

GUÍA DOCENTE
INTRODUCCION A LA CIBERSEGURIDAD

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

CURSO 2022-23

Fecha de publicación: 10-07-2022

I.-Identificación de la Asignatura	
Tipo	OBLIGATORIA
Período de impartición	1 curso, 1Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

II.-Presentación
<p>En esta asignatura trataremos la importancia de la ciberseguridad en la actualidad y el contexto en el que se trabaja en este campo en diferentes sectores, escenarios y dominios de aplicación. Para ello, realizaremos una introducción a la Informática que nos permita comprender los aspectos básicos de cualquier sistema informático actual (desde la representación de la información hasta el desarrollo de aplicaciones, pasando por conceptos básicos de estructura y arquitectura de computadores, sistemas operativos, compiladores, redes o Internet).</p> <p>Una vez adquiridos estos conocimientos básicos ya podremos comprender la importancia de la confidencialidad, la integridad, la disponibilidad, el control de acceso y el no repudio así como conocer los conceptos de riesgo, amenaza y vulnerabilidad. Y analizar los más comunes en la actualidad para poder estudiar los distintos tipos de contramedidas, protecciones, controles o salvaguardas que se pueden diseñar y desplegar. Todo esto se estudiará en mucha mayor profundidad en las diferentes asignaturas que componen el plan de estudios del Grado, pero al finalizar el cuatrimestre los estudiantes tendrán una visión global de este campo y habrán adquirido las bases sobre las que se asentarán todas estas asignaturas en el futuro.</p>

III.-Competencias
Competencias Generales

CG4. Capacidad para dirigir y liderar las actividades objeto de los proyectos del ámbito de la informática y la ciberseguridad comprendiendo los criterios de calidad que rigen dichas actividades investigadora y profesional.

CG7. Capacidad para evaluar y asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.

CG8. Capacidad para definir, evaluar y seleccionar contramedidas para la protección de los activos tecnológicos, entendiendo las peculiaridades de los distintos contextos en los que deben desplegarse.

CG15. Capacidad para aplicar conocimientos a su trabajo o vocación de una forma profesional. Capacidad para elaborar y defender argumentos y resolver problemas dentro de su área de estudio.

CG16. Capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CG17. Capacidad para transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CG18. Capacidad para aplicar las habilidades de aprendizaje adquiridas necesarias para emprender estudios posteriores con un alto grado de autonomía.

Competencias Específicas

CE03. Conocer el concepto, marco institucional y jurídico, organización y gestión de la empresa, y en especial de aquellas que operan en el sector de la ciberseguridad.

CE13. Comprender y analizar las implicaciones que para la seguridad tiene desarrollar, desplegar y utilizar aplicaciones y servicios basados en tecnologías de red, incluyendo: Internet, web, comercio electrónico, multimedia, servicios interactivos, redes sociales, computación móvil, Internet de las cosas.

CE16. Conocer el concepto de ciberseguridad y sus pilares fundamentales e implicaciones en un contexto globalizado, tecnológico y conectado como el actual.

CE19. Comprender los algoritmos criptográficos de clave pública y de clave privada más importantes y conocer sus aplicaciones en ciberseguridad.

IV.-Contenido		
IV.A.-Temario de la asignatura		
Bloque	Unidad didáctica	Contenidos
I- Los fundamentos de la Informática y de la Seguridad	1. Bits y bytes	Representación de la información. Código binario, hexadecimal y ASCII. Imágenes y gráficos. ¿Qué es la criptografía? Esteganografía.
	2. La arquitectura de un computador	Tipos de computador. Modelo Von Neumann. Procesador, memoria y sistema de E/S. Lenguaje ensamblador.
	3. ¿Qué es la ciberseguridad?	Los pilares de la ciberseguridad: confidencialidad, integridad y disponibilidad. Conceptos de riesgo, amenaza y vulnerabilidad. Arquitecturas y principios de ciberseguridad. Contexto actual y escenarios.
II- Sistemas, aplicaciones y personas	4. El sistema operativo	Servicios del sistema operativo. Sistemas operativos actuales y evolución. Virtualización. Protección proporcionada por el sistema operativo. Control de accesos y autenticación.
	5. Compiladores y lenguajes de programación	El compilador. Necesidad de lenguajes de alto nivel y tipos. Instrucciones y datos. Algoritmos. Desarrollo de aplicaciones.
	6. El factor humano y el económico en ciberseguridad	Amenazas internas. Ingeniería social. Políticas y procedimientos. Modelos de negocio. Marco regulatorio.
III- Redes e Internet	7. Redes de comunicaciones e Internet	Modelos en capas. Pila de protocolos. Tipos de red. Redes de área local e Internet. La arquitectura cliente/servidor. El navegador.
	8. Bases de datos y repositorios de información	Sistemas de información. Sistema de ficheros vs bases de datos. Tipos de bases de datos. ¿Qué es SQL?
	9. Amenazas, ciberataques y protecciones	Principales amenazas en la actualidad. Tipos de atacante. Anatomía de un ataque. Incidentes y gestión de incidentes. Protecciones, contramedidas y salvaguardas.

	10. Privacidad y anonimato	Concepto de privacidad. Relación de la privacidad con la seguridad. Privacidad desde el diseño y en el despliegue. Técnicas de anonimato.
--	----------------------------	---

IV.B.-Actividades formativas	
Tipo	Descripción
Prácticas / Resolución de ejercicios	Práctica 1 - Bloque I de la asignatura
Prácticas / Resolución de ejercicios	Práctica 2 - Bloque II de la asignatura
Prácticas / Resolución de ejercicios	Práctica 3 - Bloque III de la asignatura
Otras	Evaluación continua- resolución de casos prácticos y pruebas

V.-Tiempo de Trabajo	
Clases teóricas	20
Clases prácticas de resolución de problemas, casos, etc.	18
Prácticas en laboratorios tecnológicos, clínicos, etc.	18
Realización de pruebas	4
Tutorías académicas	10
Actividades relacionadas: jornadas, seminarios, etc.	8
Preparación de clases teóricas	30
Preparación de clases prácticas/problemas/casos	32
Preparación de pruebas	40
Total de horas de trabajo del estudiante	180

VI.-Metodología y plan de trabajo		
Tipo	Periodo	Contenido
Lecturas	Semana 1 a Semana 15	Apoyo en las clases teóricas y prácticas (noticias de actualidad, documentación introductoria, manuales, etc.)
Prácticas	Semana 4 a Semana 7	Práctica 2 - En grupo, asistencia obligatoria
Prácticas	Semana 8 a Semana 14	Práctica 3 - En grupo, asistencia obligatoria
Tutorías académicas	Semana 1 a Semana 15	Tutorías individuales/grupales acerca de todo el temario de la asignatura
Seminarios	Semana 1 a Semana 15	Jornadas o seminarios de interés para la asignatura
Clases Teóricas	Semana 1 a Semana 14	Contenidos teóricos de las unidades didácticas del programa de la asignatura
Prácticas	Semana 1 a Semana 3	Práctica 1 - En grupo, asistencia obligatoria
Pruebas	Semana 1 a Semana 15	Evaluación continua (resolución de casos prácticos y pruebas según se vaya avanzando en las unidades didácticas)

VII.-Métodos de evaluación

VII.A.-Ponderación para la evaluación

Evaluación ordinaria continua:

La distribución y características de las pruebas de evaluación son las que se describen a continuación. Solo en casos excepcionales y especialmente motivados, el profesor podrá incorporar adaptaciones en la Guía. Dichos cambios requerirán, previa consulta al Responsable de la Asignatura, la autorización previa y expresa del Coordinador de Grado, quien notificará al Vicerrectorado con competencias en materia de Ordenación Académica la modificación realizada. En todo caso, las modificaciones que se propongan deberán atender a lo establecido en la memoria verificada. Para que tales cambios sean efectivos, deberán ser debidamente comunicados a comienzo de curso a los estudiantes a través del Aula Virtual.

La suma de las actividades no revaluables no podrá superar el 50% de la nota de la asignatura y, en general, no podrán tener nota mínima (salvo en el caso de las prácticas de laboratorio o prácticas clínicas, cuando esté debidamente justificado), evitando incorporar pruebas que superen el 60% de la ponderación de la asignatura.

Evaluación extraordinaria: Los estudiantes que no consigan superar la evaluación ordinaria, o no se hayan presentado, serán objeto de la realización de una evaluación extraordinaria para verificar la adquisición de las competencias establecidas en la guía, únicamente de las actividades de evaluación revaluables.

Descripción de las pruebas de evaluación y su ponderación

Actividad de evaluación continua	Re-evaluable (podrá evaluarse en la convocatoria extraordinaria)	Ponderación	Pruebas	Nota mínima	Contenidos	Fecha
Pruebas escritas: Cuestiones de respuesta abierta	Sí, mediante una prueba con el mismo formato	40%	1	5	Todo el temario de la asignatura	Periodo de exámenes de la ETSII según calendario académico
Resolución de casos prácticos	Sí, mediante la entrega de los mismos casos	20% (cada caso un 10%)	2	4	Caso 1: Ética Caso 2: Factor humano	Semana 6 Semana 10
Prácticas con ordenador: Tests/informes y entrega/discusión de resultados	Sí, mediante la realización de las mismas prácticas	40% (un 10% las prácticas 1 y 2, el 20% restante la práctica 3)	3	4	Práctica 1: Bloque I del temario Práctica 2: Bloque II del temario Práctica 3: Bloque III del temario	Semanas 1-3 Semanas 4-7 Semanas 8-14
TOTAL		100%				

Se exigirá la nota mínima indicada en cada una de las partes para hacer media y poder aprobar la asignatura (nota media igual o superior a 5).

Las entregas de soluciones de casos y memorias de prácticas se realizará siempre a través de Aula Virtual, el resto de pruebas serán siempre presenciales. Las fechas concretas se anunciarán en el calendario de Aula Virtual con antelación suficiente.

Nota sobre las actividades

Si el estudiante debe presentarse a la convocatoria extraordinaria para re-evaluar alguna de las actividades de la tabla anterior (para llegar a las notas mínimas), se le guardará la nota de las que ya la hayan superado. No es posible presentarse a "subir nota" en ningún caso.

Normativa aplicable a la realización de las pruebas

En todas las pruebas de evaluación será necesario que el estudiante disponga de documentación identificativa (DNI, pasaporte, permiso de conducir o carnet de estudiante de la URJC) que le podrá ser requerida en cualquier momento. El estudiante se compromete a entregar siempre una solución propia y original así como a incluir, cuando se estime necesario, las referencias bibliográficas y las fuentes consultadas. El plagio total o parcial de las soluciones, o cualquier otro tipo de fraude académico, se penalizará aplicando la normativa de la URJC y se notificará a la ETSII.

VII.B.-Evaluación de estudiantes con dispensa académica de asistencia a clase

Para que un alumno pueda optar a esta evaluación, tendrá que obtener la 'Dispensa Académica de asistencia a clase' para la asignatura, que habrá solicitado al Decano/a o Director/a del Centro que imparte su titulación. La Dispensa Académica se podrá conceder siempre y cuando las peculiaridades propias de la asignatura lo permitan. Una vez que se haya notificado la concesión de la Dispensa Académica, el docente deberá informar al estudiante a través del Aula Virtual acerca del plan de evaluación establecido en cada caso.

Asignatura con posibilidad de dispensa: Si

VII.C.-Revisión de las pruebas de evaluación

Conforme a la normativa de reclamación de exámenes de la Universidad Rey Juan Carlos.

VII.D.-Estudiantes con discapacidad o necesidades educativas especiales

Las adaptaciones curriculares para estudiantes con discapacidad o con necesidades educativas especiales, a fin de garantizar la igualdad de oportunidades, no discriminación, la accesibilidad universal y la mayor garantía de éxito académico serán pautadas por la Unidad de Atención a Personas con Discapacidad en virtud de la Normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.

Será requisito para ello la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que los estudiantes con discapacidad o necesidades educativas especiales deberán contactar con ella, a fin de analizar conjuntamente las distintas alternativas.

VII.E.-Conducta Académica, integridad y honestidad académica

La Universidad Rey Juan Carlos está plenamente comprometida con los más altos estándares de integridad y honestidad académica, por lo que estudiar en la URJC supone asumir y suscribir los valores de integridad y la honestidad académica recogidos en el Código Ético de la Universidad (<https://www.urjc.es/codigoetico>). Para acompañar este proceso, la Universidad dispone de la Normativa sobre conducta académica de la Universidad Rey Juan Carlos (https://urjc.es/images/Universidad/Presentacion/normativa/Normativa_conducta_academica_URJC.pdf) y de diferentes herramientas (antiplagio, supervisión) que ofrecen una garantía colectiva para el completo desarrollo de estos valores esenciales.

VIII.-Recursos y materiales didácticos	
Bibliografía	
"Computing". Yoshihide Igarashi; Tom Altman; Mariko Funada; Barbara Kamiyama, Chapman and Hall/CRC (2014). ISBN: 978-1-4822-2741-3. Disponible en la plataforma de O'Reilly.	
"Computer Security Fundamentals, Third Edition". Chuck Easttom. Pearson Certification (2016). ISBN: 978-0-13-447062-7. Disponible en la plataforma de O'Reilly.	
"Computer & Internet Security: A Hands-on Approach, 3rd Edition". Wenliang Du (2019). ISBN: 978-17330039-4-0.	
Bibliografía de consulta	
Se proporcionarán enlaces a blogs, noticias, artículos, estándares, manuales y otros documentos de interés para las diferentes actividades que se realicen en la asignatura. Todo estará disponible a través del Aula Virtual.	

IX.-Profesorado	
Nombre y apellidos	MARTA BELTRAN PARDO
Correo electrónico	marta.beltran@urjc.es
Departamento	Ciencias de la Computación, Arquitectura de Computadores, Lenguajes y Sistemas Informáticos y Estadística e Investigación Operativa
Categoría	Titular de Universidad
Titulación académica	Doctor
Responsable Asignatura	Si
Horario de Tutorías	Para consultar las tutorías póngase en contacto con el/la profesor/-a a través de correo electrónico
Nº de Quinquenios	4
Nº de Sexenios	2
Nº de Sexenios de transferencia	0
Tramo Docencia	5
Nombre y apellidos	
MIGUEL CALVO MATALOBOS	
Correo electrónico	miguel.calvo@urjc.es
Categoría	Profesional
Responsable Asignatura	No
Horario de Tutorías	Para consultar las tutorías póngase en contacto con el/la profesor/-a a través de correo electrónico

Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Tramo Docencia	0