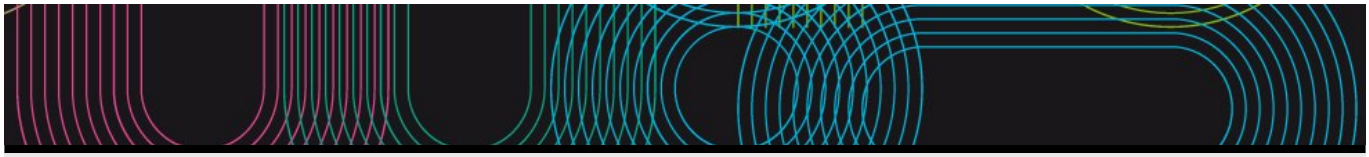

DATOS IDENTIFICATIVOS				
Seguridad ubicua				
Asignatura	Seguridad ubicua			
Código	V05M175V01208			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano Gallego			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Gil Castiñeira, Felipe José			
Profesorado	Gil Castiñeira, Felipe José Rabuñal Dopico, Juan Ramón			
Correo-e	xil@gti.uvigo.es			
Web				
Descripción general	Los dispositivos inteligentes nos están proporcionando cada vez más servicios casi sin que seamos conscientes de su presencia: el coche ha dejado de ser una máquina simplemente mecánica para convertirse en un sistema conectado y con un enorme control electrónico; en los hoteles ya no utilizamos una llave, sino que podemos abrir nuestra habitación con una tarjeta o incluso con el móvil; los termostatos de nuestra casa se pueden conectar con un servicio de predicción meteorológica y adecuarse al tiempo de las próxima horas. Son todos ejemplos de las aplicaciones que permiten las tecnologías "embedded", las redes de comunicación inalámbricas, y en definitiva, la "Internet of Things" (IoT). Esta asignatura analiza los problemas y las mejores prácticas a la hora de hacer que este tipo de sistemas sean seguros.			

Competencias	
Código	
A2	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
A3	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.
A4	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
B1	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
B2	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.
B5	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	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información
C9	Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
D4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
D5	Tener capacidad para comunicarse oralmente y por escrito en inglés.

Resultados de aprendizaje	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Conocer la seguridad en las diferentes capas relacionadas con los sistemas ubicuos y las tecnologías que se utilizan.	A2 A3 A4 B1 B2 B5 C4 C9 D4 D5
Entender los problemas de seguridad asociados al mundo ubicuo.	A2 A3 A4 B1 B2 B5 C4 C9 D4 D5
Conocer casos reales de ataques a sistemas ubicuos.	A2 A3 A4 B5 C4 D4 D5

Contenidos

Tema	
Seguridad física	■ Elementos de hardware. ▹ Componentes. ▹ Buses de comunicación. ▹ Interfaces. ▹ Hardware criptográfico. ■ Ataques. ▹ Volcado de firmware. ▹ Captura de tráfico en buses. ▹ Interfaces. ▹ "Glitches".
Seguridad en el middleware	■ Seguridad en el proceso de inicio. ■ Seguridad en el sistema operativo. ■ Control de acceso. ■ Cifrado. ■ Actualización del firmware.
Seguridad en las comunicaciones	■ Comunicaciones inalámbricas. ■ Riesgos y amenazas en las comunicaciones. ■ Seguridad en las redes Wi-Fi. ■ Seguridad en redes celulares. ■ Seguridad en redes de sensores.
Seguridad en la percepción del entorno	■ Ataques en los sistemas de posicionamiento. ■ Ataques a las medidas de los sensores. ■ Privacidad.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Aprendizaje basado en proyectos	10	35	45
Lección magistral	10	20	30

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción

Aprendizaje basado en proyectos	Realización en grupo del diseño, implementación y prueba de un sistema IoT, poniendo un énfasis especial en la seguridad. Realización en grupo de ataques a la seguridad de lo sistemas implementados por otros compañeros o de terceros. Con esta metodología se trabajarán las competencias CB2, CB3, CB4, CG1, CG2, CG5, CE4, CE9, CT4 y CT5.
Lección magistral	Exposición, por parte de los profesores, de los principales contenidos teóricos relacionados con la seguridad para sistemas ubicuos (seguridad empotrada, en las comunicaciones y en los backends) Con esta metodología se contribuirá a la adquisición de las competencias CB2, CB3, CB4, CG1, CG2, CE4 y CE9.

Atención personalizada

Metodologías	Descripción
Lección magistral	Los profesores de la asignatura proporcionarán atención individual y personalizada a los alumnos durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial (durante la propia sesión magistral, o durante el horario establecido para tutorías). El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.
Aprendizaje basado en proyectos	Los profesores de la materia proporcionarán atención individual y personalizada a los alumnos durante el curso, solucionando sus dudas y preguntas. Así mismo, los profesores orientarán y guiarán a los alumnos durante la realización del proyecto. Las dudas se atenderán de forma presencial (durante las sesiones de tutoría en grupo, o durante el horario establecido para las tutorías). El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la materia.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Aprendizaje basado en proyectos	El alumnado se dividirá en grupos para la realización del diseño, implementación y prueba de un sistema IoT, poniendo un énfasis especial en la seguridad. El mismo grupo realizará ataques a la seguridad de los sistemas implementados por otros compañeros o por terceros. El proyecto realizado, y el informe que contiene el resultado de los ataques completados (en cuanto a su calidad y a su éxito) serán evaluados después de su entrega valorando aspectos como la corrección, la calidad, las prestaciones y las funcionalidades. Se deberá entregar el código, prototipos y documentación realizados. Asimismo, será necesario realizar una presentación de los resultados. Durante la realización del proyecto se realizará un seguimiento continuo del diseño y de la evolución de la implementación. Si los resultados intermedios no son satisfactorios, se podrá aplicar una penalización de hasta el 20% de la nota. El seguimiento será grupal e individual: cada uno de lo miembros del grupo debe documentar las tareas desarrolladas dentro de su equipo y responder sobre ellas.	80	A2 B1 C4 D4 A3 B2 C9 D5 A4 B5
Lección magistral	Se realizarán uno o varios examenes para evaluar la comprensión de los contenidos presentados en las sesiones magistrales. Si hay más de un examen, la nota final será la media aritmética de las distintas pruebas.	20	A2 B1 C4 A3 B2 C9 A4

Otros comentarios sobre la Evaluación

Para superar la asignatura es necesario completar las distintas partes en las que se divide (examen o exámenes acerca de los contenidos expuestos en la sesión magistral y el proyecto). La nota final será el resultado de aplicar la **media geométrica ponderada** de la nota de cada una de las partes.

Así, si la nota de las sesiones magistrales es NT, y la nota del proyecto es NP, la nota final será:

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

Durante el primer mes, los estudiantes deberán indicar explícitamente y por escrito su deseo de cursar la materia siguiendo la evaluación única. En otro caso se considerará que siguen la evaluación continua. Aquellos que sigan la evaluación continua no se podrán considerar "no presentados" así que hayan realizado la entrega del primer cuestionario o tarea.

Los alumnos que opten por la evaluación única deberán presentar adicionalmente un *dossier* que deberán defender presencialmente ante los profesores, en el que se incluyan todos los detalles sobre la realización de las distintas tareas, y muy especialmente el proyecto. En el caso de seguir la evaluación única, los alumnos deberán realizar el trabajo de forma individual, salvo que el profesorado les comunique explícitamente la autorización para realizarlo en grupo.

Segunda oportunidad

Solo podrán optar a al segunda oportunidad los alumnos que no superaron la primera oportunidad (al finalizar el cuatrimestre). La evaluación será la descrita en los apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante los profesores, en el que se incluyan todos los detalles sobre la realización de las distintas tareas, muy especialmente el proyecto.

Aquellos estudiantes que hubiesen seguido la evaluación continua pueden optar por mantener las notas obtenidas en la primera oportunidad para las distintas partes de la asignatura o descartarlas.

Otros comentarios

Las puntuaciones obtenidas solo son válidas para el curso académico en vigor. Aunque el proyecto se desarrollará (en la medida de lo posible) en grupos, los alumnos deben guardar evidencias de su trabajo individual dentro del grupo. En el caso en el que el rendimiento de un alumno o alumna no sea acorde al de sus compañeros de grupo, se considerará su expulsión del mismo y/o podrá ser evaluado de forma completamente individual en esta parte.

El uso de cualquiera material durante la realización de los exámenes tendrá que ser autorizado explícitamente por el profesorado.

En caso de detección de plagio o de comportamiento no ético en alguno de los trabajos/pruebas realizadas, la calificación de la materia será de "suspenso (0)" y los profesores comunicarán el asunto a las autoridades académicas para que tomen las medidas oportunas.

Fuentes de información

Bibliografía Básica

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

Bibliografía Complementaria

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

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Fortificación de sistemas operativos/V05M175V01202
Redes Seguras/V05M175V01105
Seguridad de aplicaciones/V05M175V01104
Seguridad de la información/V05M175V01102
Seguridade en comunicacións/V05M175V01103
Tests de intrusión/V05M175V01203