ESCUELA POLITÉCNICA SUPERIOR DE CÓRDOBA

GRADO DE INGENIERÍA INFORMÁTICA

CURSO 2024/25

SEGURIDAD INFORMÁTICA

Datos de la asignatura

Denominación: SEGURIDAD INFORMÁTICA
Código: 101411
Plan de estudios: GRADO DE INGENIERÍA INFORMÁTICA **Curso:** 4
Materia: SEGURIDAD INFORMÁTICA
Carácter: OBLIGATORIA **Duración:** PRIMER CUATRIMESTRE
Créditos ECTS: 6.0 **Horas de trabajo presencial:** 60
Porcentaje de presencialidad: 40.0% **Horas de trabajo no presencial:** 90
Plataforma virtual: https://moodle.uco.es/

Profesor coordinador

Nombre: ROMERO DEL CASTILLO, JUAN ANTONIO
Departamento: INFORMÁTICA Y ANÁLISIS NUMÉRICO
Ubicación del despacho: Edificio Albert Einstein, 3ª Planta. Ala Sur.
E-Mail: aromero@uco.es **Teléfono:** 957211043

Breve descripción de los contenidos

La formación en Ciberseguridad es cada vez más importante y una capacidad fundamental e imprescindible para cualquier experto informático, más aún un/a ingeniero/a.
Los contenidos de esta asignatura se han elaborado teniendo en cuenta que el objetivo fundamental de esta asignatura es la mejora de la capacitación profesional en Ciberseguridad, Seguridad Informática y Seguridad de la Información tanto a nivel teórico, como a nivel práctico.
Una clave fundamental de la ciberseguridad en la empresa es la planificación. Se plantea también como objetivo fundamental de la asignatura entender el papel de cada plan de ciberseguridad en la empresa.

Conocimientos previos necesarios

Requisitos previos establecidos en el plan de estudios

Ninguna especificada

Recomendaciones

Ninguna especificada

Programa de la asignatura

1. Contenidos teóricos

1. Introducción. Seguridad en sistemas distribuidos.
2. La política de seguridad en la empresa
3. Gestión y dirección de la seguridad. Security Management
4. Desarrollo seguro de aplicaciones
5. Servicios de Seguridad
6. Encriptación Clásica.
7. Encriptación simétrica.
8. Encriptación de clave pública
9. Seguridad perimetral.
10. Aplicaciones y protocolos de seguridad.
11. Legislación.
12. Seguridad física y otros aspectos de la seguridad

2. Contenidos prácticos

Usaremos herramientas de Software Libre y los laboratorios de la plataforma educativa AWS Academy.

1.- Algoritmos de encriptación clásica.
2.- Algoritmos de encriptación simétrica.
3.- Incorporar la encriptación moderna a nuestros desarrollos.
4.- Funciones HASH e integridad de los datos.
5.- Encriptación de clave pública.
6.- Ejercicios con otras herramientas y técnicas de seguridad
7.- Hacking usando el Lenguaje Python.

Bibliografía

Referebcias básicas

- "Computer Security. Principles and Practice". William Stallings, Lawrie Brown. Pearson Education, Inc. 2008.
- Bruce Schneier. Applied Cryptography. 1996 John Wiley & Sons, Inc.
- "Cryptography and Network Security". William Stallings. Principles and Practices. Fourth Edition. 2006 Pearson
Education, Inc.
- "Building internet Firewalls". Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman. O Reilly2nd Edition. 2000.
- Security in Computing. Fifth Edition. Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies.Prentice Hall. 2015.
- Certified Information Systems Security Professional. CISSP Oficial Study Guide. Eighth Edition. Mike Chapple et al. SYBEX A Wiley Brand. 2018

Referencias aspectos normativos y legales:

- Web de la Escuela Politécnica Superior de Córdoba. https://www.uco.es/eps/es/titulaciones/gr-ing-informatica

- Normativa legal de la titulación: https://www.uco.es/eps/es/normativa-de-la-epsc#epsc

Metodología

Aclaraciones generales sobre la metodología (opcional)

- Todo el software y lenguajes de programación que se utilizan en la asignatura están disponibles libre y gratuitamente en internet para el uso e instalación por parte de cualquier alumno. Hay multitud de documentación y materiales didácticos en Internet sobre cada uno de ellos.
- El profesor elabora unos apuntes/presentaciones de la asignatura con toda la teoría que están disponibles en el moodle de la asignatura para descarga del alumno.
- Los ejercicios prácticos de la asignatura están disponibles en el moodle de la asignatura para facilitar su realización a cualquier alumno que no pueda asistir a clases
- Existe un foro de noticias en el moodle de la asignatura para cualquier consulta y el profesor está disponible en su e-mail, teléfono y en horario de tutorías

NOTA: A pesar de que se facilita el trabajo al alumnado a tiempo parcial, esta asignatura está diseñada para un seguimiento presencial por parte del alumno, y la asistencia a todas las clases de teoría y de prácticas es muy recomendable para el correcto seguimiento de la misma.

Adaptaciones metodológicas para alumnado a tiempo parcial y estudiantes con discapacidad y necesidades educativas especiales

Para los estudiantes a tiempo parcial o con necesidades específicas, se tendrá en cuanta su condición y disponibilidad en la asignatura, tanto en el desarrollo de la misma como en su evaluación.
La adaptación del estudiante a tiempo parcial a la asignatura se llevará a cabo de mutuo acuerdo con el profesorado responsable de la misma al inicio del cuatrimestre, debiéndose poner en contacto cada estudiante con el/la profesor/a para indicar su situación.
En casos excepcionales debidamente justificados, los criterios de evaluación podrán ser modificados y adaptados a dichos alumnos, siempre que se garantice la igualdad de derechos y oportunidades entre todos los compañeros.

Actividades presenciales

Actividad	Grupo completo	Grupo mediano	Total
Actividades de acción tutorial	5	-	5
Actividades de evaluación	5	-	5
Actividades de experimentacion práctica	2	22	24
Actividades de exposición de contenidos elaborados	24	2	26
Total horas:	***36***	***24***	***60***

Actividades no presenciales

Actividad	Total
Actividades de búsqueda de información	10
Actividades de procesamiento de la información	40
Actividades de resolución de ejercicios y problemas	40
Total horas:	***90***

Resultados del proceso de aprendizaje

Conocimientos, competencias y habilidades

CB3 Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes en el campo de la Ingeniería Informática para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CTEIS5 Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.

CTEIS6 Capacidad para diseñar soluciones apropiadas en uno o más dominios de aplicación utilizando métodos de la ingeniería del software que integren aspectos éticos, sociales, legales y económicos.

Métodos e instrumentos de evaluación

Competencias	Examen	Medios de ejecución práctica	Producciones elaboradas por el estudiantado
CB3	X	X	X
CTEIS5	X	X	X
CTEIS6	X	X	X
Total (100%)	***60%***	***20%***	***20%***
Nota mínima (*)	***5***	***5***	***5***

(*)Nota mínima (sobre 10) necesaria para que el método de evaluación sea considerado en la calificación final de la asignatura. En todo caso, la calificación final para aprobar la asignatura debe ser igual o superior a 5,0.

Aclaraciones generales sobre los instrumentos de evaluación:

Los alumnos deberán superar un examen final en el que deberán hacer frente a una serie de cuestiones teóricas y/o preguntas de desarrollo. Además se podrán plantear en dicho examen algunos ejercicios teórico-prácticos. El alumno deberá superar este examen para aprobar la asignatura. Independientemente de lo anterior, podrán proponerse al alumno trabajos de investigación o de análisis complementario sobre temática de Seguridad Informática. Si los trabajos tienen el rigor y el nivel adecuado serán considerados en la evaluación final del alumno.
La nota final de la asignatura en actas será la obtenida de forma ponderada según el cuadro anterior.
Estos criterios de evaluación se aplicarán en todas las convocatorias (ordinarias o extraordinarias).

Aclaraciones sobre la evaluación para el alumnado a tiempo parcial y necesidades educativas especiales:

Los alumnos deberán superar un examen final en el que deberán hacer frente a una serie de cuestiones teóricas y/o preguntas de desarrollo. Además se podrán plantear en dicho examen algunos ejercicios teórico-prácticos. El alumno deberá superar este examen para aprobar la asignatura. Independientemente de lo anterior, podrán proponerse al alumno trabajos de investigación o de análisis complementario sobre temática de Seguridad Informática. Si los trabajos tienen el rigor y el nivel adecuado serán considerados en la evaluación final del alumno.
La nota final de la asignatura en actas será la obtenida de forma ponderada según el cuadro anterior.

Aclaraciones sobre la evaluación de la convocatoria extraordinaria y convocatoria extraordinaria de finalización de estudios:

Los alumnos deberán superar un examen final en el que deberán hacer frente a una serie de cuestiones teóricas y/o preguntas de desarrollo. Además se podrán plantear en dicho examen algunos ejercicios teórico-prácticos. El alumno deberá superar este examen para aprobar la asignatura. Independientemente de lo anterior, podrán proponerse al alumno trabajos de investigación o de análisis complementario sobre temática de Seguridad Informática. Si los trabajos tienen el rigor y el nivel adecuado serán considerados en la evaluación final del alumno.
La nota final de la asignatura en actas será la obtenida de forma ponderada según el cuadro anterior.

Criterios de calificación para la obtención de Matrícula de Honor:

más de 9 en cada calificación y participación muy activa y muy destacada en la asignatura

Objetivos de desarrollo sostenible

Salud y bienestar
Educación de calidad
Igualdad de género
Industria, innovación e infraestructura
Reducción de las desigualdades
Paz, justicia e instituciones sólidas
Alianzas para lograr los objetivos

Las estrategias metodológicas y el sistema de evaluación contempladas en esta Guía Docente responderán a los principios de igualdad y no discriminación y deberán ser adaptadas de acuerdo a las necesidades presentadas por estudiantes con discapacidad y necesidades educativas especiales en los casos que se requieran.
El estudiantado deberá ser informado de los riesgos y las medidas que les afectan, en especial las que puedan tener consecuencias graves o muy graves (artículo 6 de la Política de Seguridad, Salud y Bienestar; BOUCO 23-02-23).