| Guía Docente | | | | | |
|---|---|---|---|---|---|
| Datos Identificativos | | | | | 2020/21 |
| Asignatura (*) | Seguridade nos sistemas Informáticos | | | Código | 614G01079 |
| Titulación | Grao en Enxeñaría Informática | | | | |
| Descriptores | | | | | |
| Ciclo | Período | Curso | | Tipo | Créditos |
| Grao | 1º cuadrimestre | Cuarto | | Optativa | 6 |
| Idioma | Castelán | | | | |
| Modalidade docente | Híbrida | | | | |
| Prerrequisitos | | | | | |
| Departamento | Ciencias da Computación e Tecnoloxías da InformaciónComputación | | | | |
| Coordinación | Vázquez Naya, José Manuel | | Correo electrónico | jose.manuel.vazquez.naya@udc.es | |
| Profesorado | Vázquez Naya, José Manuel | | Correo electrónico | jose.manuel.vazquez.naya@udc.es | |
| Web | moodle.udc.es | | | | |
| Descrición xeral | A seguridade nos sistemas de información é crucial en todos e cada un dos servizos ofertados pola denominada sociedade da información. Posto que cada vez máis información está accesible, cada vez requírense controis de seguridade máis estritos. O avance tecnolóxico neste caso funciona de catalizador en ambas as direccións: por unha banda favorece o acceso a novos tipos e a maior cantidade de información (o que require un aumento dos controis de seguridade) e doutra banda posibilita a implantación de mecanismos de seguridade máis refinados (que posibilitan o acceso seguro a novos tipos de información).<br><br>A materia está exposta para proporcionar ao alumno o coñecemento necesario dos conceptos básicos e técnicas empregadas para a protección dos sistemas de información, desde o punto de vista físico, lóxico e administrativo. Estes conceptos básicos incluirán, como paso de inicio, a evolución dos diferentes métodos e algoritmos de cifrado. Debido ao enorme auxe dos diversos medios electrónicos de intercambio de información (correo electrónico, páxinas web, e-commerce, firma dixital, etc.), un aspecto fundamental cando se traballa neste ámbito será ter a formación suficiente na seguridade deste tipo de sistemas. Para o correcto funcionamento dos servizos referidos esíxese a existencia dunha infraestrutura (redes de comunicacións e sistemas operativos) que funcione de modo seguro e fiable. Por tanto será preciso coñecer os aspectos fundamentais dos compoñentes, protocolos de funcionamento, configuración, etc. da devandita infraestrutura. Este coñecemento será o que lle permita ao alumno entender e solucionar os riscos actuais, e os que inevitablemente xurdirán no futuro, que afectan a todo sistema de información. | | | | | |

| | |
|---|---|
| Plan de continxencia | 1. Modificacións nos contidos<br>- Non se realizarán cambios<br><br>2. Metodoloxías<br>*Metodoloxías docentes que se manteñen<br>- Mantéñense as metodoloxías docentes, coa excepción de que en lugar de realizarse de maneira presencial na aula, realizaranse coa axuda de ferramentas TIC, como se explica a continuación.<br><br>*Metodoloxías docentes que se modifican<br>- Sesión maxistral: impartirase a través de videoconferencia.<br>- Prácticas de laboratorio: Tanto a docencia, coma a defensa das prácticas, cando proceda, realizaranse a través de videoconferencia.<br>- Proba obxectiva: realizarase a través de Moodle, en combinación con videoconferencia.<br>- Exame de prácticas (segunda oportunidade e convocatoria extraordinaria): realizarase a través de videoconferencia.<br><br>3. Mecanismos de atención personalizada ao alumnado<br>- Correo electrónico: Diariamente. De uso para facer consultas, e solicitar encontros virtuais para resolver dúbidas.<br>- Moodle: Diariamente. Segundo a necesidade do alumnado.<br>- Teams: Durante as horas programadas de teoría e práctica. Tamén baixo demanda, para resolución de dúbidas.<br><br>4. Modificacións na avaliación<br>- Non se realizarán cambios<br><br>*Observacións de avaliación:<br>Mantéñense as mesmas que figuran na guía docente. A maiores:<br><br>- No caso de que non poidan realizarse presencialmente, levaranse a cabo segundo o indicado no apartado de "Metodoloxías".<br><br>- Se por algún motivo xustificado o alumno non puidese realizar o exame final (proba obxectiva) no momento establecido, o exame pasará a realizarse a maior brevidade posible, pasando a ser unha proba oral por videoconferencia.<br><br>5. Modificacións da bibliografía ou webgrafía<br>Ningunha. |

| Competencias / Resultados do título | |
|---|---|
| Código | Competencias / Resultados do título |
| A58 | Capacidade para comprender, aplicar e xestionar a garantía e seguranza dos sistemas informáticos. |
| B1 | Capacidade de resolución de problemas |
| B3 | Capacidade de análise e síntese |
| C3 | Utilizar as ferramentas básicas das tecnoloxías da información e as comunicacións (TIC) necesarias para o exercicio da súa profesión e para a aprendizaxe ao longo da súa vida. |
| C6 | Valorar criticamente o coñecemento, a tecnoloxía e a información dispoñible para resolver os problemas cos que deben enfrontarse. |

| Resultados da aprendizaxe |
|---|

| Resultados de aprendizaxe | Competencias / Resultados do título | | |
|---|---|---|---|
| Identificar os fundamentos dos criptosistemas e identificar os mecanismos de seguridade así como a súa integración nas organizacións | A58 | B3 | C3<br>C6 |
| Definir os riscos e vulnerabilidades dun sistema de información e a súa aplicación en contornas reais. | A58 | B1 | C3<br>C6 |
| Utilizar ferramentas de seguridade. | A58 | B1 | C3 |
| Organizar a seguridade dun sistema de información. | A58 | B1 | C3<br>C6 |
| Expresar de forma clara e efectiva a necesidade, implantación, vantaxes e desvantaxes das medidas de seguridade. | A58 | B3 | C3<br>C6 |

| Contidos | |
|---|---|
| Temas | Subtemas |
| Criptoloxía | Sistemas criptográficos clásicos<br>Sistemas criptográficos de clave secreta<br>Sistemas criptográficos de clave pública<br>Firma dixital<br>Esteganografía |
| Seguridade no correo electrónico | PGP<br>GPG<br>S/MIME |
| Sistemas de Xestión de Seguridade da Información | Normativas de Seguridade<br>Estándares de Xestión da Seguridade da Información<br>Normas ISO / IEC 27000<br>Implantación de un SGSI |
| Análise de Riscos e Medidas de Seguridade | Análise de Riscos<br>Xestión do Risco<br>Medidas de Seguridade |
| Malware | Virus<br>"Trojans"<br>"Rootkits"<br>"Exploits" |
| Análise Forense | Fases da Análise Forense<br>Ferramentas HW e SW |
| Estudo de casos | Estudo de casos reais de ataques a sistemas de información |
| Prácticas | Proba de distintas ferramentas de seguridade, relacionadas cos temas de teoría |

| Planificación | | | | |
|---|---|---|---|---|
| Metodoloxías / probas | Competencias / Resultados | Horas lectivas (presenciais e virtuais) | Horas traballo autónomo | Horas totais |
| Sesión maxistral | B3 | 16 | 32 | 48 |
| Prácticas de laboratorio | A58 B1 C3 C6 | 18 | 36 | 54 |
| Traballos tutelados | A58 B3 C3 C6 | 10 | 30 | 40 |
| Proba obxectiva | A58 B1 | 1 | 0 | 1 |
| Atención personalizada | | 7 | 0 | 7 |
| *Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado | | | | |

| Metodoloxías |
|---|

| Metodoloxías | Descrición |
|---|---|
| Sesión maxistral | Clases expositivas de presentación dos coñecementos teóricos de cada un dos temas.<br><br>O material utilizado nestas clases estará dispoñible na plataforma de formación da Universidade da Coruña. |
| Prácticas de laboratorio | Sesións prácticas en computador, nas que se deben resolver unha serie de boletíns de exercicios prácticos propostos polo profesor. Os exercicios buscan consolidar os coñecementos presentados nas sesións maxistrais e tamén fomentar a aprendizaxe autónoma do alumno. Na resolución dos exercicios, utilizaranse distintas ferramentas de seguridade, co obxectivo de que o alumno as coñeza e adquira destreza no seu uso.<br><br>Algúns exercicios teñen carácter individual, mentres que outros serán realizados en grupo.<br><br>Os boletíns de exercicios publicaranse a través da plataforma de formación da Universidade da Coruña. |
| Traballos tutelados | Traballos académicos relativos ao contido da materia, que se realizan en grupos pequenos. O profesor proporá unha listaxe de temas, relacionados co temario da materia. Os alumnos deberán escoller un tema e acordar a estrutura do traballo co profesor. Finalmente, os alumnos deben realizar unha presentación na clase do traballo realizado.<br><br>O obxectivo dos traballos é que o alumno profunde nun tema do seu interese. |
| Proba obxectiva | Proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno. |

| Atención personalizada | |
|---|---|
| Metodoloxías | Descrición |
| Traballos tutelados<br>Prácticas de laboratorio | Seguimento das prácticas de laboratorio e dos traballos tutelados.<br>Seguimento da actividade do/a estudante ó longo do curso. |

| Avaliación | | | |
|---|---|---|---|
| Metodoloxías | Competencias / Resultados | Descrición | **Cualificación** |
| Proba obxectiva | A58 B1 | Ao finalizar o cuadrimestre, realizarase unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno. | 40 |
| Traballos tutelados | A58 B3 C3 C6 | Realización do traballo tutelado e a súa presentación en clase.<br><br>Criterios avaliación: dificultade da temática, traballo de procura e selección de material relevante, calidade e cantidade das fontes de información seleccionadas, capacidade de síntese, existencia de compoñente práctica ou realización de probas, calidade da memoria e calidade da presentación. | 30 |
| Prácticas de laboratorio | A58 B1 C3 C6 | No enunciado de cada práctica especificarase a data límite para a realización da mesma, así como a metodoloxía de avaliación, que pode ser a través da entrega dunha memoria, da realización dunha proba en ordenador, ou mediante ambas. | 30 |
| Outros | | | |

| Observacións avaliación |
|---|

1. PRIMEIRA OPORTUNIDADE

Ó longo do curso realizaranse unha serie de "prácticas de laboratorio" e un "traballo tutelado", coas características e peso indicados no cadro anterior.

Ó finalizar o curso realizarase unha "proba obxectiva", coas características e peso indicados no cadro anterior.

2. SEGUNDA OPORTUNIDADE E OPORTUNIDADE ADIANTADA

Realizarase unha "proba obxectiva", coas características e peso indicados no cadro anterior.

As notas de "prácticas de laboratorio", e do "traballo tutelado" obtidas na primeira oportunidade, consérvase para o resto de oportunidades dese curso.

Caso de non ter nota nalgún destes apartados, e querer optar a ela, o alumno debe contactar co coordinador da materia cunha antelación mínima de 30 días naturais antes da data do exame.

A nota de "prácticas de laboratorio" poderá recuperarse mediante a realización e defensa das prácticas que se determinen para a segunda oportunidade (ou oportunidade adiantada de decembro, segundo corresponda).

A nota do "traballo tutelado" poderá recuperarse mediante a realización e defensa dun traballo tutelado individual, cuxa temática debe ser acordada co coordinador da materia.

3. CONDICIÓN DE "NON PRESENTADO"

Consideraranse como "non presentados" aos alumnos que non realicen a proba obxectiva.

4. ALUMNOS A TEMPO PARCIAL

Alumnado con recoñecemento de dedicación a tempo parcial.

Os alumnos que cursen a materia a tempo parcial deben realizar as mesmas probas de avaliación que os alumnos que as cursen a tempo completo, coas seguintes consideracións:

- En canto á defensa das prácticas, se o alumno non puidese asistir á defensa no horario de prácticas, convirase con el un horario alternativo.
- En canto á realización do traballo tutelado, exímese ao alumno da necesidade de realizar o traballo en grupo, podendo realizalo individualmente, e, en caso de non poder presentar o traballo en clase por incompatibilidade no horario, o alumno poderá realizar a presentación ao profesor no horario convido por ambos.

O alumno deberá notificar ao coordinador da materia a súa condición de estudante a tempo parcial tan pronto como lle sexa recoñecida, para que o profesor poida realizar unha correcta planificación das actividades docentes.

| Fontes de información | |
|---|---|
| Bibliografía básica | - Jorge Ramió (1999). Aplicaciones Criptográficas. UPM<br>- M. Mackrill, C. Nowell, K. Stopford, C. Trautwein (2011). Official ISC2 Guide to the SSCP CBK. 2ª Edición. Ed. Harold F. Tripton<br>- S. Harris (2010). CISSP All in one. 5ª Edición. Mc-Graw Hill<br>- W. Stallings (2004). Fundamentos de Seguridad en Redes. Aplicaciones y Estándares. 2ª Edición. Pearson Educación |
| Bibliografía complementaria | - Manuel J. Lucena (). Critpografía y seguridad en Computadores. http://wwwdi.ujaen.es/~mlucena<br>- Information Security Forum (). The Standard of good Practice for Information Security. http://www.isfsecuritystandard.com<br>- Simson Garfinkel, Gene Spafford, Alan Schwartz (2003). Practical UNIX and Internet Security, Third Edition. O'Reilly |

| Recomendacións |
|---|
| Materias que se recomenda ter cursado previamente |
| Lexislación e Seguridade Informática/614G01024<br>Administración de Sistemas Operativos/614G01047<br>Administración de Redes/614G01048<br>Administración de Bases de Datos/614G01050 |
| Materias que se recomenda cursar simultaneamente |
| |
| Materias que continúan o temario |
| |

| Observacións |
| --- |
| |

(*)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