Seguridad en IoT

Curso Académico: (2019 / 2020) **Fecha de revisión: 30/04/2020 18:38:38**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: CAMARA NUÑEZ, MARIA CARMEN

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Ninguno

OBJETIVOS

Competencias Básicas
CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 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
CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular 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
CB9 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

Competencias generales
CG2 Capacidad de recopilación y análisis de los conocimientos existentes en las diferentes áreas de IOT, de forma autónoma, y capacidad de hacer una propuesta de posibles soluciones a los problemas planteados.
CG7 Capacidad para saber comunicar (de forma oral y escrita) las conclusiones - y los conocimientos y razones últimas que las sustentan - a públicos especializados y no especializados de un modo claro y sin ambigüedades.

Competencias específicas
CE5 Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de garantía de seguridad en el tratamiento y acceso a la información en dispositivos computacionalmente limitados y en redes IoT.
CE6 Capacidad para aplicar métodos matemáticos, estadísticos y de inteligencia artificial para modelar, diseñar y desarrollar aplicaciones, servicios y sistemas inteligentes en el ámbito de la IoT.
CE10 Habilidad de integrar los diferentes sistemas de percepción y control de procesos tanto desde el punto de vista hardware como software.
CE13 Capacidad para aplicar la legislación, regulación y normalización de la IoT.

RESULTADOS DEL APRENDIZAJE
Los resultados del aprendizaje que los estudiantes deberán tener son:
- Conocer y aplicar el derecho y aspectos legales de IoT.
- Conocer los modelos y estructuras de referencia de IoT.
- Capacidad de análisis, diseño y control de sistemas y de servicios
- Conocer los riesgos de seguridad propios de un entorno IoT.
- Conocer las medidas de seguridad física aplicables a dispositivos móviles.
- Conocer y aplicar las técnicas fundamentales de protección de la información almacenada en dispositivos móviles.
- Dominar los principales protocolos de seguridad existentes para comunicaciones móviles y su espectro de aplicación.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Tema 1. Introducción.
   a. Introducción a ciberseguridad.
   b. Introducción a la IoT.

2. Tema 2. Arquitecturas en IoT
   a. Arquitecturas.
   b. Dispositivos.

3. Tema 3. Servicios y mecanismos de Seguridad
   a. Protocolos de seguridad/comunicaciones.
   b. Autenticación.
   c. Identificación (Biometría)
   d. Primitivas criptográficas.

4. Tema 4. Conceptos avanzados
   a. Dispositivos médicos (implantables).
   b. Análisis forense de dispositivos IoT.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS DEL PLAN DE ESTUDIOS REFERIDAS A MATERIAS

AF1 Clase teórica
AF4 Prácticas de laboratorio
AF6 Trabajo en grupo
AF7 Trabajo individual del estudiante
AF8 Exámenes parciales y finales

Código actividad	Nº Horas totales	Nº Horas Presenciales	% Presencialidad Estudiante
AF1	26	26	100
AF4	16	16	100
AF6	40	0	0
AF7	64	0	0
AF8	4	4	100
TOTAL MATERIA	150	46	31%

METODOLOGÍAS DOCENTES FORMATIVAS DEL PLAN REFERIDAS A MATERIAS

MD1 Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
MD2 Lectura crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
MD3 Resolución de casos prácticos, problemas, etc.¿ planteados por el profesor de manera individual o en grupo.
MD4 Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos
MD5 Elaboración de trabajos e informes de manera individual o en grupo.

SISTEMA DE EVALUACIÓN

Peso porcentual del Examen/Prueba Final:	50
Peso porcentual del resto de la evaluación:	50

Se establece el siguiente sistema de evaluación:

1. Convocatoria ordinaria - evaluación continua

A. Examen final (50% de la nota final)
-La nota mínima será de 4.0 para superar la asignatura

B. Trabajos periódicos (50% de la nota final)
-Estado del arte sobre un tema relacionado con la asignatura.

Peso porcentual del Examen/Prueba Final:	50
Peso porcentual del resto de la evaluación:	50

-Trabajos prácticos (ej., sistema biométrico, análisis forense de dispositivos IoT).

2. Convocatoria ordinaria - evaluación no continua
A. Examen final (100% de la nota final)
-La calificación máxima obtenible será de 6 puntos
-Será necesario obtener 5 puntos para superar la asignatura.
-El examen contendrá ejercicios específicos para comprobar la adquisición de competencias relativas a los trabajos.

3. Convocatoria extraordinaria
La calificación de los estudiantes en la convocatoria extraordinaria se ajustará a las siguientes reglas:

a. Si el estudiante siguió el proceso de evaluación continua, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.

b. Si el estudiante no siguió el proceso de evaluación continua, tendrá derecho a realizar un examen en la convocatoria extraordinaria con un valor del 100 % de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las actividades realizadas durante el curso. En esta asignatura no se permite la reentrega de los trabajos en esta convocatoria.

c. Aunque el estudiante hubiera seguido el proceso de evaluación continua, tendrá derecho a ser calificado en la convocatoria extraordinaria teniendo en cuenta únicamente la nota obtenida en el examen final cuando le resulte más favorable.

BIBLIOGRAFÍA BÁSICA

- Aaron Guzman, Aditya Gupta IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, Packt Publishing, 2017

- D. Uckelmann, M. Harrison and F. Michahelles Architecting the Internet of Things, Springer-Verlag Berlin Heidelberg, 2011

- Dimitrios Serpanos, Marilyn Wolf Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies, Springer, 2018

- FTC Staff Report Internet of Things: Privacy & Security in a Connected World, FTC, 2015

- Francis daCosta Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, Apress, 2014

- IoT Hackers Handbook IoT Hackers Handbook: An Ultimate Guide to Hacking the Internet of Things and Learning IoT Security , IoT Hackers Handbook, 2017

BIBLIOGRAFÍA COMPLEMENTARIA

- N. Jeyanthi, Ajith Abraham, Hamid Mcheick Ubiquitous Computing and Computing Security of IoT, Springer, 2018

- Sunil Cheruvu, Anil Kumar, Ned Smith, David Wheeler Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform security deployment, Apress, 2019