GUÍA DOCENTE 2021-2022

SEGURIDAD INFORMÁTICA

1. Denominación de la asignatura:

SEGURIDAD INFORMÁTICA

Titulación

Grado en Ingeniería Informática

Código

6370

2. Materia o módulo a la que pertenece la asignatura:

SISTEMAS OPERATIVOS, SISTEMAS DISTRIBUIDOS Y REDES

3. Departamento(s) responsable(s) de la asignatura:

INGENIERÍA INFORMÁTICA

4.a Profesor que imparte la docencia (Si fuese impartida por mas de uno/a incluir todos/as) :

JOSÉ MANUEL SÁIZ DIEZ; IGNACIO PARDO AGUILAR

4.b Coordinador de la asignatura

JOSÉ MANUEL SÁIZ DIEZ

5. Curso y semestre en el que se imparte la asignatura:

Curso: 3 – Semestre: 6

6. Tipo de la asignatura: (Básica, obligatoria u optativa)

Obligatoria

7. Número de créditos ECTS de la asignatura:

6

8. Competencias que debe adquirir el alumno/a al cursar la asignatura

CG1: Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas. CG2: Capacidad para dirigir las actividades objeto de los proyectos del ámbito de la informática. CG3: Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan. CG4: Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas. CG5: Capacidad para concebir, desarrollar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. CG6: Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes. CG7: Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento. CG8: Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones. CG9: Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática. CG10: Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos de informática. IS5: Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse. SI2: Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente. SI5: Capacidad para comprender los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación. CT1: Capacidad de análisis y síntesis.

CT2: Capacidad de organización y planificación.
CT3: Comunicación oral y escrita en la lengua nativa.
CT4: Conocimiento de una lengua extranjera.
CT5: Conocimientos de informática relativos al ámbito de estudio.
CT6: Capacidad de gestión de la información.
CT7: Resolución de problemas.
CT8: Toma de decisiones.
CT9: Trabajo en equipo.
CT12: Habilidades en las relaciones interpersonales.
CT14: Razonamiento crítico.
CT15: Compromiso ético.
CT16: Aprendizaje autónomo.
CT17: Adaptación a nuevas situaciones.
CT18: Creatividad.
CT19: Liderazgo.
CT21: Iniciativa y espíritu emprendedor.
CT22: Motivación por la calidad.
CT24: Comunicarse con personas expertas y no expertas en la materia.
CT25: Elaborar y defender argumentos dentro del ámbito de la Informática.
CT26: Desarrollar habilidades de aprendizaje para emprender estudios posteriores con un alto grado de autonomía.
CT27: Planificación y gestión del tiempo.

9. Programa de la asignatura

9.1- Objetivos docentes
Los objetivos a desarrollar serán: introducir la problemática de la seguridad como elemento básico en el entorno informático, analizar la seguridad en ordenadores personales, sistemas operativos, redes e Internet, analizar y planificar los riesgos y planes de contingencia, introducir las técnicas y productos para la seguridad y analizar el ámbito legal y ético de la seguridad informática.
9.2- Unidades docentes (Bloques de contenidos)
1. Introducción a la problemática de la seguridad informática . **2. Seguridad Física.**

3. Seguridad en Ordenadores Personales.

4. Seguridad en Sistemas Operativos.

5. Virus y otras amenazas programadas.

6. Criptografía.

7. Seguridad en Redes e Internet.

8. Análisis y Planificación de Riesgos.

9. Técnicas y productos para la Seguridad.

10. Ámbito legal y ético en relación con la Seguridad Informática.

9.3- Bibliografía

BIBLIOGRAFÍA BÁSICA

1. Jorge Ramió Aguirre., 1. Curso de Seguridad Informática y Criptografía, Apuntes, http://www.criptored.upm.es/guiateoria/gt_m001a.htm.

BIBLIOGRAFÍA COMPLEMENTARIA

Amparo Fúster Sabater, Dolores de la Guía Martínez, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muñoz Masque, (2000) Técnicas Criptográficas de protección de datos, 2, Ra-ma ,
Anónimo, (1980) Specifications for DES MODES OF OPERATION, 81,] Federal Information Processing Standards Publication, http://www.itl.nist.gov/fipspubs/fip81.htm.
Anónimo, (1999) DATA ENCRYPTION STANDARD (DES), 46-3, Federal Information Processing Standards Publication , http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.
Anónimo, (2001) ADVANCED ENCRYPTION STANDARD (AES)., 197, Federal Information Processing Standards Publication, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
Anónimo, (1994) 10. Los virus informáticos. Qué son, Cómo actúan y cómo combatirlos, 10. Multimedia Ediciones S.A.,
Anónimo, (2000) Edición Especial Linux. Máxima Seguridad, Prentice Hall.,
B. Schneier, (1996) Applied Cryptography, 2, John Wiley & Sons,
Bellovin S. y Cheswick B. , (1994) Firewalls and Internet Security, Addison-Wesley,
C.P. Pfleeger, (1997) Security in Computing, 2, Prentice Hall,
Chapman B. y Zwicky E.D., (1995) Building Internet Firewalls, 2, Prentice Hall,
D. Bell and L. La.Pa.dula, (1975) Secure Computer Systems: Unified Exposit,ion and hZultics Interpretation, MITRE, Bed- ford, Mass,

D. Russell y G.T. Gangemi, (1991) Computer Security Basics, 1. O'Reilly & Associates,
Department of defense standard, Orange Book. Trusted computer system evaluation criteria, Department of defense standard,
Edison Castaño, Dario Melo, Juan Pablo Garzón Ruiz y Andres Gonzalez, (2003) El Modelo de Seguridad Biba, Universidad de los Andes, Bogotá, Colombia,
Fred B. Schneider, Cryptosystem Design and AES, Sin editar, http:// www.cs.cornell.edu/Courses/cs513/2002fa/L23a.html.
Gil Valera J. , (1997) Estudio de Técnicas de Criptografía Aplicadas a las Comunicaciones, Fac. Informática. U. Murcia,
J.M. Morat, A. Ribagorda y J. Sancho, (1994) Seguridad y Protección de la Información, Centro de Estudios Ramón Areces,
José Lucena López, (2003) Criptografía y Seguridad en Computadores, 3, UNED,
José Pastor Franco, Miguel Ángel Sarasa López, (1998) Criptografía digital. Fundamentos y aplicaciones, 2, Prensas Universitarias de Zaragoza. ,
S. Garfinkel y G. Spafford, (1996) Practical UNIX and Internet Security, 2, S. Garfinkel y G. Spafford. O'Reilly & Associates,

10. Metodología de enseñanza y aprendizaje y su relación con las competencias que debe adquirir el estudiante:

Metodología	Competencia relacionada	Horas presenciales	Horas de trabajo	Total de horas
Clases teóricas	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10, IS5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19, CT21, CT22, CT24, CT25, CT26, CT27	25	52	77
Clases prácticas (pequeño grupo)	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10, IS5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8,	26	40	66

	CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19, CT21, CT22, CT24, CT25, CT26, CT27			
Exposiciones públicas	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10, IS5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19, CT21, CT22, CT24, CT25, CT26, CT27	1	2	3
Tutorías	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10, IS5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19, CT21, CT22, CT24, CT25, CT26, CT27	0	0	0
Realización de trabajos, informes, memorias	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10, IS5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19, CT21, CT22, CT24, CT25, CT26, CT27	0	2	2
Pruebas de evaluación	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9,	2	0	2

	CG10, IS5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19, CT21, CT22, CT24, CT25, CT26, CT27			
Total		54	96	150

11. Sistemas de evaluación:

Para superar la asignatura se deben superar tanto la parte de Prácticas como el Examen de teoría y los Entregables con al menos el 50% de su valoración.
Además se valorarán todas las aportaciones realizadas a través de la Participación en el Aula, Tutorías, Seminarios, Informes y Foros. Y esas valoraciones se tomarán como mejoras de nota y se sumarán al 100% de la nota calculada a partir de los otros procedimientos.

La recuperación de las diferentes partes se hará a través de los mismos procedimientos de evaluación para la prueba final, la entrega de prácticas de laboratorio y los entregables.

Procedimiento	Peso primera convocatoria	Peso segunda convocatoria
Entregables; Seminarios, Informes y Foros (Evaluable cuando proceda); Otras Aportaciones	20 %	20 %
Prácticas	40 %	40 %
Examen final de teoría	40 %	40 %
Total	**100 %**	**100 %**

Evaluación excepcional:

- Examen de teoría (40%)
- Realización de las prácticas propuestas durante el curso (40%)
- Realización de entregables (20%)

12. Recursos de aprendizaje y apoyo tutorial:

Pizarra y Proyectores
Páginas Webs relacionadas
Bibliografía disponible en la Biblioteca
Aplicaciones para ejercitar los contenidos de la materia.
Tutorías individualizadas o en grupo a demanda de los alumnos
El material dedicado a la docencia se hará público desde el comienzo del curso: Material de prácticas y guiones, aplicaciones, transparencias y otros ficheros en Internet

13. Calendarios y horarios:

El calendario aprobado por la Junta de Escuela de la Escuela Politécnica Superior y los horarios publicados en los tablones oficiales de la E.P.S.

14. Idioma en que se imparte:

Español

MODELO PARA RECOGER LAS ADAPTACIONES/ADENDAS DE LAS GUÍAS DOCENTES 2021-2022		
TITULACIÓN	Grado en Ingeniería Informática	
CURSO	3º	
ASIGNATURA / CÓDIGO	Seguridad Informática / 6370	
SEMESTRE (1.º/2.º)	2º	
TIPO DE ASIGNATURA Y CRÉDITOS	Obligatoria	6 créditos
COORDINADOR/A	José Manuel Sáiz Diez	
PROFESORADO	José Manuel Sáiz Diez	

CAMBIOS EN LA METODOLOGÍA DE ENSEÑANZA Y APRENDIZAJE RESPECTO A LA GUÍA INICIALMENTE APROBADA PARA UN CONTEXTO DE PRESENCIALIDAD

1. Por razones de reorganización de espacios y tiempos (paso del escenario A al B) <u>para aquellas materias que proceda</u>

<u>NO PROCEDE</u>

2. Ante un eventual rebrote de la enfermedad con paso al escenario C, <u>para todas las materias</u>

Todas las clases teóricas y prácticas se realizarán mediante videoconferencias, material de trabajo online y/o mediante vídeos grabados por los docentes que se pondrán a disposición de los alumnos.

La realización de trabajos, informes, memorias y pruebas de evaluación se realizarán mediante las herramientas que la Universidad de Burgos pone a nuestra disposición a través de UBUVirtual, de las herramientas Office 365 (Tales como Teams o Forms), de otras herramientas que ya han demostrado ser útiles y soportar un número elevado de interlocutores como Skype, así como otras que vayan incorporando. También podrán ser utilizadas otras herramientas propuestas por el docente que puedan suponer una alternativa o que puedan dar un valor añadido a la asignatura.

La asignatura de Seguridad Informática está completamente virtualizada en la modalidad online por lo que no habría problemas de adaptación y se podría realizar el cambio con la máxima urgencia sin impactar de forma relevante en el transcurso normal de la docencia.

CAMBIOS EN LA ATENCIÓN TUTORIAL DE LOS ESTUDIANTES:

1. Por razones de reorganización de espacios y tiempos (paso del escenario A al B) <u>para aquellas</u>

materias que proceda

NO PROCEDE

2. Ante un eventual rebrote de la enfermedad con paso al escenario C, para todas las materias

Se realizarán a través de los foros de la asignatura en ubuvirtual y/o por correo electrónico y/o por videoconferencia, en horario acordado para tutorías.

CAMBIOS EN LOS SISTEMAS DE EVALUACIÓN (especifique los nuevos procedimientos y el peso relativo asignado a la calificación)

1. Por razones de reorganización de espacios y tiempos (paso del escenario A al B) para aquellas materias que proceda

NO PROCEDE

2. Ante un eventual rebrote de la enfermedad con paso al escenario C, para todas las materias

Las distintas metodologías de evaluación se realizarán mediante las herramientas que la Universidad de Burgos pone a disposición a través de UBUVirtual, de las herramientas Office 365, así como otras que se vayan incorporando.

Se mantendrán los procedimientos y pesos relativos salvo indicación contraria, en cuyo caso serán publicitados con tiempo suficiente cuando se establezca la eventualidad, adaptándose en cada caso a la nueva temporalidad.

CALENDARIO DE PRUEBAS DE EVALUACIÓN NO PRESENCIAL (las pruebas presenciales se ajustarán al calendario establecido por los centros, pudiendo modificar el mismo si la evaluación no presencial utilizase otros procedimientos)

Se mantendrán los calendarios y horarios propuestos por el centro, salvo indicación contraria y siempre con la publicidad necesaria.

COMENTARIOS