



Teaching Guide

| Identifying Data | | | | | 2024/25 |
|---------------------|---|--------|---|---------|---------|
| Subject (*) | Computer Systems Security | Code | 614G01079 | | |
| Study programme | Grao en Enxeñaría Informática | | | | |
| Descriptors | | | | | |
| Cycle | Period | Year | Type | Credits | |
| Graduate | 1st four-month period | Fourth | Optional | 6 | |
| Language | Spanish | | | | |
| Teaching method | Face-to-face | | | | |
| Prerequisites | | | | | |
| Department | Ciencias da Computación e Tecnoloxías da InformaciónComputación | | | | |
| Coordinador | Vázquez Naya, José Manuel | E-mail | jose.manuel.vazquez.naya@udc.es | | |
| Lecturers | Pérez Jove, Rubén Rivera Dourado, Martiño Vázquez Naya, José Manuel | E-mail | ruben.perez.jove@udc.es martino.rivera.dourado@udc.es jose.manuel.vazquez.naya@udc.es | | |
| Web | https://campusvirtual.udc.gal | | | | |
| General description | <p>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 requirense 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).</p> <p>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 incluírán, 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.</p> | | | | |

Study programme competences / results

| Code | Study programme competences / results |
|------|---|
| 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. |

Learning outcomes

| Learning outcomes | Study programme competences / results | | |
|--|---------------------------------------|----|----------|
| Identificar os fundamentos dos criptosistemas e identificar os mecanismos de seguridade así como a súa integración nas organizacións | A58 | B3 | C3 C6 |



| | | | |
|--|-----|----|----------|
| Definir os riscos e vulnerabilidades dun sistema de información e a súa aplicación en contornas reais. | A58 | B1 | C3 C6 |
| Utilizar ferramentas de seguridade. | A58 | B1 | C3 |
| Organizar a seguridade dun sistema de información. | A58 | B1 | C3 C6 |
| Expresar de forma clara e efectiva a necesidade, implantación, vantaxes e desvantaxes das medidas de seguridade. | A58 | B3 | C3 C6 |

| Contents | |
|---|--|
| Topic | Sub-topic |
| Cryptography | Sistemas criptográficos de clave secreta - Cifradores de bloque - Cifradores de flujo Sistemas criptográficos de clave pública Técnicas de criptoanálise Esteganografía Funcións hash Firma dixital Certificados dixitais Autoridades de certificación Tarxetas intelixentes |
| Email security | PGP - GPG S/MIME |
| Information Security Management System (ISMS) | Estándares de Xestión da Seguridade da Información Normas ISO / IEC 27000 Implantación de un SGSI |
| Malware | Virus "Trojans" "Rootkits" "Exploits" |
| Forensic Analysis | Fases da Análise Forense Ferramentas HW e SW |
| Case studies | Estudo de casos reais de ataques a sistemas de información |
| Practices | Proba de distintas ferramentas de seguridade, relacionadas cos temas de teoría |

| Planning | | | | |
|--------------------------------|------------------------|--------------------------------------|-------------------------------|-------------|
| Methodologies / tests | Competencies / Results | Teaching hours (in-person & virtual) | Student?s personal work hours | Total hours |
| Guest lecture / keynote speech | B3 | 21 | 42 | 63 |
| Laboratory practice | A58 B1 C3 C6 | 15 | 30 | 45 |
| Supervised projects | A58 B3 C3 C6 | 6 | 24 | 30 |
| Objective test | A58 B1 | 1 | 0 | 1 |
| Personalized attention | | 11 | 0 | 11 |

(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

| Methodologies | |
|---------------|-------------|
| Methodologies | Description |
| | |



| | |
|--------------------------------|--|
| Guest lecture / keynote speech | <p>Clases expositivas de presentación dos coñecementos teóricos de cada un dos temas.</p> <p>O material utilizado nestas clases estará dispoñible na plataforma de formación da Universidade da Coruña.</p> |
| Laboratory practice | <p>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.</p> <p>Algúns exercicios teñen carácter individual, mentres que outros serán realizados en grupo.</p> <p>Os boletíns de exercicios publicaranse a través da plataforma de formación da Universidade da Coruña.</p> |
| Supervised projects | <p>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.</p> <p>O obxectivo dos traballos é que o alumno profunde nun tema do seu interese.</p> |
| Objective test | <p>Proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno.</p> |

Personalized attention

| Methodologies | Description |
|--|---|
| Supervised projects Laboratory practice Guest lecture / keynote speech | <p>Na realización das prácticas de laboratorio e dos traballos tutelados, realizarase un "Seguimento continuado" ou "Atención personalizada". De xeito que, para obter a máxima nota, será necesario participar de maneira activa durante o desenvolvemento dos mesmos.</p> <p>Tamén na "Sesión Maxistral" realizarase un "Seguimento continuado" ou "Atención personalizada". Exporanse preguntas e retos. Fomentarase o debate na clase. Valorarase a participación activa.</p> |

Assessment

| Methodologies | Competencies / Results | Description | Qualification |
|---------------------|------------------------|--|---------------|
| Objective test | A58 B1 | Ao finalizar o cuadrimestre, realizarase unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno. | 50 |
| Supervised projects | A58 B3 C3 C6 | <p>Realización do traballo tutelado e a súa presentación en clase.</p> <p>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.</p> <p>Realizarase un "Seguimento continuado" ou "Atención personalizada". De xeito que, para obter a máxima nota, será necesario participar de maneira activa durante o desenvolvemento dos traballos tutelados.</p> | 20 |
| Laboratory practice | A58 B1 C3 C6 | <p>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.</p> <p>Realizarase un "Seguimento continuado" ou "Atención personalizada". De xeito que, para obter a máxima nota, será necesario participar de maneira activa durante o desenvolvemento das prácticas.</p> | 30 |



| | | | |
|--------|--|--|--|
| Others | | | |
|--------|--|--|--|

Assessment comments

Será necesario obter como mínimo o 50% da nota para aprobar a materia. Ademais, para aprobar a materia será preciso (en calquera oportunidade) obter un mínimo dun 45% da nota na proba obxectiva. En caso contrario, a nota máxima que se poderá obter é de 4.5.

A nota da proba obxectiva NON se conserva en ningunha convocatoria. A nota de "prácticas de laboratorio" e de "traballos tutelados" consérvase para o resto de oportunidades do curso académico.

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.

A nota de "prácticas de laboratorio" poderá recuperarse mediante a realización das prácticas que se determinen para a segunda oportunidade (ou oportunidade adiantada). A presentación das prácticas na convocatoria de segunda oportunidade (ou oportunidade adiantada) implica a renuncia á nota obtida previamente, se a houbese.

A nota do "traballo tutelado" poderá recuperarse mediante a realización dun novo traballo, cuxa temática debe ser acordada co coordinador da materia. A presentación do traballo tutelado na convocatoria de segunda oportunidade (ou oportunidade adiantada) implica a renuncia á nota obtida na primeira oportunidade, se a houbese.

Caso de querer recuperar a nota de prácticas de laboratorio ou do traballo tutelado na convocatoria de segunda oportunidade (ou oportunidade adiantada), o alumnado deberá contactar co coordinador da materia, cunha antelación mínima de 20 días naturais antes da data do exame da correspondente convocatoria.

3. CONDICIÓN DE "NON PRESENTADO"

Considerarase como "non presentado" ao alumnado que non se presente a ningunha das actividades avaliadas nunha convocatoria dada.

4. ALUMNADO A TEMPO PARCIAL OU CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA

O alumnado que curse a materia a tempo parcial ou con dispensa académica de exención de docencia debe realizar as mesmas probas de avaliación que o alumnado que a curse a tempo completo, coas seguintes consideracións:

- En canto á realización das prácticas, poderá realizalas de xeito individual. No caso de que non puidese asistir á defensa no horario de prácticas, convirase un horario alternativo.

- En canto á realización do traballo tutelado, poderá realizalo de xeito individual. No caso de que non puidese asistir á presentación do mesmo no horario de prácticas, convirase un horario alternativo.

O alumnado deberá notificar ao coordinador da materia a súa condición de estudante a tempo parcial ou con dispensa académica de exención de docencia tan pronto como lle sexa recoñecida, para que este poida realizar unha correcta planificación das actividades docentes.

5. COPIA E/OU PLAXIO

A realización fraudulenta das probas ou actividades de avaliación, unha vez comprobada, implicará directamente a cualificación de suspenso na convocatoria en que se cometa: o/a estudante será cualificado con "suspenso" (nota numérica 0) na convocatoria correspondente do curso académico, tanto se a comisión da falta se produce na primeira oportunidade como na segunda. Para isto, procederase a modificar a súa cualificación na acta de primeira oportunidade, se fose necesario.

Sources of information

| | |
|--------------|--|
| Basic | <ul style="list-style-type: none">- Stallings, W. (2011). <i>Cryptography and Network Security: Principles and Practice</i> (Fifth ed.). Prentice Hall- Jorge Ramió (1999). <i>Aplicaciones Criptográficas</i>. UPM- M. Mackrill, C. Nowell, K. Stopford, C. Trautwein (2011). <i>Official ISC2 Guide to the SSCP CBK</i>. 2ª Edición. Ed. Harold F. Tripton- S. Harris (2010). <i>CISSP All in one</i>. 5ª Edición. Mc-Graw Hill |
|--------------|--|



| | |
|----------------------|--|
| Complementary | <ul style="list-style-type: none">- Schneier, B. (2007). Applied cryptography: protocols, algorithms, and source code in C. Wiley-India- Simson Garfinkel, Gene Spafford, Alan Schwartz (2003). Practical UNIX and Internet Security, Third Edition. O'Reilly- Manuel J. Lucena (). Critpografía y seguridad en Computadores. http://wwwdi.ujaen.es/~mlucena- Information Security Forum (). The Standard of good Practice for Information Security. http://www.isfsecuritystandard.com |
|----------------------|--|

Recommendations

Subjects that it is recommended to have taken before

Computer Security and Legislation/614G01024
Operating Systems Administration/614G01047
Network Administration/614G01048
Database Administration/614G01050

Subjects that are recommended to be taken simultaneously

Subjects that continue the syllabus

Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.