



GUÍA DOCENTE 2022-2023
SEGURIDAD INFORMÁTICA

1. Denominación de la asignatura:

SEGURIDAD INFORMÁTICA

Titulación

Grado de 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 en el curso online (Si fuese impartida por mas de uno/a incluir todos/as) :

JOSÉ MANUEL SÁIZ DIEZ

4.b Coordinador de la asignatura online

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

Jorge Ramió Aguirre, Curso de Seguridad Informática y Criptografía, Apuntes, Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid,,
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, 2ª, 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) 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,
D. Bell and L. LaPadula, (1975) Secure Computer Systems: Unified Exposition and



Zultics Interpretation, MITRE, Bedford, 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, O'Reilly & Associates,

9.4- Acceso a la Bibliografía Recomendada desde Leganto

https://leganto.ubu.es/leganto/public/34BUC_UBU/lists?courseCode=6370&auth=SAML

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

Metodología	Competencia relacionada	Horas de trabajo
Actividades autónomas (trabajos y lecturas dirigidas - casos de uso, problemas, informes)	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10, SI5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19, CT21, CT22, CT24, CT25, CT26, CT27	80
Pruebas de seguimiento	CG1, CG2, CG3, CG4, CG5, CG6, CG7, CG8, CG9, CG10, SI5, SI2, SI5, CT1, CT2, CT3, CT4, CT5, CT6, CT7, CT8, CT9, CT12, CT14, CT15, CT16, CT17, CT18, CT19,	25



	CT21,CT22, CT24, CT25, CT26, CT27	
Tutoría individual y grupal, participación en foros y otros medios colaborativos	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	23
Diferentes técnicas expositivas	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	22
Total		150

11. Sistemas de evaluación:

Para superar la asignatura se deben superar tanto la parte de Prácticas como los Cuestionarios de teoría y los Entregables con al menos el 50% de su valoración.

Deberán ser entregadas todas las prácticas propuestas para poder optar a aprobar esta parte. Las prácticas serán evaluadas según los porcentajes establecidos para cada una de ellas y, en caso de no haber sido entregadas la totalidad de las mismas, la nota de esta parte nunca podrá superar la nota mínima necesaria para aprobar.

Además se valorarán todas las aportaciones realizadas a través de la Participación en el Aula Virtual, 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.

También se considerarán las contribuciones originales y/o pactadas con el responsable de la asignatura, de los alumnos, en beneficio de la documentación y material de la asignatura. Estas contribuciones pueden ser correcciones de errores en el material de la asignatura así como cualquier nuevo elemento realizado. Su valoración se sumará a la valoración conseguida a través de las otras tres partes, como en el caso de la Participación en el Aula Virtual, Tutorías, Seminarios, Informes y Foros.



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.

Para la realización de tutorías y exámenes, resulta imprescindible disponer de webcam y micrófono activados. Además, determinadas pruebas de evaluación podrán realizarse mediante videoconferencia (Teams vinculado a la cuenta de alumno de laUBU) y/o requerir validación de identidad mediante el uso de sistemas de reconocimiento facial.

La Universidad de Burgos dispone de herramientas tecnológicas autorizadas para la identificación, seguimiento y grabación visual del alumno durante las pruebas de evaluación. Es decisión de cada uno de los profesores de las distintas materias su uso para garantizar la autoría de la prueba.

El carácter ONLINE de la titulación no implica que no se pueda citar a los alumnos en día y hora determinados para la realización de las pruebas de evaluación.

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

12. Recursos de aprendizaje y apoyo tutorial del curso online:

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. Idioma en que se imparte la asignatura online:

Español