Guía Docente				
Datos Identificativos				2021/22
Asignatura (*)	Lexislación e Seguridade Informática		Código	614G01024
Titulación				
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Grao	1º cuadrimestre	Terceiro	Obrigatoria	6
Idioma	Castelán			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónDereito PrivadoDereito Público			
Coordinación	Santos Del Riego, Antonino		Correo electrónico	antonino.santos@udc.es
Profesorado	Carballal Mato, Adrián Crego Blanco, Jorge Fernández Lozano, Carlos Romero Cardalda, Juan Jesus Santos Del Riego, Antonino		Correo electrónico	adrian.carballal@udc.es jorge.crego@udc.es carlos.fernandez@udc.es juan.romero1@udc.es antonino.santos@udc.es
Web	psi-udc.blogspot.com/			

Descrición xeral	Na actualidade, as empresas, os gobernos e a sociedade en xeral demandan un maior número de expertos en seguridade informática. Un profesional das tecnoloxías da información e as comunicacións, tanto do ámbito dos sistemas como do desenvolvemento do software, sen uns bos fundamentos en seguridade, estará claramente devaluado. A nosa profesión non consiste unicamente na administración de sistemas e desenvolvemento de software e hardware. Noutras palabras, un programa ou sistema que simplemente funciona, sen considerar o factor seguridade, pode supor un gran perigo para unha organización. O apagar e acender unha máquina pode arranxar un problema, a análise das causas e a procura de solucións constitúe unha clara diferenza entre un bo e mal profesional. Na materia de Lexislación e Seguridade Informática proporciónase ao alumno uns fundamentos en seguridade da información, e con iso un valor engadido sobre outros "profesionais" do sector. En todo momento centrámonos naqueles aspectos de interese para o seu futuro profesional, tentado levar os contidos da materia cara aos temas e contornas de relevancia para o mundo empresarial. A nosa profesión céntrase en "facer", non unicamente en "saber facer", e se é posible en "facelo o mellor posible". E, que nos piden as empresas?, claramente profesionais que saiban o que hai que facer, que o fagan ben, no menor dos tempos e cun custo mínimo. Sen ningunha dúbida, "deseñar" e "construír" profesionais deste tipo, altamente produtivos, é unha tarefa moi complexa. Obxectivos.: - Adquirir os fundamentos en seguridade necesarios para proporcionar un valor engadido aos nosos futuros profesionais. - As ameazas que sofre a información durante o seu proceso, almacenamento e transmisión son crecentes, multiformes e complexas. Para contrarrestalas desenvolvéronse numerosas medidas de protección, que se implementan mediante os denominados mecanismos de seguridade. A lista destes mecanismos é xa moi numerosa e nela atópase, entre outros moitos: procesos de identificación e autenticación, control de accesos, control de fluxo de información, rexistros de auditoría, cifrado de información, etc. Ser consciente desta realidade, coas súas vantaxes e limitacións, proporcionará aos alumnos unha base para afrontar unha gran parte das implementaciones tecnolóxicas ás que se poidan enfrontar no seu futuro profesional. - Identificar os aspectos relacionados coa seguridade da información, tanto desde o punto de vista técnico como legal, proporcionando as habilidades necesarias para "saber o que hai que facer", "facelo o mellor posible", no menor tempo e cun custo mínimo. Neste contexto será fundamental a exposición e estudo de casos reais, reforzando no alumno a necesidade de utilizar en todo momento o "sentido común", afastando da toma de decisións os moitos perigos e factores que poden "contaminar", total ou parcialmente, moitos dos nosos desenvolvementos. - Analizar os aspectos prácticos da contorna legal no que se desenvolverá a futura actividade profesional dos nosos alumnos, con especial referencia ás súas obrigacións en materia de datos de carácter persoal e seguridade informática. - Un alumno que senta un gran entusiasmo polas tecnoloxías proporcionará ás nosas empresas uns maiores niveis de produtividade, e durante máis tempo. Reforzar esta calidade no alumno, e espertala nos que a poidan ter lixeiramente aletargada será un dos principais obxectivos da materia.

Plan de continxencia	1. Modificacións nos contidos Non se farán cambios. 2. Metodoloxías *Metodoloxías docentes que se manteñen Mantemos todas as metodoloxías en liña. *Metodoloxías docentes que se modifican 3. Mecanismos de atención personalizada ao alumnado Utilizaranse diferentes ferramentas .: Micorosft Teams.: para sesións maxistrais con gravación de vídeo, titorías e prácticas de laboratorio. Máquinas virtuais sobre plataforma ESXi .: para prácticas de laboratorio. Forms e moodle.: para probas de resposta múltiple e comunicacións varias. Correo electrónico.: para comunicacións varias. Blog da materia.: para comunicacións varias, xestións, novas, informes, etc. 4. Modificacións na avaliación Sen modificacións pasan a ser en liña. 5. Modificacións da bibliografía ou webgrafía A mesma e incorpórase ás sesións maxistrais dispoñibles en vídeo.

Competencias / Resultados do título	
Código	Competencias / Resultados do título

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Identificar os fundamentos da certificación dixital.	A58		C3
Definir os riscos e vulnerabilidades dun sistema de información.	A5 A7 A36 A47 A50 A58	B1 B6 B7	C3 C7

Identificar os mecanismos de seguridade e a súa integración nas organizacións.	A5 A7 A47 A50 A58	B1 B6 B7	C3 C7
Utilizar as ferramentas de seguridade.			C3
Organizar a seguridade dun sistema de información.	A5 A7 A36 A47 A50 A58	B1 B6 B7	C3 C7
Asumir responsabilidades sobre os sistemas de información e tomar decisións en canto á súa seguridade.	A5 A7 A36 A47 A50 A58	B4 B5 B6	C7
Aplicar o "sentido común" na toma de decisións, identificando os moitos perigos e factores que poden "contaminar", total ou parcialmente, moitos dos nosos desenvolvementos.		B6 B7	C6 C7
Enfrontarse a casos "reais" e "saber o que hai que facer", "facelo o mellor posible", no menor tempo e cun custo mínimo.	A5 A7 A36 A47 A50 A58	B1 B6 B7	C7
Evitar a proliferación de profesionais mediocres que, no peor dos casos, especialícense na destrución de todo o que tocan.		B1 B6 B7	C4 C5 C6 C7 C8
Coñecer a regulación legal da sociedade da información e da protección dos datos de carácter persoal, con especial atención á seguridade informática.	A7 A24 A47 A58		
Comportarse con ética e responsabilidade social como cidadán e profesional.			C4
Razoamento crítico, en especial en relación cos valores e os dereitos.	A7 A24 A47	B3 B6	C6
Capacidade para a análise e a síntese.		B1 B3 B5 B6	C6

Contidos	
Temas	**Subtemas**

Fundamentos e categorías de ataques.	- A triloxía ("host discovey", "port scanning", "fingerprinting") - Ocultación. - ?Sniffing?. - [D]DoS.
Seguridade a nivel físico.	
Monitorización e filtrado en seguridade da información.	
Certificados dixitais e autoridades de certificación.	
Auditorías de seguridade.	
A regulación xurídica da informática.	- Dereito. Elementos e conceptos xurídicos básicos. - Ética profesional e deontología. - Autorregulación. Códigos de conduta, códigos de práctica, códigos tipo.
A prestación de servizos e a tutela dos dereitos na sociedade da información.	- A prestación de servizos na sociedade da información. Servizos de intermediación. Servizos de certificación. - A contratación electrónica e a contratación informática. - As comunicacións comerciais electrónicas. - A firma electrónica. - A administración electrónica. - A resolución xudicial de conflitos. - As solucións extraxudiciais. A autorregulación. A arbitraxe electrónica.
A protección dos datos de carácter persoal.	- Introdución e delimitacións conceptuais. - Constitución, dereitos fundamentais e protección de datos. - A lexislación española de protección de datos de carácter persoal. Disposicións xerais. Principios. Suxeitos. Dereitos. Obrigacións. Medidas de seguridade. Procedementos. - Autorregulación e protección de datos persoais. - Criminalidade informática e datos persoais.
Temario Prácticas.	- Seguridade (fundamentos e configuracións básicas). - Categorías de ataques e identificación de recursos. - Autoridades de certificación - Auditorías de seguridade.

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Prácticas de laboratorio	A5 A7 A24 A36 A47 A50 A58 B1 B3 B4 B5 B6 B7 C3 C4 C5 C6 C7 C8	28	42	70
Proba de resposta múltiple	A5 A24 A36 A47 A50 A58 B5 B6	0.5	0	0.5
Sesión maxistral	A5 A7 A24 A36 A47 A50 A58 B1 B3 B4 B5 B6 B7 C3 C4 C5 C6 C7 C8	27	40.5	67.5
Análise de fontes documentais	A5 A7 A24 A36 A47 A50 A58 B1 B3 B4 B5 B6 B7 C3 C6 C8	3	3.6	6.6

Estudo de casos	A5 A7 A24 A36 A47 A50 A58 B1 B3 B4 B5 B6 B7 C3 C6	2	2.4	4.4
Atención personalizada		1	0	1
***Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado**				

Metodoloxías	
Metodoloxías	**Descrición**
Prácticas de laboratorio	As prácticas de laboratorio permiten sacar o máximo proveito na retroalimentación, reforzo e asimilación dos obxectivos. Os desenvolvementos prácticos iníciansе cunha práctica básica, e elévase a súa dificultade paulatinamente. En todo momento preséntase ao alumno o conxunto de ideas e técnicas que permiten o desenvolvemento práctico dos coñecementos transmitidos nas sesións maxistrais. Nas prácticas proponse diversos apartados que expoñen unha batería de dificultades tratadas durante o estudo do tema. Buscarase a interrelación entre os distintos apartados, achegando un contexto de exercicio completo, para lograr no alumno unha visión de conxunto, revelando os nexos existentes entre cuestións que poderían parecer afastadas. En todas as clases prácticas utilízanse máquinas virtuais sobre computadoras como ferramenta básica para a resolución dos exercicios. O alumno poderá seleccionar e instalar aquelas ferramentas que considere máis oportunas en cada caso. Desta forma, requiriráselle, desde un primeiro momento, que se enfronte a toma de decisións, analizando as vantaxes e desvantaxes en todos e cada un dos casos. Neste punto inicial, será fundamental un asesoramento personalizado, que permita unha análise realista sobre as decisións tomadas, facilitando a retroalimentación de novos parámetros non considerados a priori.
Proba de resposta múltiple	Esta proba estará orientada a determinar se o alumno asimilou os distintos obxectivos da materia.
Sesión maxistral	Transmisión de información e coñecementos crave de cada un dos temas. Poténciase en certos momentos a participación do alumno. Como parte da metodoloxía, un enfoque crítico da disciplina levará aos alumnos a reflexionar e descubrir as relacións entre os diversos conceptos, formar unha mentalidade crítica para afrontar os problemas e a existencia dun método, facilitando o proceso de aprendizaxe no alumno. Tamén será fundamental a transmisión dos conceptos e coñecementos éticos e xurídicos básicos en seguridade da información. A súa singularidade fai que se dedique certo tempo á exposición da linguaxe específica que soporta os conceptos, e que serve de principal medio de comunicación e argumentación ética e xurídica. Isto permitirá ao alumno comprender a linguaxe e os conceptos que integran os aspectos éticos e xurídicos da informática. Para loitar contra a posible pasividade do alumno, en certos momentos exponse pequenas cuestións, que fagan reflexionar ao alumno, complementando devanditos aspectos con referencias bibliográficas que lle permitan enriquecer o coñecemento adquirido. Este intercambio co alumno, como parte da lección maxistral, permítenos controlar o grao de asimilación dos coñecementos por parte do mesmo. As leccións maxistrais inclúen, tanto coñecementos extraídos das referencias da asginatura, como os resultantes de nosas propias experiencias profesionais, fomentando a capacidade de análise crítica. En todo momento búscase que certa parte dos contidos achegados non requiran do alumno unha tarefa de memorización. Esta metodoloxía tratará de conseguir un alto grao de motivación no alumno.
Análise de fontes documentais	Lectura e exame crítico dos principais documentos éticos e xurídicos da informática. Serven de introdución xeral aos temas. Proporcionan unha explicación histórica e sistemática do seu significado. Son de gran impotancia no contexto do resto de metologías utilizadas na materia.
Estudo de casos	A análise ética e xurídica da informática ten unhas características específicas. Co estudo de casos preténdese examinar a estrutura e os contidos dos problemas presentes nos casos, tanto de maneira individual como en grupo. É unha forma de aprendizaxe de contidos e tamén metodolóxica, na que o estudante aprende a analizar, deliberar e chegar a conclusións fundamentadas e razoables cos argumentos éticos e xurídicos. Resulta de gran utilidade para exercitar as destrezas e habilidades argumentativas.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas de laboratorio	Prácticas de laboratorio.: Se guía ao alumno de forma individualizada no desenvolvemento de cada unha das prácticas de laboratorio. Aínda que no desenvolvemento da primeira práctica existen grandes diferenzas nas necesidades de cada alumno, progresivamente vanse homoxeneizando en canto ás súas necesidades de atención personalizada. Sen ningunha dúbida, a identificación deste parámetro é fundamental para determinar que a totalidade dos alumnos progresa durante o desenvolvemento da materia. Tamén faremos pequenos grupos de traballo conxunto en desenvolvementos prácticos. Atención personalizada.: Toda cuestión tecnolóxica exposta polo alumno, en persoa, tutorías, email., etc.

Avaliación			
Metodoloxías	**Competencias / Resultados**	**Descrición**	**Cualificación**
Prácticas de laboratorio	A5 A7 A24 A36 A47 A50 A58 B1 B3 B4 B5 B6 B7 C3 C4 C5 C6 C7 C8	Cada alumno de prácticas de laboratorio, e tras considerar que superou cada práctica, sempre antes do prazo establecido para cada práctica, deberá pasar unha proba oral. Nela o profesor expón pequenas probas que os alumnos deberán resolver sobre as máquinas virtuais do laboratorio de prácticas, defendendo os seus desenvolvementos de forma oral. Durante o curso informaranse dos prazos para a defensa das prácticas.	40
Sesión maxistral	A5 A7 A24 A36 A47 A50 A58 B1 B3 B4 B5 B6 B7 C3 C4 C5 C6 C7 C8	Para loitar contra a posible pasividade do alumno, en certos momentos das sesións maxistrais exponse pequenas cuestións, que fagan reflexionar ao alumno. Este intercambio co alumno, como parte da lección maxistral, permítenos controlar o grao de asimilación dos coñecementos por parte do mesmo. Para potenciar a participación do alumno estás cuestións teñen asignado unha pequena puntuación, segundo o grao de dificultade (puntuación complementaria fóra de guía).	0
Proba de resposta múltiple	A5 A24 A36 A47 A50 A58 B5 B6	Esta proba inclúe os contidos e, en xeral, todo aspecto relacionado cos obxectivos da materia. Nela exponse diversas cuestións relacionadas tanto cos contidos das sesións maxistrais como das prácticas de laboratorio, dándolle un maior peso ás primeiras.	60
Outros			

Observacións avaliación
Para aprobar a materia será necesario ter superadas as prácticas de laboratorio. Sen as prácticas de laboratorio superadas a cualificación da proba de resposta múltiple dividirase por dúas. Durante o curso informaranse dos prazos para a defensa das prácticas.Todos os alumnos, incluídos os de tempo parcial, terán que defender en persoa cada práctica nas datas e lugar establecidos. Na convocatoria de xullo, na súa falta, á proba de resposta múltiple engadiráselle unha proba da parte práctica, que deberá ser superada por separado.

Fontes de información

Bibliografía básica	- A. Santos del Riego (). Legislación [Protección] y Seguridad de la Información. http://psi-udc.blogspot.com - debian.org (). Debian. http://www.debian.org/ - yolinux (). yolinux. http://www.yolinux.com/ - Packet Storm (). Packet Storm. http://packetstormsecurity.org/ - (). Criptored. http://www.criptored.upm.es/ - Miguel PEGUERA POCH (coord.) (2010). Principio de Derecho de la sociedad de la información. Cizur Menor: Aranzadi - José APARICIO SALOM (2009). Estudio sobre la Ley Orgánica de protección de datos de carácter personal. Pamplona: Aranzadi - Lorenzo COTINO, Julián VLAERO (coords.) (2010). Administración electrónica. Valencia: Tirant lo Blanch - José Luis PIÑAR MAÑAS (dir.) (2011). electrónica y ciudadanos. Madrid: Civitas - Manuel CASTELLS (2009). Comunicación y poder. Madrid: Alianza - Miguel Ángel DAVARA RODRÍGUEZ (2008). Manual de Derecho informático. Pamplona: Aranzadi - Antonio TRONCOSO (2010). La protección de datos personales. En busca del equilibrio. Valencia: Tirant lo Blanch - Gonzalo F. GÁLLEGO HIGUERAS (2010). Código de Derecho informático y de las nuevas tecnologías. Madrid: Civitas - Javier ORDUÑA, Gonzalo AGUILERA (dir.) (2009). Comercio, Administración y Registros electrónicos. Madrid: Civitas - Willian Stallings (2014). Network Security Essentials. Applications and Standards. Prentice Hall
Bibliografía complementaria	- (). Security Focus. http://www.securityfocus.com/ - (). Common Vulnerabilities and Exposures (CVE). http://www.cve.mitre.org/ - (). NIST Computer Security Division. http://csrc.nist.gov/ - (). CERT:Computer Emergence Response Team. http://www.cert.org - (). AntiOnline. http://www.antionline.com/ - (). Delitos Informáticos. http://www.delitosinformaticos.com/ - (). (in)secure magazine. http://www.net-security.org/insecure-archive.php - (). Linux Journal. http://www.linuxjournal.com/ - (). Security art work. http://www.securityartwork.com/ - (). Security by default. http://www.securitybydefault.com/ - Pekka HIMANEN (2002). La ética del hacker y el espíritu de la era de la información. Barcelona, Destino - Lawrence LESSIG (2001). El código y otras leyes del ciberespacio. Madrid, Taurus - Justo GÓMEZ NAVAJAS (2005). La protección de los datos personales. Cizur Menor, Thomson Civitas - Fernando MIRÓ LLINARES (2005). Internet y delitos contra la propiedad intelectual. Valencia: Tirant lo Blanch - Antoni FARRIOLS I SOLA (2006). La protección de datos de carácter personal en los centros de trabajo. Madrid: Cinca - Pedro DE MIGUEL ASENSIO (2011). Derecho privado de internet. Madrid: Civitas - Esther MORÓN LERMA (2002). Internet y Derecho penal. Pamplona: Aranzadi

Recomendacións
Materias que se recomenda ter cursado previamente
Sistemas Operativos/614G01016 Redes/614G01017
Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Seguridade nos sistemas Informáticos/614G01079 Seguridade nos Sistemas Informáticos/614G01214
Observacións

UNIVERSIDADE DA CORUÑA

(*)A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías