



**GUÍA DOCENTE DE
SISTEMAS de GESTIÓN de la SEGURIDAD
INFORMÁTICA**

Curso 2011-2012

TITULACION: MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN SISTEMAS HARDWARE Y SOFTWARE AVANZADOS

GUIA DOCENTE DE LA ASIGNATURA: SISTEMAS DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Profesor:

Nombre y apellidos: Antonio Guzmán Sacristán (antonio.guzman@urjc.es)

I.- Identificación de la asignatura

| | |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Tipo | Optativa |
| Materia | Sistemas de Gestión de la Seguridad Informática |
| Período de impartición | Segundo semestre |
| Nº Créditos | 6 |
| Idioma en el que se imparte | Castellano |
| Departamento | Departamento de Arquitectura y Tecnología de Computadores, Ciencias de la Computación e Inteligencia Artificial |
| Asignaturas llave | Ninguna |
| Tasa de éxito | Este dato será incluido por el Vicerrectorado de Profesorado, Titulaciones, Ordenación Académica, Coordinación y Campus |

II.- Presentación

Las redes de comunicaciones y los sistemas de información han llegado a ser en nuestros días un factor esencial para el desarrollo económico y el bienestar social. La informática y las redes telemáticas, fijas y móviles, se están convirtiendo en recursos omnipresentes, actualmente utilizadas por igual en el ocio y en el negocio, configurando lo que se ha dado en llamar la moderna Sociedad de la Información.

Por consiguiente, garantizar la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad en su conjunto. A medida que la Sociedad de la Información va incrementando su importancia para la economía y para los sectores productivos, la seguridad de las infraestructuras y de la información que circula por las mismas se presenta como una prioridad básica.

Esta asignatura responde a esta necesidad de aprender los mecanismos básicos que garanticen la seguridad de la información. Está estructurada en tres grandes bloques. En el primero, se acercan los conceptos básicos de criptografía a quienes no están familiarizadas con las complejidades matemáticas de algoritmos y protocolos criptográficos. Este bloque ayudará a comprender las tecnologías básicas de seguridad dependientes de la criptografía, tales como el cifrado, las firmas digitales, certificación o las infraestructuras de clave pública.

En el segundo bloque se analizan las vulnerabilidades y ataques más importantes que pueden sufrir las aplicaciones actuales, así como las contramedidas que pueden utilizarse para evitarlos o mitigar sus efectos. Además se estudian las herramientas de auditoría de seguridad de aplicaciones más útiles.

El último bloque describe el proceso de un análisis forense en un sistema de información que ha sufrido una intrusión, así como los distintos tipos de informes que un perito puede desarrollar según el incidente, ya sea en derecho laboral, penal o mercantil. Es común que se requiera una pericia independiente, así como asesoramiento en casos de cualquier índole, como son el control empresarial del ordenador usado por el trabajador, descubrimiento y revelación de secretos, amenazas, calumnias o injurias, análisis de plagio en programas informáticos o sabotajes.

III.- Competencias

| | |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Competencias transversales | Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. |
| | Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. |
| | Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. |
| | Que los estudiantes adquirirán una comprensión sistemática en el campo de la Informática y el dominio de las habilidades y métodos de investigación relacionados con dicho campo. |
| Competencias específicas | El alumno comprenderá la vinculación existente entre aspectos propios de la criptografía aplicada y aspectos derivados de las comunicaciones basadas en redes de ordenadores, sistemas operativos y aplicaciones |
| | El alumno será capaz de desarrollar soluciones adecuadas para distintos sistemas a partir de un conocimiento global que debe abarcar el conocimiento de las últimas técnicas hacker, de las últimas contramedidas existentes y de las distintas metodologías para la evaluación del nivel de seguridad. |
| | El alumno será capaz de desarrollar un modelo de evaluación de riesgos para diferentes escenarios. |

IV.- Contenido

IV. A. Temario de la asignatura

| Bloque temático | Unidades | Apartados |
|----------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I.- "Criptografía" | Unidad 1. "Introducción a la criptografía y al criptoanálisis" | Algoritmos clásicos de criptografía Principios de sustitución y transposición Técnicas básicas de criptoanálisis Ataques de fuerza bruta |
| | Unidad 2. "Esquemas criptográficos de clave simétrica" | Propiedades de confusión y difusión Clases de algoritmos de criptografía simétrica: cifrado en bloque y cifrado en flujo Operación del cifrado en bloque: modos de encadenamientos de bloques |
| | Unidad 3. "Esquemas criptográficos de clave pública" | Funciones unidireccionales Ejemplos de cifradores de clave pública RSA Hashes Firma digital Infraestructuras de clave pública Certificados digitales |
| II.- "Seguridad en Aplicaciones" | Unidad 4. "Vulnerabilidades, ataques y contramedidas" | Bugs, Exploits & parches OWASP Top Ten 2010 Técnicas de inyección de código Ataques a ciegas Técnicas de desarrollo seguro |
| | Unidad 5. "Herramientas de auditoría de seguridad" | Escáneres de vulnerabilidades Escáneres de seguridad Informe de resultados |
| III.- "Análisis Forense" | Unidad 6. "Análisis forense" | Introducción al análisis forense El análisis de una intrusión Herramientas Documentación |
| | Unidad 7. "Peritaje Informático" | Extracción y Gestión de evidencias digitales. |

IV. B. Actividades obligatorias (evaluables):

1. Prácticas

| |
|---------------------------------------------------|
| Portafolios Bloque I - Criptografía |
| Portafolios Bloque II – Seguridad en Aplicaciones |
| Portafolios Bloque III – Análisis Forense |

5. Otras

| |
|-----------------------------------------------------------------------------------|
| Examen tipo test/respuestas cortas. Contenidos teórico-prácticos de la asignatura |
|-----------------------------------------------------------------------------------|

V.- Tiempo de trabajo

| | |
|----------------------------------------------------------|------------|
| Clases teóricas | 36 |
| Clases prácticas/de resolución de problemas, casos, etc. | 12 |
| Prácticas en laboratorios tecnológicos, clínicos, etc. | 0 |
| Realización de pruebas | 0 |
| Tutorías académicas | 6 |
| Actividades relacionadas: jornadas, seminarios, etc. | 6 |
| Preparación de clases teóricas | 20 |
| Preparación de clases prácticas/problemas/casos | 35 |
| Preparación de pruebas | 35 |
| Total de horas de trabajo del estudiante | 150 |

VI.- Metodología y plan de trabajo

Clases teóricas y Prácticas/de Resolución de problemas, casos, etc.

| Periodo | Contenidos |
|-----------|----------------------|
| Semana 1 | Bloque I (3 horas) |
| Semana 2 | Bloque I (3 horas) |
| Semana 3 | Bloque I (3 horas) |
| Semana 5 | Bloque II (3 horas) |
| Semana 6 | Bloque II (3 horas) |
| Semana 7 | Bloque II (3 horas) |
| Semana 9 | Bloque III (3 horas) |
| Semana 10 | Bloque III (3 horas) |
| Semana 11 | Bloque III (3 horas) |

Prácticas/de resolución de problemas, casos, etc. (12 horas)

| | |
|-----------|----------------------|
| Semana 4 | Bloque I (4 horas) |
| Semana 8 | Bloque II (4 horas) |
| Semana 12 | Bloque III (4 horas) |

Otras actividades

| Fecha | Contenidos |
|-----------|---------------------------------------------------------------------------|
| Semana 12 | Herramientas para la realización del portafolios del Bloque I (2 horas) |
| Semana 13 | Herramientas para la realización del portafolios del Bloque II (2 horas) |
| Semana 14 | Herramientas para la realización del portafolios del Bloque III (2 horas) |

Pruebas

| Fecha | Contenidos |
|-----------|----------------|
| Semana 14 | Prueba Escrita |



VII.- Métodos de evaluación

VII. A. Ponderación para la evaluación continua

% Mínimo de asistencia a clase: 80%.

| Actividad evaluadora | Tipo | | Ponderación | Periodo | Contenido |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------|-------------|---------------|-----------------------------------------------|
| Prueba Escrita <input checked="" type="checkbox"/> Test | <input checked="" type="checkbox"/> Liberatoria Puntuación mínima (de 1 a 10):...5..... | <input checked="" type="checkbox"/> Reevaluable | 25% | Semanas 14 | Contenidos teóricos de la asignatura Completa |
| Portafolio de criptografía <input checked="" type="checkbox"/> Trabajo Individual | <input checked="" type="checkbox"/> Liberatoria Puntuación mínima (de 1 a 10):...5..... | <input checked="" type="checkbox"/> Reevaluable | 25 % | Semanas 4 y 5 | Unidades 1, 2 y 3 |
| Portafolio de seguridad en Aplicaciones <input checked="" type="checkbox"/> Trabajo Individual | <input checked="" type="checkbox"/> Liberatoria Puntuación mínima (de 1 a 10):...5..... | <input checked="" type="checkbox"/> Reevaluable | 25% | Semana 9 | Unidades 4 y 5 |
| Portafolio de Análisis forense <input checked="" type="checkbox"/> Trabajo Individual | <input checked="" type="checkbox"/> Liberatoria Puntuación mínima (de 1 a 10):...5..... | <input checked="" type="checkbox"/> Reevaluable | 25% | Semana 12 | Unidades 6 y 7 |
| Total | | | 100% | | |

VII. B. Ponderación para la evaluación de alumnos a tiempo parcial

Para que un alumno pueda optar a esta evaluación, tendrá que obtener la "Dispensa Académica" para la asignatura, que habrá solicitado al Decano o Director/a del Centro que imparte su titulación.

La "Dispensa Académica" no excluye de la evaluación continua. Dicha evaluación se acomodará por el profesor, asistido por el coordinador del máster, estableciéndose la adaptación curricular según las características de cada caso concreto.

VII. C. Revisión de las pruebas de evaluación

Estos serán los mecanismos de revisión para las diferentes actividades evaluadoras obligatorias:

| |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Comentarios lecturas e Informes de los temas surgidos en los seminarios – Revisión en tutorías académicas individuales o en grupo a lo largo de todo el cuatrimestre (necesario concertar cita). |
| Resolución de casos – Revisión en el aula durante y tras su realización. |
| Portafolios – Revisión en tutoría académica individual cuando estén disponibles las correcciones (se especificará día y hora). |

VIII.- Recursos y materiales didácticos

General

| | |
|-----------|-----------------------------------------------------------------------------------------------------------------------|
| Título | Técnicas Criptográficas de protección de datos |
| Autor | Amparo Fúster Sabater, Dolores de la Guía Martínez, Fausto Montoya Vitini, Jaime Muñoz Masqué, Luis Hernández Encinas |
| Editorial | Ra-Ma |
| Título | Cómo protegernos de los peligros de Internet |
| Autor | Gonzalo Álvarez Marañón |
| Editorial | Catarata/CSIC |
| Título | Hacking Exposed Computer Forensics, Second Edition: Computer Forensics Secrets & Solutions |
| Autor | Aaron Philipp, David Cowen, Chris Davis |
| Editorial | McGraw-Hill |

Complementaria

| | |
|-----------|-----------------------------------------------|
| Título | Análisis Forense Digital en Entornos Windows. |
| Autor | Juan Garrido Caballero. |
| Editorial | Informatica64 |

Direcciones web de interés

| |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OWASP: http://www.owasp.org/ |
| OWASP Top Ten Project: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project |

IX.- Profesorado

| | |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre y apellidos | Antonio Guzmán Sacristán |
| Horario de tutorías académicas | Martes de 13:00 a 14:00 Miércoles y Jueves de 11.00 a 13.00 |
| Correo electrónico | antonio.guzman@urjc.es |
| Departamento/área de conocimiento | DATCCCIA/Arquitectura y Tecnología de Computadores |
| Categoría | Profesor Contratado Doctor |
| Titulación Académica | Licenciatura en Ciencias (Física) (UAM) Doctorado (URJC) |
| Experiencia Docente | En los tres últimos cursos: Fundamentos de los Computadores (1º de Ingeniería Informática), Fundamentos de los computadores (1º Grado en Ing. Informática Online), Arquitectura de Computadores (3º de Ingeniería Informática), Seguridad Informática (5º de Ingeniería Informática), Arquitecturas para Gráficos y Multimedia (Máster en Informática Gráfica, Sistemas de Gestión de la Seguridad Informática (Máster en Investigación en Sistemas Hardware y Software Avanzados), Diseño y Evaluación de Sistemas de Altas Prestaciones (Máster en Investigación en Sistemas Hardware y Software Avanzados), Simulación (Máster en Sistemas de Información y Comunicaciones para la Defensa). |
| Experiencia profesional | En Octubre del 2000 se incorporó como profesor al Área de Arquitectura y Tecnología de Computadores de la Universidad Rey Juan Carlos de Madrid, en la que en la actualidad sigue desarrollando sus labores docentes e investigadoras, con 200 créditos impartidos en estos últimos 9 cursos, más de 20 publicaciones internacionales e involucrada siempre en multitud de proyectos y colaboraciones con otros grupos y empresas. En este momento integra el grupo de investigación GAAP y sus principales trabajos están relacionados con las arquitecturas de altas prestaciones (clusters, Grids, FPGAs, GPUs y videoconsolas). |