Guia docente				
Datos Identificativos				2020/21
Asignatura (*)	Seguridad Ubicua		Código	614530013
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero	Optativa	3
Idioma	CastellanoGallego			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da Información			
Coordinador/a	Rabuñal Dopico, Juan Ramon	Correo electrónico	juan.rabunal@udc.es	
Profesorado	Alvarellos González, Alberto José Martinez Perez, Maria Rabuñal Dopico, Juan Ramon	Correo electrónico	alberto.alvarellos@udc.es maria.martinez@udc.es juan.rabunal@udc.es	
Web	faitic.uvigo.es			
Descripción general	Coordinada por la Universidade de Vigo. Consultad la guía en: https://secretaria.uvigo.gal/docnet-nuevo/guia_docent/?centre=305			
Plan de contingencia	1. Modificaciones en los contenidos 2. Metodologías *Metodologías docentes que se mantienen *Metodologías docentes que se modifican 3. Mecanismos de atención personalizada al alumnado 4. Modificacines en la evaluación *Observaciones de evaluación: 5. Modificaciones de la bibliografía o webgrafía			

Competencias del título	
Código	Competencias del título
A4	CE4 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información
A9	CE9 - Tener capacidad para elaborar de planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
B2	CB2 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
B3	CB3 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
B4	CB4 - Que los estudiantes sepan comunicar sus conclusiones, y los conocimientos y razones últimas que las sustentan, a públicos especializados y no especializados de un modo claro y sin ambigüedades
B6	CG1 - Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación

B7	CG2 - Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones
B10	CG5 - Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
C4	CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
C5	CT5 - Tener capacidad para comunicarse oralmente y por escrito en inglés

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias del título		
Coñecer a seguridade nas diferentes capas relacionadas cos sistemas ubicuos e as tecnoloxías que utilizan.	AP4 AP9	BP2 BP3 BP4 BP6 BP7 BP10	CP4 CP5
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

Contenidos	
Tema	Subtema
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				
Metodologías / pruebas	Competéncias	Horas presenciales	Horas no presenciales / trabajo autónomo	Horas totales
Sesión magistral	A4 A9 B2 B3 B4 B6 B7 B10 C4 C5	10	20	30

Prácticas de laboratorio	A4 A9 B2 B3 B4 B6 B7	10	35	45
Atención personalizada		0		0
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	**Descripción**
Sesión magistral	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	
Metodologías	**Descripción**
Prácticas de laboratorio Sesión magistral	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 publicarase na páxina web da materia.

Evaluación			
Metodologías	**Competéncias**	**Descripción**	**Calificación**
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 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 magistral	A4 A9 B2 B3 B4 B6 B7 B10 C4 C5	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

Observaciones evaluación
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: Nota = NT^0.2 ? 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 avaliacióncontinua 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.

Fuentes de información	
Básica	- Brian Russell, Drew Van Duren (2016). Practical Internet of Things Security. Packt Publishing
Complementária	- 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

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Seguridad de la Información/614530003 Test de Intrusión/614530008 Fortificación de Sistemas Operativos/614530007 Seguridad en Comunicaciones/614530004 Seguridad de Aplicaciones/614530005 Redes Seguras/614530006
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías