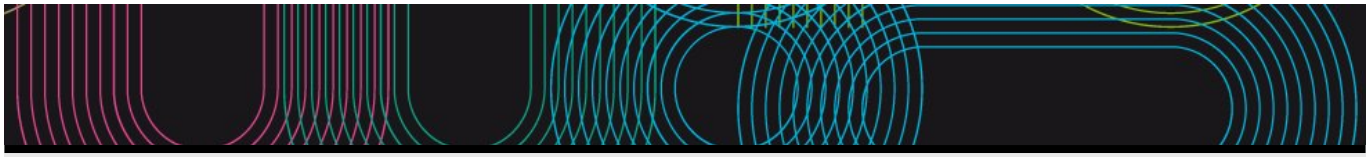

DATOS IDENTIFICATIVOS				
Seguridade				
Materia	Seguridade			
Código	V05G301V01305			
Titulación	Grao en Enxeñaría de Tecnoloxías de Telecomunicación			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OP	3	1c
Lingua de impartición	Castelán			
Departamento	Enxeñaría telemática			
Coordinador/a	Fernández Masaguer, Francisco 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://moovi.uvigo.gal			
Descrición xeral	Nesta asignatura estúdianse, dunha maneira unificada, 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 asegurar. Este bloque forman-no 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 chaves. O obxectivo é que o alumno adquira unha base sólida que lle capacite para facilitar a súa comprensión das técnicas particulares que cada aplicación require así como para aplicalo a outros ámbitos cos que teña que enfrontarse. Logo trátase o tema dunha forma algo máis particular, revisando os problemas, técnicas e estándares de seguridade en algúns dos entornos de comunicación máis prevalentes na actualidade. Así dedícase un tema á seguridade a nivel IP, protocolo central na arquitectura Internet, e outro tema á seguridade na Web, dada a vixencia actual deste medio de intercomunicación telemática, 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, tamén se dedica un tema a eles. Pecha o curso cunha introdución a outros dous temas de transcendencia crecente: as redes e software malicioso e o análise forense de sistemas de información.			

Resultados de Formación e Aprendizaxe	
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 Facilidade 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 previstos na materia

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 basicas de Teoría da Complexidade. - Nocions basicas de Teoría dos Números.
2. Algoritmos de cifrado, sinatura dixital e hash.	- Tipos de criptosistemas e algoritmos. - Integridade e Algoritmos de Hash. - Criptosistemas de chave simétrica. Funcions 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. - Criptosistemas de chave pública. RSA, DSA e curva eliptica. - Influencia da computacion cuantica na criptografia.
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 autenticidade e convenio de chave.	- Métodos de autenticidade. - Ameazas a un protocolo de autenticidade. Contramedidas. - Requisitos dun protocolo de convenio de chave. Protocolo D-H. - Autenticidade en criptosistemas simétricos. Casos de estudo: GSM y Kerberos. - Autenticidade en criptosistemas asimétricos. Casos de estudo: autenticidade X509 e SSL. - Protocolos baseados en contrasinais: SRP, SAE-Dragonfly. - Single Sign On (SSO).
5. Seguridade no nivel de Rede	- Analise de ameazas no nivel de rede. - Arquitectura de seguridade en IP. - Protocolo IPsec. Túneles 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 sen fíos e protocolos AAA.	- Ameazas a seguridade en comunicacións sen fíos. - Wireless Aplication Protocol (WAP).WTLS. Protocolos WEP, WPA, WPA2, WPA3. - Protocolos AAA: RADIUS
8. Seguridade de Sistemas.	- Cortalumes e sistemas contra intrusións. - Software e redes maliciosas. - Análise Forense de Sistemas da Información.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	21	38	59
Resolución de problemas de forma autónoma	0	10	10
Traballo tutelado	6	28	34
Prácticas de laboratorio	11	22	33
Práctica de laboratorio	1	0	1
Traballo	1	0	1
Exame de preguntas de desenvolvemento	1	5	6
Exame de preguntas 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 de forma autónoma	O alumno resolverá de forma autonoma os exercicios do boletin non realizados nas horas presenciais. 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	Traballo en grupo. 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	Traballo en grupo. O grupo desenvolverá unha ou duas prácticas no laboratorio, enfocadas 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 realizacion 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 comprension dos paquetes JCA/JCE e JSSE. Axuda individualizada para a instalación da ferramenta de xestión de almacéns de chaves (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 de forma autónoma	Revisión e comentarios dos diversas exercicios propostos. O alumno podrá dispor en Faitic da solución a varios dos exercicios que se propoñan.

Avaliación					
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe		
Práctica de laboratorio	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 ultíma ou penúltima semana do cuadrimestre, segundo se publicará en Moovi nas primeiras semanas do cuadrimestre. 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
Traballo	Proba de grupo. Valoración do proxecto ou traballo tutelado realizado polo grupo (tipo C). O grupo fará unha demostración ao profesor do proxecto ou traballo realizado e resultados obtidos. Esta proba realizarase na ultíma ou penúltima semana do cuadrimestre, segundo se publicará en Moovi nas primeiras semanas do cuadrimestre. Todos os integrantes do grupo deberán estar presentes no momento da presentación. Realizárase 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
Exame de preguntas 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	

Exame de preguntas de desenvolvemento	Exame parcial da materia, obrigatorio para os alumnos que vaian por AC. Este exame constará dun conxunto de exercicios/cuestións sobre os contidos dados ata aproximadamente a mitade do curso teórico.	25	B3 B4	C28

Outros comentarios sobre a Avaliación

- ELECCION DE AVALIACIÓN CONTINUA.

  Por defecto considerarase que o alumnado vai por avaliación continua (AC). Si un alumno desexa ir por avaliación global (AG) deberá comunicalo ao profesorado antes de concluír a semana 5 do cuadrimestre. A comunicación será por correo electrónico ao profesorado.

- **OPORTUNIDADE ORDINARIA.**

  Avaliacion continua. A avaliación continua (AC) estará formada por:

  1. Traballo B de laboratorio, representando un 25% da nota. Este traballo deberá ser entregado via Moovi. A data concreta de entrega publicarase en Moovi nas primeiras semanas do cuadrimestre, tras reunión de coordinación co resto das materias.
  2. Proxecto C, representando un 25% da nota. Este proxecto deberá ser entregado via Moovi. A data concreta de entrega publicarase en Moovi nas primeiras semanas do cuadrimestre, tras reunión de coordinación co resto das materias.
  3. Exame parcial dos contidos dados ata aproximadamente a metade do cuadrimestre, representando o 50% da nota total de teoria. Este exame promediará co exame final si o alumno saca un mánimo de 4 puntos sobre 10. Si o alumno saca unha nota inferior a esta, deberá volver avaliarse desta parte no exame final.
  4. A planificación das diferentes probas de avaliación intermedia se aprobará nunha Comisión Academica de Grao (CAG) e estará dispoñible ao principio do cuadrimestre.
  5. Exame teorico final, na data acordada en Xunta de Escola. Habrá dous casos:

     - Alumnado que supere a nota minima do exame parcial. Neste exame entrarán os temas dados desde aproximadamente a metade do cuadrimestre até o final. Representará un 25% da nota total. Para poder superar a materia o alumno deberá obter neste exame unha nota minima de 4 puntos sobre 10.
     - Alumnado que non supere a nota minima do exame parcial. Neste exame entrarán todos os temas dados no curso teorico. Representara un 50% da nota total. Para poder superar a materia o alumno deberá obter neste exame unha nota minima de 4 puntos sobre 10, cun minimo de 4 puntos en cada unha das dúas partes do exame.

  Avaliación global. A avaliación global (AG) estará formada por:

  1. Un exame teorico final polo 75% da nota, que constará de dous partes e que se realizará o mesmo dia e hora que o de AC.
  2. As practicas de laboratorio B, que completara o outro 25%. Se entregarán en Moovi, con data tope o mesmo dia que a de AC.
  3. Para poder superar a materia o alumno debera obter no exame teorico un mínimo de 4,5 puntos sobre 10, en cada unha das dúas partes do exame. E un minimo de 1 punto sobre 2,5 nas practicas B.

  O exame final será o mesmo para todos os alumnos, tanto para os que opten por avaliación continua como para os que opten por avaliacion global.

- **OPORTUNIDADE EXTRAORDINARIA.**

Para o alumnado que opte durante o cuadrimestre por avaliación continua a nota total se obtendrá segun:

1. 50% de parte teorica, 25% de practicas B de laboratorio e 25% do traballo C.
2. Gardase, da oportunidade ordinaria, as notas do exame teorico parcial e final (sempre que superen a nota minima), da practica B de laboratorio (sempre que supere o minimo) e do traballo C.
3. Deberá presentarse ao exame teorico desta oportunidade todo o alumnado que non supere a nota minima teorica, nalgunha das dúas partes do exame, da oportunidade ordinaria. Con todo, só serÃ necesario realizar o exame da parte ou partes das que non se alcanzou ese minimo. Sera obrigatorio obter un minimo de 4 puntos sobre 10, en calquera das partes ás que se presente o alumno, para poder aprobar a materia.
4. O alumnado que non entregue a practica de laboratorio B na oportunidade ordinaria, e aqueles que non alcancen a nota minima desta parte, deberán realizar e entregar a mesma practica que a da oportunidade ordinaria. A data tope de entrega sera a do dia e hora do exame teorico. Sera obrigatorio obter nesta parte un mínimo de 1 punto sobre 2,5 para poder aprobar a materia.
5. Os alumnos que non entreguen o traballo C na oportunidade ordinaria, deberan realizar unha proba escrita que realizarase o mesmo dia do exame de teoria e da que se obtendrá o 25% da nota total. Por tanto, non se realizara ningunha entrega propiamente dita de traballo C.

Para o alumnado que opte na oportunidade ordinaria por avaliación global, realizarase un exame final cun valor do 75%, xunto co traballo B de laboratorio que representara o 25%. Se garda a nota do exame teorico da oportunidade ordinaria (sempre que supere o minimo de 4,5 puntos) e a do laboratorio B (sempre que supere o minimo de 1 sobre 2,5 puntos).

- **OUTRAS OBSERVACIÓNS.**
  - Considerarase a un alumno/a como "Non Presentado" si non seguiu a avaliación continua e non se presentou ao exame teorico final. Igualmente, si un alumno vai por AC e non se presenta a ningun exame (A,B e C) se lle considerará como "non presentado".
  - As cualificacións obtidas nas practicas B de laboratorio e traballo C soamente seran válidas durante o curso academico en que se realicen.
  - Si a nota total é igual ou superior a 5 pero non se alcanzou a nota mínima en algures, a nota final será 4.9 puntos (suspenso).
- **CONVOCATORIA DE FIN DE CARREIRA.**
  - A avaliación na convocatoria de fin de carreira estará formada por:
    - Exame teórico (50%). Exame individual dos contidos da materia representando o 50% da nota total. O alumnado deberá obter unha nota minima de 4 puntos (en cada unha das dúas partes do exame) sobre 10 para aprobar a materia.
    - Traballo B de laboratorio, representando un 25% da nota, e cun minimo de 1 punto sobre 2,5.
    - Proxecto C, representando un 25% da nota.

Bibliografía. Fontes de información

Bibliografía Básica

F. Fernandez Masaguer, **Apuntes de Seguridad en Redes y Sistemas de Informacion,**, 1ª ed., 2024

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

Bibliografía Complementaria

Joseph Migga Kizza,, **Guide to Computer Network Security**, 4ª Ed, Springer, 2015

M. Laurent Maknavicius, **Wireless and Mobile Network Security**, 1ª Ed, Wiley, 2014

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

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

Recomendacións

Materias que se recomenda cursar simultaneamente

Materias que se recomenda ter cursado previamente

Programación II/V05G301V01110