GUÍA DOCENTE
EXPERIENCIA PILOTO DE APLICACIÓN DEL SISTEMA EUROPEO DE CRÉDITOS (ECTS)
UNIVERSIDADES ANDALUZAS

TITULACIÓN: INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

DATOS BÁSICOS DE LA ASIGNATURA

NOMBRE: SEGURIDAD INFORMÁTICA		
CÓDIGO: 918	AÑO DE PLAN DE ESTUDIO: 2004	
TIPO (troncal/obligatoria/optativa): Obligatoria		
Créditos totales (LRU/ECTS): 6	Créditos LRU/ECTS teóricos: 3	Créditos LRU/ECTS prácticos: 3
CURSO: 3º	CUATRIMESTRE(S): 2º	CICLO: 1º

EQUIPO DOCENTE

Responsable / Coordinador de la asignatura:		
NOMBRE: Eloy Rafael Sanz Tapia		
CENTRO/DEPARTAMENTO: Escuela Politécnica Superior / Deporte e Informática		
ÁREA: Lenguajes y Sistemas Informáticos		
CATEGORÍA: Profesor Asociado TP		
HORARIO DE TUTORÍAS:		
Nº DESPACHO: 23.1.50	E-MAIL: esanz@upo.es	TF:
URL WEB:		
NOMBRE: Francisco Javier Duque		
CENTRO/DEPARTAMENTO: Escuela Politécnica Superior / Deporte e Informática		
ÁREA: Lenguajes y Sistemas Informáticos		
CATEGORÍA: Profesor Asociado TP		
HORARIO DE TUTORÍAS:		
Nº DESPACHO: 23.1.50	E-MAIL: fjduqpin@upo.es	TF:
URL WEB:		

LA ASIGNATURA EN EL PROGRAMA FORMATIVO

1. DESCRIPTOR.

Problemática de la seguridad informática. Servicios de seguridad. Análisis de riesgos y planes de contingencia. Seguridad en comunicaciones y redes de ordenadores. Criptografía.

2. UBICACIÓN EN EL PROGRAMA FORMATIVO.

2.1. PRERREQUISITOS:

Ninguno.

2.2. CONTEXTO DENTRO DE LA TITULACIÓN:

La asignatura *Seguridad Informática* se articula como una introducción al amplio campo de la seguridad informática. Los contenidos de la asignatura tocarán cada una de las áreas en las que se ve involucrada la seguridad informática, desde la seguridad en redes y equipos hasta el desarrollo de software junto con fundamentos sobre las técnicas criptográficas y el ámbito legal que la afecta.

2.3. RECOMENDACIONES:

3. LA ASIGNATURA EN LA ADQUISICIÓN DE COMPETENCIAS.

3.1. COMPETENCIAS TRANSVERSALES/GENÉRICAS:

Conocimientos generales básicos.
Solidez en los conocimientos básicos de la profesión.
Habilidades avanzadas en informática.
Capacidad de aprender.

3.2. COMPETENCIAS ESPECÍFICAS:

- ***Cognitivas (Saber):*** Conocer las técnicas y buenas prácticas que permitan el mantenimiento y desarrollo de sistemas de información seguros.

- ***Procedimentales/Instrumentales (Saber hacer):*** Aplicar de forma efectiva las técnicas y buenas prácticas para la securización de sistemas informáticos y ser diestro en el manejo de las herramientas empleadas para tal propósito.

- ***Actitudinales (Ser):*** Ser disciplinado en la aplicación sistemática de medidas de seguridad.

4. OBJETIVOS.

- Conocer y comprender los fundamentos de la seguridad informática.
- Conocer y aplicar de forma efectiva las técnicas y buenas prácticas que garantizan la seguridad en sistemas informáticos.
- Conocer el marco legal relativo a la seguridad informática.

DISTRIBUCIÓN DEL TRABAJO PRESENCIAL.

	Gran Grupo	Grupo de Docencia	Actividades dirigidas (seminarios)
Nº de grupos	1	3	4
Nº de horas	18	20	8
Nº de sesiones	12	10	4

5. METODOLOGÍA.

NÚMERO TOTAL DE HORAS DE TRABAJO DEL ALUMNO: 179

SEGUNDO SEMESTRE: 179 horas de trabajo

Nº de Horas:

- Enseñanzas básicas (Gran Grupo): 18
- Enseñanzas prácticas y de desarrollo (Grupo de Docencia): 20
- Actividades académicas dirigidas (Seminarios-Grupo de Trabajo): 8
- Tutorías especializadas (presenciales o virtuales):
  A) Colectivas:
  B) Individuales:
- Trabajo personal autónomo:
  A) Horas de estudio de enseñanzas básicas: 45
  B) Horas de estudio-preparación de las enseñanzas básicas y de desarrollo: 60
  C) Horas de trabajo personal o en grupo derivadas de las actividades académicas dirigidas: 24
- Otras actividades (visitas, excursiones, etc.)
- Realización de pruebas de evaluación y/o exámenes:
  A) Pruebas de evaluación y/o exámenes escritos: 4
  B) Pruebas de evaluación y/o exámenes orales (control del Trabajo Personal):

6. TÉCNICAS DOCENTES. (Señale con una X las técnicas que va a utilizar en el desarrollo de su asignatura. Puede señalar más de una).

Sesiones académicas teóricas: X	Exposición y debate: X	Tutorías especializadas:
Sesiones académicas prácticas: X	Visitas y excursiones:	Controles de lecturas obligatorias:

Otras (especificar):

DESARROLLO Y JUSTIFICACIÓN:

Todas las Actividades Prácticas y de Desarrollo así como las Actividades Académicas Dirigidas llevarán asociada una documentación que se proporcionará al alumno a través de la página web de la asignatura dentro del aula virtual WebCT.

7. BLOQUES TEMÁTICOS. (Dividir el temario en grandes bloques temáticos; no hay número mínimo ni máximo).

- BLOQUE 1: Fundamentos
- BLOQUE 2: Ámbitos de la Seguridad
- BLOQUE 3: Desarrollo de Sistemas Seguros
- BLOQUE 4: Buenas Prácticas y Marco Legal

8. BIBLIOGRAFÍA.

8.1 GENERAL:

- Seguridad en Redes. William Stallings. Prentice Hall
- Fundamentos de Seguridad en Redes. Aplicaciones y estándares (segunda edición). William Stallings. Pearson Educación, 2004
- Cryptography and Network Security, 4th edition. William Stallings. Prentice Hall, 2006
- Computer Security: Principles and Practice. William Stallings. Prentice Hall, 2008
- Seguridad Práctica en Unix e Internet, 2nd Edition. Simson Garfinkel, Gene Spafford. McGraw Hill, 1999
- Seguridad de Servidores Linux. De Bauer, Michael D. Anaya Multimedia-Anaya Interactiva, 2005.
- Seguridad Informática para la Empresa Y Particulares. Alvarez Marañon, Gonzalo y Perez Garcia, Pedro P.McGraw-Hill, 2004.
- Software Libre: Herramientas de Seguridad. Howlett, Tony. Anaya Multimedia-Anaya Interactiva, 2005.
- Seguridad de Redes Locales (Guia Práctica). Gutierrez, Juan Diego Y Lopez Guisado, Angel. Anaya Multimedia-Anaya Interactiva, 2008.

8.2 ESPECÍFICA: (con remisiones concretas en lo posible)

Tema 1: Introducción y Conceptos Básicos

- Seguridad en Redes Telemáticas. Justo Carracedo Gallardo. McGraw-Hill
- Seguridad informática para empresas y particulares. Gonzalo Álvarez Marañón. McGraw-Hill
- Seguridad de la Información. Vicente Aceituno Canal. Creaciones Copyright
- Prevención y Detección de delitos informáticos. Debra Littlejohn Shinder. Anaya Multimedia.
- Seguridad en Internet. Gonzalo Asensio. Editorial Nowtilus.
- HACKER. Jimeno García, María Teresa ; Míguez Pérez, Carlos ; Matas García, Abel Mariano ; y otros. Anaya Multimedia

Tema 2: El ciclo de la Seguridad

- ISO/IEC 27001:2005: Information technology -- Security techniques -- Information security management systems -- Requirements. International Organization for Standardization (ISO).
- ISO/IEC 27002:2005: Information technology -- Security techniques -- Code of practice for information security management. International Organization for Standardization (ISO).
- http://www.csi.map.es/csi/pg5m20.htm
- http://www.ar-tools.com/index.html
- http://www.arcert.gov.ar/politica/
- http://www.unal.edu.co/seguridad/instructivos.htm
- http://www.sans.org/resources/policies/#primer

- http://www.sans.org/resources/policies/#template

Tema 3: Aspectos Organizativos
- http://www.arcert.gov.ar/politica/
- http://www.sans.org/resources/policies/#primer
- http://www.unal.edu.co/seguridad/instructivos.htm
- http://www.microsoft.com/spain/technet/recursos/articulos/srsgch03.mspx
- http://dban.sourceforge.net/

Tema 4: Seguridad Física y del Entorno
- http://es.tldp.org/Manuales-LuCAS/doc-como-seguridad-fisica/COMO-seguridad-fisica.html

Tema 5: Seguridad en Equipos
- Hackers 4. Stuart McClure, Joel Scambray, George Kurtz. McGraw-Hill Interamericana, 2003
- http://windowsupdate.microsoft.com/
- http://update.microsoft.com/microsoftupdate
- http://v4.windowsupdate.microsoft.com/catalog/es/default.asp
- http://www.microsoft.com/latam/technet/articulos/tn/2007/ago-14.mspx
- http://www.jasonn.com/turning_off_unnecessary_services_on_windows_xp
- http://labmice.techtarget.com/articles/securingwin2000.htm
- http://www.securewin.net/
- http://linuxhelp.blogspot.com/2005/12/concise-apt-get-dpkg-primer-for-new.html
- http://www.sans.org/score/checklists/linuxchecklist.pdf
- http://www.bastille-linux.org/

Tema 6: Seguridad en Redes
- Seguridad de Redes. Chris McNab. Anaya Multimedia.
- Seguridad de Redes. Los mejores trucos. Andrew Lockhart. Anaya Multimedia.
- Building Internet Firewalls, 2nd edition. Elizabeth D. Zwicky, Simon Cooper D. Brent Chapman. O'Reilly, 2000.
- http://www.netfilter.org/documentation/
- http://es.tldp.org/Manuales-LuCAS/doc-seguridad-tcpip/

Tema 7: Control de Acceso
- http://www.authenticationworld.com/
- http://psynch.com/docs/password-managementbest-practices.html
- https://www.prime-project.eu/tutorials/gpto/

Tema 8: Desarrollo Seguro
- http://www.owasp.org

Tema 9: Criptografía

- Seguridad en redes telemáticas. Justo Carracedo Gallardo. McGraw-Hill.
- Técnicas Criptográficas de protección de datos. Amparo Fúster Sabater, Dolores de la Guía Martínez, Fausto Montoya Vitini y Jaime Muñoz Masquí. Editorial RA-MA, 1997.
- Introducción a la Criptografía, 2ª edición actualizada. Pino Caballero Gil. Editorial RA-MA
- http://en.wikipedia.org/wiki/Substitution_cipher
- http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
- http://en.wikipedia.org/wiki/Transposition_cipher
- http://www.aci.net/kalliste/des.htm
- http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsechtml/node314.html
- http://en.wikipedia.org/wiki/Deep_Crack
- http://www.aci.net/kalliste/des.htm
- http://people.eku.edu/styere/Encrypt/JS-DES.html
- http://en.wikipedia.org/wiki/Data_Encryption_Standard

- http://celtickane.com/programming/code/DESEncrypt001.cpp
- http://www.hispasec.com/unaaldia/708
- http://en.wikipedia.org/wiki/Rc4
- http://en.wikipedia.org/wiki/Public_key
- http://en.wikipedia.org/wiki/Diffie-Hellman
- http://en.wikipedia.org/wiki/RSA
- http://www.gax.nl/wiskundePO/
- http://www.dia.unisa.it/research/grace/
- Usando Infraestructura PKI para implementar FIRMA DIGITAL www.linti.unlp.edu.ar/publicaciones/2000/firmadig.pdf

Tema 10: Gestión de Incidentes de Seguridad

- NIST Computer Security Incident Handling Guide (800-61): http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- CERT - Computer Emergency Response Team: http://www.cert.org/
- NIST IT Contingency Planning Guide (800-34): http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

Tema 11: Continuidad

- http://support.microsoft.com/kb/814583/es
- http://en.wikipedia.org/wiki/Crontab
- https://help.ubuntu.com/community/CronHowto
- http://bacula.org/en/
- http://vtroger.blogspot.com/2006/03/excelente-herramienta-de-copiasde.html
- http://crysol.inf-cr.uclm.es/node/400
- http://vtroger.blogspot.com/2006/03/excelente-herramienta-de-copiasde.html
- http://www.vicente-navarro.com/blog/2008/01/13/backups-con-rsync/
- http://linuxfocus.org/Castellano/March2004/article326.shtml

- http://www.ubuntu-es.org/index.php?q=node/60946
- http://pintucoperu.wordpress.com/2007/11/27/como-realizar-copias-deseguridad-con-rsync/
- http://www.aboutmyip.com/AboutMyXApp/DeltaCopy.jsp

Tema 12: Cumplimiento
- https://www.agpd.es

9. TÉCNICAS DE EVALUACIÓN.

- La evaluación se basará principalmente en los conocimientos adquiridos tanto en clase de teoría como en aula de informática. La participación también será evaluada.
- Para la realización de cualquier prueba evaluable no se permitirá el uso o consulta de documentación, salvo indicación expresa del profesor en convocatoria oficial.

Criterios de evaluación y calificación: (referidos a las competencias trabajadas durante el curso)

La nota oscilará entre 0 y 10 puntos, los cuales se acumularán en función de los porcentajes descritos a continuación:

- Enseñanzas básicas: 30%
- Actividades prácticas y de desarrollo: 45%
- Actividades académicas dirigidas: 25%

Para aprobar la asignatura, el alumno debe obtener un mínimo de 3 puntos sobre 10 en cada parte (EB, APD y AAD).

Nota: Título II. Capítulo II. Artículo 14.2 y 14.3 de la Normativa de Régimen Académico y de Evaluación del Alumnado (aprobada en Consejo de Gobierno de la UPO el 18 de julio de 2006): "En la realización de trabajos, el **plagio** y la utilización de material no original, incluido aquél obtenido a través de Internet, sin indicación expresa de su procedencia y, si es el caso, permiso de su autor, podrá ser considerada causa de calificación de **suspenso** de la asignatura, sin perjuicio de que pueda derivar en **sanción académica**.
Corresponderá a la Dirección del Departamento responsable de la asignatura, oídos el profesorado responsable de la misma, los estudiantes afectados y cualquier otra instancia académica requerida por la Dirección del Departamento, decidir sobre la posibilidad de solicitar la apertura del correspondiente **expediente sancionador**".

10. ORGANIZACIÓN DOCENTE SEMANAL. (Sólo hay que indicar el número de horas que a ese tipo de sesión va a dedicar el estudiante cada semana)

SEMANA	Enseñanzas básicas (Gran Grupo) Nº de horas	Enseñanzas básicas y de desarrollo (Grupo de Docencia) Nº de horas	Actividades académicas dirigidas (Seminarios-Grupos de Trabajo) Nº de horas	Visita y excursiones Nº de horas	Tutorías especializadas Nº de horas	Control de lecturas obligatorias Nº de horas	Exámenes	Temas del temario a tratar
Segundo Cuatrimestre								
SEMANA 1 (13-17 feb)	1.5	2						T1 y T2/APD1
SEMANA 2 (20-24 feb)	1.5							T3 T4
SEMANA 3 (27, 28 feb - 2 mar)	1.5	2						T5a/APD2
SEMANA 4 (5-9 mar)	1.5		2					T5b/AAD1
SEMANA 5 (12-16 mar)	1.5	2						T6/APD3
SEMANA 6 (19-23 mar)	1.5	2						T7/APD4
SEMANA 7 (26-30 mar)	1.5	2						T8/APD5
SEMANA 8 (9-14 abr)	1.5		2					T9a/AAD2
SEMANA 9 (16-21 abr)	1.5	2						T9b/APD6
SEMANA 10 (30 abr-1,4 may)	1.5	2						T10/APD7
SEMANA 11 (7-11 may)	1.5		2					T11/AAD3
SEMANA 12 (14-18 may)	1.5	2						T12/APD8
SEMANA 13 (21-25 may)		2						APD9
SEMANA 14 (28 may-1 jun)			2					AAD4
SEMANA 15 (4-7,8 jun)		2						APD10
SEMANAS 16 a 20 (11 jun - 13 jul) Evaluaciones finales							4	

11. TEMARIO DESARROLLADO. (Con indicación de las competencias que se van a trabajar en cada tema).

BLOQUE 1: FUNDAMENTOS

Tema 1: Introducción y Conceptos Básicos

1. Necesidad de la seguridad de la información
2. Seguridad de la información frente a seguridad informática
3. Aspectos de la seguridad

Tema 2: El ciclo de la Seguridad

1. Análisis de Riesgos
2. Gestión de Riesgos
3. Implantación de controles
4. Procesos de seguridad
5. Métricas y evaluación
6. Realimentación y mejora continua
7. Sistemas de gestión de seguridad de la información

Tema 3: Aspectos Organizativos

1. Políticas y organización
2. Gestión de activos
3. Seguridad de personal

BLOQUE 2: ÁMBITOS DE LA SEGURIDAD

Tema 4: Seguridad Física y del Entorno

1. Áreas seguras
2. Seguridad del hardware
3. Gestión de medios

Tema 5: Seguridad en Equipos

1. Configuración segura
2. Protección frente a código malicioso
3. Sistemas de detección de intrusiones en hosts (HIDs)
4. Gestión de actualizaciones

5. Monitorización y registros

Tema 6: Seguridad en Redes

1. Aspectos de la seguridad en redes TCP/IP
2. Cortafuegos: tipos y arquitecturas de despliegue
3. Sistemas de detección de intrusiones (NIDs)
4. Seguridad en redes inalámbricas

BLOQUE 3: DESARROLLO DE SISTEMAS SEGUROS

Tema 7: Control de Acceso

1. Conceptos
2. Principales métodos de control de acceso
3. Buenas prácticas para la gestión de claves
4. Políticas de equipos desatendidos y mesa limpia
5. Registros
6. Sistemas de gestión de identidades y Single Sign-On
7. Network access control (NAC)

Tema 8: Desarrollo Seguro

1. Introducción
2. Principales vulnerabilidades del software
3. Buenas prácticas
4. Herramientas de apoyo al desarrollo seguro

Tema 9: Criptografía

1. Tipos de métodos criptográficos
2. Criptografía de clave privada
3. Criptografía de clave pública
4. Funciones hash
5. Firma electrónica
6. Certificados digitales
7. Infraestructura de clave pública (PKI)
8. Esteganografía

BLOQUE 4: BUENAS PRÁCTICAS Y MARCO LEGAL

Tema 10: Gestión de Incidentes de Seguridad

1. Contactos
2. Procedimientos
3. Análisis forense

Tema 11: Continuidad

1. Conceptos
2. Copias de seguridad
3. Redundancia
4. Sistemas de alta disponibilidad
5. Centros de respaldo

Tema 12: Cumplimiento

1. LOPD
2. LSSI
3. LFE

ACTIVIDADES PRÁCTICAS Y DE DESARROLLO

APD 1: Herramientas para análisis de vulnerabilidades
APD 2: Bastionado Windows
APD 3: Copias de respaldo
APD 4: Cortafuegos personales
APD 5: Criptografía I
APD 6: Criptografía II
APD 7: Gestión de registros
APD 8: Monitorización y estado del sistema
APD 9: Cumplimiento
APD 10: IDS y Honeypots

ACTIVIDADES ACADÉMICAS DIRIGIDAS

AAD 1: Análisis de riesgos y políticas de seguridad

AAD 2: Bastionado de Sistemas Linux
AAD 3: Cortafuegos avanzados y vulnerabilidades software
AAD 4: Estudio de herramientas y técnicas avanzadas

12. MECANISMOS DE CONTROL Y SEGUIMIENTO. (Al margen de los contemplados a nivel general para toda la Experiencia Piloto, se recogerán aquí los mecanismos concretos que los docentes propongan para el seguimiento de cada asignatura).