BlockChain y Tecnologías de Seguridad

Curso Académico: (2020 / 2021) **Fecha de revisión: 10-07-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA DE

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Ninguna

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
CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Competencias generales
CG1 Capacidad para comprender y aplicar métodos y técnicas del ámbito de la Ingeniería Informática en los mercados financieros
CG2 Capacidad de concebir, diseñar o crear, poner en práctica y adoptar un proceso sustancial de desarrollo o creación de software para mercados financieros
CG3 Capacidad para la aplicación de los conocimientos adquiridos y para resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, hasta ser capaces de integrar estos conocimientos.
CG4 Capacidad para elaborar adecuadamente y con cierta originalidad composiciones escritas o argumentos motivados, de redactar planes o proyectos de trabajo.

Competencias específicas
CE2 Analizar y evaluar las principales tecnologías de la información y las comunicaciones aplicadas en el sector financiero
CE3 Participar en el desarrollo de software financiero, desde su concepción en las fases de análisis, hasta su implantación e integración con otros sistemas

Resultados de aprendizaje que adquiere el estudiante
- Comprender el uso de Sistemas de Información en los Mercados Financieros
- Entender las principales tecnologías del sector financiero
- Capacidad de analizar las Infraestructuras tecnológicas para los Mercados Financieros
- Entender los principales Ejemplos de Aplicación
- Comprender los requisitos en infraestructura para implantar sistemas de información financieros

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1.- Introducción a la seguridad en las TIC
- 1.1. Definiciones
- 1.2. Servicios de seguridad
- 1.3. Mecanismos de seguridad

1.4. Amenazas y vulnerabilidades. Situación actual

2.- Fundamentos criptográficos
- 2.1. Entropía y aleatoriedad
- 2.2. Ataques. Complejidad

3.- Mecanismos de aseguramiento de la información financiera
- 3.1. Cifrado de información
- 3.2. Autenticación
- 3.3. Funciones resumen
- 3.4. Firma electrónica

4.- Blockchain. Fundamentos y aplicaciones
- 4.1. Conceptos básicos de Blockchain
- 4.2. Estrategias de consenso
- 4.3. Contratos inteligentes
- 4.4. Aplicaciones de Blockchain

5.- Criptomonedas
- 5.1. Bitcoin
- 5.2. Ethereum
- 5.3. Monero
- 5.4. Otras altcoins

6.- Marco regulatorio
- 6.1. GDPR
- 6.2. Reglamento eIDAS
- 6.3. Directiva NIS
- 6.4. Esquema Nacional de Seguridad

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Actividades formativas

AF1 Clase teórica
AF2 Actividades de e-learning
AF3 Clases teórico prácticas
AF4 Prácticas de laboratorio
AF5 Tutorías
AF6 Trabajo en grupo
AF7 Trabajo individual del estudiante

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

MD5 Elaboración de trabajos e informes de manera individual o en grupo

MD6 Actividades específicas de e-learning, relacionadas con el carácter semi-presencial del título, incluyendo la visualización de contenidos grabados, actividades de auto-corrección, participación en foros, y cualquier otro mecanismo de enseñanza on-line

Los horarios de las tutorías, ajustados a lo dispuesto por la Universidad, se podrán consultar en el espacio propio de la asignatura en la plataforma de enseñanza y aprendizaje (Aula Global). Incluirán al menos dos tramos, uno para atención presencial y otro para atención en línea, que deberán ser solicitados por correo electrónico con suficiente antelación. Además de estas tutorías fijadas oficialmente para la asignatura, los alumnos pueden solicitar y concertar con el profesor tutorías presenciales o en línea fuera de esos horarios.

SISTEMA DE EVALUACIÓN

SE1 Participación en clase (10%)
SE2 Trabajos individuales o en grupo realizados durante el curso, tanto en actividades presenciales como de e-learning (60%)
SE3 Examen final (30%)

Se establece el siguiente sistema de evaluación:
1. Convocatoria ordinaria

Examen final
- Representará el 30% de la nota final
- Tendrá carácter Teórico/Práctico
- Obligatorio e individual

Trabajo(s) Teórico(s)/Práctico(s).
- Representará el 60% de la nota final
- Obligatorio
- En grupos o individual, a definir al comienzo de la asignatura

Consideraciones para superar la asignatura:

- La nota mínima en el examen será de 4.0.
- Deberán entregarse todos los trabajos.

2. 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 adicionales específicas a los trabajos. En esta convocatoria no se podrán re-entregar los trabajos de evaluación continua, salvo indicación en contrario al comienzo de la asignatura.

Peso porcentual del Examen Final:	30
Peso porcentual del resto de la evaluación:	70

BIBLIOGRAFÍA BÁSICA

- Anderson, Ross Security Engineering: A guide to Building Dependable Distributed Sistems (2nd edition), Wiley, 2008
- Antonopoulos, Andreas Mastering Bitcoin, O'Reilly, 2015
- Antonopoulos, Andreas; Wood, Gavin Mastering Ethereum, O'Reilly, 2018
- Pfleeger, Charles et al Security in Computing (4th edition), Prentice Hall, 2007
- Stallings, William Cryptography and Network Security: Principles and Practice, Prentice Hall, 2013

BIBLIOGRAFÍA COMPLEMENTARIA

- Antonopoulos, Andreas Mastering Ethereum: Building Smart Contracts and Dapps, O' Reilly, 2018
- Bishop, Matt Computer Security: Art & Science., Addison-Wesley, 2015

RECURSOS ELECTRÓNICOS BÁSICOS

- McGubbin, Gregory . Solidity for Beginners. Smart contract development crash course: https://www.dappuniversity.com/articles/solidity-tutorial