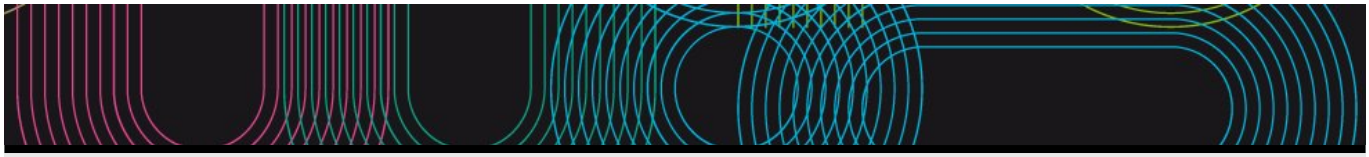

DATOS IDENTIFICATIVOS				
Seguridade ubicua				
Materia	Seguridade ubicua			
Código	V05M175V01208			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán Galego			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Gil Castiñeira, Felipe José			
Profesorado	Gil Castiñeira, Felipe José Rabuñal Dopico, Juan Ramón			
Correo-e	felipe@uvigo.es			
Web	http://faitic.uvigo.es			
Descrición xeral	Os dispositivos intelixentes estannos proporcionando cada vez máis servizos case sen que sexamos conscientes da súa presenza: o coche deixou de ser unha máquina simplemente mecánica para converterse nun sistema conectado e con un enorme control electrónico; nos hoteis xa non utilizamos unha chave, senón que podemos abrir a nosa habitación con unha tarxeta ou co noso móbil; os termostatos da nosa casa pódense conectar con un servizo de predición meteorolóxica e adecuarse ao tempo das próximas horas. Son todos exemplos das aplicacións que permiten as tecnoloxías "embedded", as redes de comunicacións sen fíos, e en definitiva, a "Internet of Things" (IoT). Esta materia analiza os problemas e as mellores prácticas á hora de facer que este tipo de sistemas sexan seguros.			

Competencias	
Código	
A2	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 más amplos (ou multidisciplinares) relacionados coa súa área de estudo
A3	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.
A4	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
B1	Ter capacidade de análisis 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
B2	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.
B5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
C4	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
C9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
D4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
D5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Coñecer a seguridade nas diferentes capas relacionadas cos sistemas ubicuos e as tecnoloxías que utilizan.	A2 A3 A4 B1 B2 B5 C4 C9 D4 D5
Entender os problemas de seguridade asociados ao mundo ubicuo.	A2 A3 A4 B1 B2 B5 C4 C9 D4 D5
Coñecer casos reais de ataques a sistemas ubicuos.	A2 A3 A4 B5 C4 D4 D5

Contidos	
Tema	
Seguridade física	Elementos de hardware. Compoñentes. - Buses de comunicación. - Interfaces. - Hardware criptográfico. Ataques.
Seguridade no middleware	Seguridade no proceso de arrinque. 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			
	Horas na aula	Horas fóra da aula	Horas totais
Aprendizaxe baseado en proxectos	10	35	45
Lección maxistral	10	20	30

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

Metodoloxía docente	
	Descrición
Aprendizaxe baseado en proxectos	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.

Lección maxistral	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
Lección maxistral	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse durante a propia sesión maxistral, ou durante o horario establecido para as titorias. O horario de titorias establecerase ao principio do curso e publicarase na páxina web da materia.
Aprendizaxe baseado en proxectos	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, os profesores orientarán e guiarán aos alumnos durante a realización do proxecto. As dúbidas atenderanse durante as sesións de titoría en grupo, ou durante o horario establecido para as titorias. O horario de titorias establecerase ao principio do curso e publicarase na páxina web da materia.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Aprendizaxe baseado en proxectos	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 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	A2 B1 C4 D4 A3 B2 C9 D5 A4 B5
Lección maxistral	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	A2 B1 C4 A3 B2 C9 A4

Outros comentarios sobre a 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:

$$\textbf{Nota} = NT^{0.2} \times NP^{0.8}$$

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.

Bibliografía. Fontes de información

Bibliografía Básica

Brian Russell, Drew Van Duren, **Practical Internet of Things Security**, 1, Packt Publishing, 2016

Bibliografía Complementaria

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 1, Wiley, 2018

Bruce Schneider, **Applied Cryptography: Protocols, Algorithms and Source Code in C**, 2, Wiley, 2015

Adam Shostack, **Threat Modeling. Designing for Security.**, 1, Wiley, 2014

Recomendacións

Materias que se recomenda ter cursado previamente

Fortificación de sistemas operativos/V05M175V01202
Redes Seguras/V05M175V01105
Seguridade de aplicacións/V05M175V01104
Seguridade da información/V05M175V01102
Seguridade en comunicacións/V05M175V01103
Tests de intrusión/V05M175V01203

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais áxil e eficaz ao ser coñecido de antemán (ou cunha ampla antelación) polo alumnado e o profesorado a través da ferramenta normalizada e institucionalizada das guías docentes DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
A metodoloxía de aprendizaxe en proxectos será modificada no caso no que se produza unha situación que impida o traballo en grupo. Se o proxecto en grupo xa estaba iniciado, farase que o sistema IoT deseñado por cada un dos grupos estea accesible a través da Internet para que o proxecto se poda rematar de forma remota. De non se ter iniciado, propoñeráselles aos alumnos a realización dun proxecto alternativo relacionado coa seguridade IoT que podan realizar individualmente (por exemplo, o modelado de ameazas e o ataque dun sistema comercial). De dispoñer do número

suficiente de dispositivos, estes faránselles chegar aos alumnos. Noutro caso realizarase un proxecto utilizando simuladores ou limitarase o traballo a unha análise teórica.