NAT. - Xestión de chaves. Protocolos IKE, ISAKMP e OAKLEY.
6. Seguridade na Web	- Problemas de seguridade na Web. - Protocolos SSL e TLS. - Certificación na Web.
7. Seguridade en comunicacións inalámbricas e protocolos AAA.	- Ameazas a seguridade en comunicacións inalámbricas. - Wireless Application Protocol (WAP). WTLS. Protocolos WEP, WPA, WPA2. - Protocolos AAA: RADIUS
8. Seguridade de Sistemas.	- Cortalumes e sistemas contra intrusións. - Software e redes maliciosas. Botnets. - Análise Forense de Sistemas de Información.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	21	38	59
Resolución de problemas e /ou exercicios de forma autónoma	0	10	10
Traballo tutelado	6	28	34
Prácticas de laboratorio	11	22	33
Probas prácticas, de execución de tarefas reais e/ou simuladas.	1	0	1
Traballos e proxectos	1	0	1
Probas de resposta longa, de desenvolvemento	1	5	6
Probas de resposta longa, de desenvolvemento	1	5	6

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente

	Descrición
Lección maxistral	Exposición mediante presentación en powerpoint e pizarra dos contidos teóricos da asignatura. Desenvolveranse os temas teóricos da materia que non queden cubertos polas outras metodoloxías empregadas. Con esta metodoloxía o alumno adquirirá parte das competencias CG3 y CE28.
Resolución de problemas e /ou exercicios de forma autónoma	O grupo resolverá de forma autónoma os exercicios do boletín non realizados nas horas presenciais. As diversas solucións que xurdan ao abordar cada problema, serán postas en común para acordar a mellor forma de resolución. As dúbidas xurdidas acordaranse e poderán exporse ao titor nas horas normais de tutoría. Esta metodoloxía esta orientada as competencias CG4 e CE28.
Traballo tutelado	Presentaranse varios traballos teóricos e prácticos a desenvolver, entre os cales cada grupo debe elixir un. Na clase tipo C, exporase a cada grupo os obxectivos do traballo, ferramentas hardware e software a usar, forma de acometelo e realizarase un seguimento a cada grupo. Esta metodoloxía esta orientada a adquisición das competencias CG4, CG6, CE28, CT2 y CT3.
Prácticas de laboratorio	O alumno desenvolverá unha práctica no laboratorio, enfocada tanto a madurar e levar a práctica os contidos teóricos, como a mellorar a súa capacidade para o desenvolvemento e/ou implantación de redes e servizos seguros. Esta metodoloxía esta orientada as competencias CG6, CE28, CT2 y CT3.

Atención personalizada

Metodoloxías	Descrición
Prácticas de laboratorio	Seguimento individualizado do traballo de cada grupo. Comentarios de forma conxunta de diversas recomendacións e estratexias para a boa realización do proxecto. Revísase con cada grupo o nivel de comprensión e avance do proxecto, dúbidas particulares que poidan xurdir, erros de deseño e codificación Xava. Axuda para a comprensión dos paquetes JCA/JCE e JSSE. Axuda individualizada para a instalación da ferramenta de xestión de almacéns de claves (keyStores) e do código Xava básico da práctica.
Traballo tutelado	Seguimento individualizado do traballo de cada alumno de cada grupo. Comentarios de forma conxunta de diversas recomendacións e estratexias para a boa realización do proxecto. Revísase con cada grupo o nivel de comprensión e avance do proxecto, dúbidas particulares que poidan xurdir, erros de deseño ou formulación e opcións de mellora.
Resolución de problemas e /ou exercicios de forma autónoma	Revisión e comentarios dos diversos exercicios propostos. O alumno poderá dispor en Faitic da solución a varios dos exercicios que se propoñan.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe		
Probas prácticas, de execución de tarefas reais e/ou simuladas.	Proba de grupo na que o profesor valorará a práctica de laboratorio, revisando o seu funcionamento cos integrantes do grupo presentes. Esta proba realizarase na semana do 9 ao 13 de Xaneiro. Todos os integrantes do grupo deben estar presentes no momento da presentación. Realizarase unha entrevista de autoría da que se determinará o nivel de participación de cada alumno e da que, xunto co correcto funcionamento, se deducirá a nota individual.	25	B6	C28	D3
Traballos e proxectos	Proba de grupo. Valoración do proxecto ou traballo tutelado realizado polo grupo (tipo C). O grupo fara unha demostración ao profesor do proxecto ou traballo realizado e resultados obtidos. Esta proba realizárase na semana do 9 ao 13 de Xaneiro. Todos os integrantes do grupo deberan estar presentes no momento da presentación. Realízase unha entrevista de autoría da que se determinará o nivel de participación de cada alumno no proxecto e da que, xunto co correcto funcionamento, se deducirá a nota individual.	25	B4 B6	C28	D2 D3
Probas de resposta longa, de desenvolvemento	Exame final da materia. Este exame consta dun conxunto de exercicios/cuestións sobre os contidos dados no curso a partir da semana 7, o de todo o curso para aqueles alumnos que non superen a nota mínima no examen parcial.	25	B3 B4	C28	
Probas de resposta longa, de desenvolvemento	Exame parcial da materia, obrigatorio para os alumnos que vaian por EC. Este exame constase dun conxunto de exercicios/cuestións sobre os contidos dados ata (inclusive) a semana 6 do curso teórico.	25	B3 B4	C28	

- ELECCION DE AVALIACIÓN CONTINUA.

Por defecto considerárase que o alumno vai por avaliación continua (EC). Se un alumno desexa ir por non continua (ET) deberá comunicalo ao profesor antes da semana 4 do curso académico. A comunicación sera por correo electrónico.

- PRIMEIRA CONVOCATORIA.

Avaliación continua. A avaliación continua estará formada por:

1. Traballo de laboratorio B, representando un 25% da nota. Este traballo debera ser entregado via Faitic antes do día 8 de Xaneiro.
2. Proxecto C, representando un 25% da nota. Este proxecto debera ser entregado via Faitic antes do día 8 de Xaneiro.
3. Exame parcial dos contidos dados ata a 6 semana inclusive, representando o 25% da nota. Este exame promediará co exame final se o alumno saca un mínimo de 1/3 do total da nota. Se o alumno saca unha nota inferior a esta deberá volver a avaliarse desta parte no exame final. Este exame realizáse na semana 7 do curso académico.
4. Exame final, na data acordada en Xunta de Escola. Habra dous casos:
 - Alumnos que haxan superado a nota mínima do exame parcial. Neste exame entrarán os temas dados desde a 7 semana ata o final. Representará un 25% da nota total. Para poder superar a materia o alumno deberá obter neste exame unha nota mínima de 3,33 puntos sobre 10.
 - Alumnos que non haxan superado a nota mínima do exame parcial. Neste exame entrarán todos os temas dados no curso teórico. Representará un 50% da nota total. Para poder superar a materia o alumno deberá obter neste exame unha nota mínima de 3,33 puntos sobre 10.

Avaliación non continua. Os alumnos que non elixan avaliación continua faran un exame final polo 80% da nota, xunto con as prácticas de laboratorio que completa o outro 20%. Sera necesario sacar un mínimo de 1/3 do exame teórico para poder superar a materia.

O exame final será o mesmo para todos os alumnos, tantos para os que opten por avaliación continua como para os que non.

- CONVOCATORIA DE XULLO

Para os alumnos que optasen na primeira convocatoria por avaliación non continua, realizarase un exame final cun valor do 80%, xunto co laboratorio que representará o 20%. Se garda a nota do laboratorio da primeira convocatoria.

Os alumnos que optasen durante o cuadrimestre por EC, poderán seguir optando en xullo por EC ou ben cambiar a só avaliación final. Os alumnos que así o fagan deberán comunicalo explicitamente ao profesor por correo electrónico:

- No primeiro caso, é dicir de que sigan por EC en xullo, se garda, da primeira convocatoria, as notas do exame parcial e final (sempre que superasen a nota mínima) de práctica de laboratorio e do proxecto tutelado. Deberan presentarse ao exame final da convocatoria todos os alumnos que non superasen a nota mínima teórica da primeira convocatoria.
- No segundo caso, é dicir de que se cambie de EC a ET (no continua) en xullo, realizarase un exame final polo 80% da nota e as prácticas de laboratorio polo 20%. Mantendrase a nota do laboratorio

obtida na primeira convocatoria, axeitadamente porcentuada.

- OUTRAS OBSERVACIÓNS.

- *Nota mínima en teoría.* Óptese ou non por EC e independentemente da convocatoria, será obrigatorio sacar un mínimo de 1/3 da nota máxima (3,33 puntos sobre 10 para EC e 3,75 sobre 10 para ET) no exame teórico, para poder aprobar a materia.
- Considerarase a un alumno/a como "non presentado" se non seguiu a avaliación continua e non se presentou ao exame final. Igualmente, se o alumno/a seguiu a avaliación continua (EC) e non se presentou o examen de ningunha das partes A,B y C , considerarase a un alumno/a como "non presentado".
- As cualificacións obtidas en as prácticas de laboratorio e proxecto en grupo soamente serán válidas durante o curso académico en que se realicen.
- Se a nota total é igual ou superior a 5 pero non se acadou a nota mínima nalgunha, a nota final será 4.5 puntos (suspense).

Bibliografía. Fontes 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

Recomendacións

Materias que se recomenda cursar simultaneamente

Arquitecturas e servizos telemáticos/V05G300V01645

Servizos de internet/V05G300V01501

Materias que se recomenda ter cursado previamente

Matemáticas: Álgebra lineal/V05G300V01104

Redes de ordenadores/V05G300V01403