Protocolos de Transporte de Datos en IoT

Curso Académico: (2019 / 2020) **Fecha de revisión: 04/05/2020 23:14:34**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: PÉREZ DÍAZ, JAIME

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Arquitecturas de Redes IoT

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

CG1 Capacidad para identificar, definir y formular los problemas a resolver relacionados con aplicaciones IOT. Esta capacidad incluye la valoración simultánea de todos los factores en juego, no sólo técnicos, sino también medioambientales y de responsabilidad civil.

CG5 Capacidad de comunicación pública de los conceptos, desarrollos y resultados, relacionados con actividades en IOT, adaptada al perfil de la audiencia.

CG6 Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, con la capacidad de integrar conocimientos.

COMPETENCIAS ESPECÍFICAS

CE3 Capacidad identificar los riesgos de seguridad en comunicaciones en entornos IoT e identificar los protocolos de comunicación adecuados para mitigar los riesgos identificados.

CE4 Capacidad de diseñar e implementar redes de comunicaciones para entornos IoT.

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.

CE11 Capacidad para diseñar y controlar las redes inalámbricas de última generación en aplicaciones IoT.

CE12 Capacidad para aplicar la comunicación de dispositivos, tanto entre ellos como de manera global, en el entorno IoT.

RESULTADOS DEL APRENDIZAJE

Los resultados del aprendizaje que los estudiantes deberán tener son:

- Conocer los protocolos de comunicaciones para redes IoT.
- Conocer los mecanismos de seguridad para comunicaciones IoT.
- Capacidad para diseñan una solución de comunicaciones para IoT seleccionando y adaptando los protocolos de comunicaciones más apto para el caso de uso.

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
CG1 Capacidad para identificar, definir y formular los problemas a resolver relacionados con aplicaciones IOT. Esta capacidad incluye la valoración simultánea de todos los factores en juego, no sólo técnicos, sino también medioambientales y de responsabilidad civil.
CG5 Capacidad de comunicación pública de los conceptos, desarrollos y resultados, relacionados con actividades en IOT, adaptada al perfil de la audiencia.
CG6 Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, con la capacidad de integrar conocimientos.

COMPETENCIAS ESPECÍFICAS
CE3 Capacidad identificar los riesgos de seguridad en comunicaciones en entornos IoT e identificar los protocolos de comunicación adecuados para mitigar los riesgos identificados.
CE4 Capacidad de diseñar e implementar redes de comunicaciones para entornos IoT.
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.
CE11 Capacidad para diseñar y controlar las redes inalámbricas de última generación en aplicaciones IoT.
CE12 Capacidad para aplicar la comunicación de dispositivos, tanto entre ellos como de manera global, en el entorno IoT.

RESULTADOS DEL APRENDIZAJE
Los resultados del aprendizaje que los estudiantes deberán tener son:
- Conocer los protocolos de comunicaciones para redes IoT.
- Conocer los mecanismos de seguridad para comunicaciones IoT.
- Capacidad para diseñan una solución de comunicaciones para IoT seleccionando y adaptando los protocolos de comunicaciones más apto para el caso de uso.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción.
2. Protocolos de aplicación: HTTP, CoAP, MQTT / MQTT-SN, otros.
3. Capa de descubrimiento: DNS-SD / mDNS, CoAP Resource Discovery.
4. Seguridad en redes de IoT: DTLS y otros.
5. Prácticas

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

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
AF	10,5	10,5	100
AF4	10,5	10,5	100
AF6	20	0	0

AF7	32	0	0
AF8	2	2	100
TOTAL	75	23	31%

METODOLOGÍA A UTILIZAR:
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:	80
Peso porcentual del resto de la evaluación:	20

SE2 Trabajos individuales o en grupo realizados durante el curso
SE3 Examen final

La evaluación de la asignatura será de acuerdo a lo siguiente:
- Trabajos individuales o en grupo realizados durante el curso (SE2): 20% de la nota final.
- Examen final (SE3): 80 % de la nota final.

BIBLIOGRAFÍA BÁSICA

- Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, Communications Surveys & Tutorials, IEEE , vol.17, no.4, pp.2347-2376,, Fourth quarter 2015

- Douglas Comer The ZigBee IP Protocol Stack, The Internet Protocol Journal, Volume 17, No. 2,, December 2014

- Ilya Grigorik HTTP/2: A New Excerpt from High Performance Browser Networking, O'Reilly, 2015

- Simone Cirani, Gianluigi Ferrari, Marco Picone, Luca Veltri Internet of Things: Architectures, Protocols and Standards, Wiley, 2018

- Stallings, W. Internet of Things: Network and Security Architecture, Internet Protocol Journal, vol.18, no. 4, pp. 2-24,, Dec 2015

- V. Karagiannis, P. Chatzimisios, F. Vázquez-Gallego, J. Alonso-Zarate A Survey on Application Layer Protocols for the Internet of Things, Transaction on IoT and Cloud Computing, Vol. 1, No. 1,, January 2015

- Villaverde, B.C.; De Paz Alberola, R.; Jara, A.J.; Fedor, S.; Das, S.K.; Pesch, D. Service Discovery Protocols for Constrained Machine-to-Machine Communications, Communications Surveys & Tutorials, IEEE ol.16, no.1, pp.41-60, First Quarter 2014

BIBLIOGRAFÍA COMPLEMENTARIA

- Selander, G.; Mattson, J.; Palombini, F.; Seitz, L. Object Security for Constrained RESTful Environments (OSCORE), Internet-Draft; IETF, Fremont, CA, USA, 2018.