



| Guía Docente | | | | |
|-----------------------|--|--------------------|-----------------------|----------|
| Datos Identificativos | | | | 2019/20 |
| Asignatura (*) | Seguridade Ubicua | Código | 614530013 | |
| Titulación | Máster Universitario en Ciberseguridade | | | |
| Descritores | | | | |
| Ciclo | Período | Curso | Tipo | Créditos |
| Mestrado Oficial | 2º cuatrimestre | Primeiro | Optativa | 3 |
| Idioma | CastelánGalego | | | |
| Modalidade docente | Presencial | | | |
| Prerrequisitos | | | | |
| Departamento | Ciencias da Computación e Tecnoloxías da Información | | | |
| Coordinación | Rabuñal Dopico, Juan Ramon | Correo electrónico | juan.rabunal@udc.es | |
| Profesorado | Martinez Perez, Maria | Correo electrónico | maria.martinez@udc.es | |
| | Rabuñal Dopico, Juan Ramon | | juan.rabunal@udc.es | |
| | Rodríguez Tajés, Álvaro | | a.tajes@udc.es | |
| Web | faitic.uvigo.es | | | |
| Descrición xeral | Coordinada pola Universidade de Vigo. Consultade a guía en: https://secretaria.uvigo.gal/docnet-nuevo/guia_docent/?centre=305 | | | |

| Competencias / Resultados do título | |
|-------------------------------------|---|
| Código | Competencias / Resultados do título |
| A4 | CE4 - Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información |
| A9 | CE9 - Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados |
| B2 | CB2 - Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos máis amplos (ou multidisciplinares) relacionados coa súa área de estudo |
| B3 | CB3 - Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos |
| B4 | CB4 - Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades |
| B6 | CG1 - Ter capacidade de análise e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación |
| B7 | CG2 - Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións |
| B10 | CG5 - Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestruturas, equipamentos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos |
| C4 | CT4 - Valorar a importancia da seguridade da información no avance socioeconómico da sociedade |
| C5 | CT5 - Ter capacidade para comunicarse oralmente e por escrito en inglés |

| Resultados da aprendizaxe | | | |
|--|-----|-------------------------------------|-----|
| Resultados de aprendizaxe | | Competencias / Resultados do título | |
| Coñecer a seguridade nas diferentes capas relacionadas cos sistemas ubicuos e as tecnoloxías que utilizan. | AP4 | BP2 | CP4 |
| | AP9 | BP3 | CP5 |
| | | BP4 | |
| | | BP6 | |
| | | BP7 | |
| | | BP10 | |



| | | | |
|--|------------|----------------------------------|------------|
| Entender os problemas de seguridade asociados ao mundo ubicuo. | AP4 AP9 | BP2 BP3 BP4 BP6 BP10 | CP4 CP5 |
| Coñecer casos reais de ataques a sistemas ubicuos. | AP4 | BP2 BP3 BP4 BP10 | CP4 CP5 |

| Contidos | |
|--------------------------------------|--|
| Temas | Subtemas |
| Seguridade física | Elementos de hardware. Compoñentes. - Buses de comunicación. - Interfaces. - Hardware criptográfico. Ataques. |
| Seguridade no middleware | Seguridade no proceso de arranque. Seguridade no sistema operativo. Control de acceso. Cifrado. Actualización do firmware. |
| Seguridade nas comunicacións | Comunicacións sen fíos. Riscos e ameazas nas comunicacións |
| Seguridade na percepción do contorno | Ataques nos sistemas de posicionamento. Ataques ás medidas dos sensores. Privacidade |

| Planificación | | | | |
|--------------------------|-----------------------------------|---|-------------------------|--------------|
| Metodoloxías / probas | Competencias / Resultados | Horas lectivas (presenciais e virtuais) | Horas traballo autónomo | Horas totais |
| Sesión maxistral | A4 A9 B2 B3 B4 B6 B7 B10 C5 C4 | 10 | 20 | 30 |
| Prácticas de laboratorio | A4 A9 B2 B3 B4 B6 B7 | 10 | 35 | 45 |
| Atención personalizada | | 0 | | 0 |

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

| Metodoloxías | |
|------------------|--|
| Metodoloxías | Descrición |
| Sesión maxistral | Realización en grupo do deseño, implementación e proba dun sistema IoT, poñendo especial énfase na seguridade. Realización en grupo de ataques á seguridade dos sistemas implementados por outros compañeiros ou de terceiros. Con esta metodoloxía traballaranse as competencias CB2, CB3, CB4, CG1, CG2, CG5, CE4, CE9, CT4 e CT5. |



| | |
|--------------------------|--|
| Prácticas de laboratorio | Exposición, por parte dos profesores, dos principais contidos teóricos relacionados coa seguridade para sistemas ubicuos (seguridade empotrada, nas comunicacións e nos backends) Con esta metodoloxía contribuirase a adquisición das competencias CB2, CB3, CB4, CG1, CG2, CE4 e CE9. |
|--------------------------|--|

Atención personalizada

| Metodoloxías | Descrición |
|--|--|
| Prácticas de laboratorio Sesión maxistral | Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial (durante a propia sesión maxistral, ou durante o horario establecido para as titorias). O horario de titorias establecerase ao principio do curso e publicarse na páxina web da materia. |

Avaliación

| Metodoloxías | Competencias / Resultados | Descrición | Cualificación |
|--------------------------|-----------------------------------|--|---------------|
| Prácticas de laboratorio | A4 A9 B2 B3 B4 B6 B7 | O alumnado dividirase en grupos para a realización do deseño, implementación e proba dun sistema IoT, poñendo especial énfase na seguridade. O mesmo grupo realizará ataques á seguridade dos sistemas implementados por outros compañeiros ou por terceiros. O proxecto realizado, e o informe contendo o resultado dos ataques completados (en canto á súa calidade e ao seu éxito) serán avaliados despois da súa entrega valorando aspectos como a corrección, a calidade, as prestacións e as funcionalidades. Deberase entregar o código, prototipos e documentación realizados. Así mesmo, será necesario realizar unha presentación dos resultados. Durante a realización do proxecto realizarase un seguimento continuo do deseño e da evolución da implementación. Se os resultados intermedios non son satisfactorios, poderase aplicar unha penalización de ata o 20% da nota. O seguimento será grupal e individual: cada un dos membros do grupo debe documentar as tarefas desenvolvidas dentro do seu equipo e responder sobre elas. | 80 |
| Sesión maxistral | A4 A9 B2 B3 B4 B6 B7 B10 C5 C4 | Realizaranse un ou varios exames para avaliar a comprensión dos contidos presentados nas sesións maxistrais. De haber máis de un exame, a nota final será a media aritmética das distintas probas | 20 |

Observacións avaliación



Para superar a materia é necesario completar as distintas partes nas que se divide (exame ou exames acerca dos contidos expostos na sesión maxistral e proxectos). A nota final será o resultado de aplicar a media xeométrica ponderada da nota de cada unha das partes.

Así, se a nota das sesións maxistrais é NT, e a nota do proxecto é NP, a nota final será:

$$\text{Nota} = \text{NT}^{0.2} + \text{NP}^{0.8}$$

Durante o primeiro mes, os estudantes deberán indicar explicitamente e por escrito o seu desexo de cursar a materia seguindo a avaliación única. Noutro caso considerarase que seguen a avaliación continua. Aqueles que sigan a avaliación continua non se poderán considerar "non presentados" unha vez se realice a entrega do primeiro cuestionario ou tarefa.

Os alumnos que opten pola avaliación única deberán presentar adicionalmente un dossier que deberá defender presencialmente ante os profesores, onde se inclúan tódolos detalles sobre a realización das distintas tarefas, moi especialmente o proxecto. No caso de seguir a avaliación única, os alumnos deberán realizar o traballo de forma individual, salvo que o profesorado lles comunique explicitamente a autorización para realizalo en grupo.

Segunda oportunidade

Só poderán optar á segunda oportunidade aqueles alumnos que non superaron a primeira oportunidade (ao finalizar o cuadrimestre). A avaliación será a descrita nos apartados anteriores, pero adicionalmente será preciso presentar un dossier que deberá ser defendido presencialmente ante os profesores, onde se inclúan tódolos detalles sobre a realización das distintas tarefas, moi especialmente o proxecto.

Aqueles estudantes que seguisen a avaliación continua poden optar por manter as notas obtidas na primeira oportunidade para as distintas partes da materia ou descartalas.

Outros comentarios

As puntuacións obtidas só son válidas para o curso académico en vigor.

Aínda que o proxecto se desenvolverá (na medida do posible) en grupos, os alumnos deben deixar evidencias do seu traballo individual dentro do grupo. No caso no que o rendemento dun alumno ou alumna non sexa acorde ao dos seus compañeiros de grupo, considerarase a súa expulsión do mesmo e/ou poderá ser avaliado de forma individual nesta parte.

O uso de calquera material durante a realización dos exames terá que ser autorizado explicitamente polo profesorado.

En caso de detección de plaxio ou de comportamento non ético nalgún dos traballos/probas realizadas, a cualificación final da materia será de "suspenso (0)" e os profesores comunicarán o asunto ás autoridades académicas para que tome as medidas oportunas.

Fontes de información

| | |
|------------------------------------|--|
| Bibliografía básica | - Brian Russell, Drew Van Duren (2016). Practical Internet of Things Security. Packt Publishing |
| Bibliografía complementaria | - Houbing Song, Glenn A. Fink, Sabina Jeschke (2018). Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.. Wiley - Bruce Schneider (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley |

Recomendacións

Materias que se recomenda ter cursado previamente

Seguridade da Información/614530003
 Test de Intrusión/614530008
 Fortificación de Sistemas Operativos/614530007
 Seguridade en Comunicacions/614530004
 Seguridade de Aplicacións/614530005
 Redes Seguras/614530006

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