Asignatura: SEGURIDAD Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN (SA-SI)
Código: 32501
Institución: Escuela Politécnica Superior
Programa: Máster Universitario en Ingeniería Informática (ing.inf)
Nivel: Máster
Tipo: Obligatoria
ECTS: 6

GUÍA DOCENTE: SEGURIDAD Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN (SA-SI)

Curso Académico: 2017-2018

Programa: Máster Universitario en Ingeniería Informática (ing.inf)
Centro: Escuela Politécnica Superior
Universidad: Universidad Autónoma de Madrid

Última modificación: 04/05/2016
Estado: Publicado 07/2017

1. ASIGNATURA

Seguridad y auditoría de los sistemas de información (SA-SI)

1.1. Programa

Máster Universitario en Ingeniería Informática (ing.inf)

1.2. Código asignatura

32501

1.3. Área de la asignatura

CCIA/LSI

1.4. Tipo de asignatura

Obligatoria

1.5. Semestre

Segundo semestre

1.6. Créditos

6 ETCS

1.7. Idioma de impartición

El material y transparencias se proporcionarán tanto en inglés/castellano. Las clases se impartirán principalmente en castellano, sin perjuicio a que algunos temas o seminarios pudiesen ser impartidos en inglés.

1.8. Recomendaciones / Requisitos previos

Seguridad y Auditoría de los Sistemas de Información es una asignatura que forma parte de la Materia 1.2: Análisis, diseño y evaluación de software, calidad, certificación, y seguridad de los sistemas informáticos delos estudios del Máster Universitario en Ingeniería Informática (ING-INF), que proporcionan formación en aspectos avanzados de la Ingeniería Informática. Esta asignatura se imparte en el

segundo semestre de este máster oficial. No se establecen requisitos específicos previos para esta asignatura. Sin embargo, se recomienda tener cierta madurez en el uso y comprensión de algoritmos así como su implementación para la cual el alumno precisa disponer de un buen nivel de programación, resultante de las asignaturas de los cursos anteriores en grado. La materia en esta asignatura se complementa con *Fundamentos de Criptografía y Seguridad Informática* de Grado de Ingeniería Informática e *Internet y Redes avanzadas* del Máster Universitario en Ingeniería Informática. Así por tanto, aunque en esta asignatura no se establecen requisitos específicos previos, el haber cursado o estar cursando estas dos asignaturas facilita el proceso de aprendizaje y compresión de la materia en cuestión. El estudio teórico de la asignatura se complementa con el trabajo aplicado en los laboratorios para el desarrollo de las habilidades prácticas, favoreciendo así la comprensión y la conexión con los fundamentos teóricos. Se requiere asimismo iniciativa personal y constancia para desarrollar estas actividades durante el curso. Finalmente, se requiere predisposición y empatía para el trabajo colaborativo en grupo.

Se recomienda para garantizar la asimilación de los contenidos y la adquisición de habilidades la lectura crítica de los textos de la bibliografía, el uso del material electrónico de esta asignatura disponible en la plataforma Moodle (http://uam-virtual.es) y la búsqueda activa de material complementario en la red. Es recomendable disponer de un dominio de inglés que permita al alumno leer la bibliografía de consulta.

1.9. Datos del equipo docente

Nota: se debe añadir @uam.es a todas las direcciones de correo electrónico.

Profesores de teoría y prácticas:

Dr. Francisco de Borja Rodríguez Ortiz (Coordinador)
Departamento de Ingeniería Informática
Escuela Politécnica Superior
Despacho - Módulo: B-328 Edificio B – 3ª Planta
Teléfono: +34 91 497 2236
Correo electrónico: f.rodriguez
Página web: http://www.eps.uam.es/~frodrig
Horario de atención al alumnado: Petición de cita previa por correo electrónico.

Dr. Álvaro Ortigosa
Departamento de Ingeniería Informática
Escuela Politécnica Superior
Despacho - Módulo: B-333 Edificio B – 3ª Planta
Teléfono: +34 91 497 2271
Correo electrónico: alvaro.ortigosa
Página web: http://www.eps.uam.es/~ortigosa
Horario de atención al alumnado: Petición de cita previa por correo electrónico.

Dr. David Arroyo Guardeño
Departamento de Ingeniería Informática
Escuela Politécnica Superior
Despacho - Módulo: B-315 Edificio B – 3ª Planta
Teléfono: +34 91 497 7530
Correo electrónico: david.arroyo
Página web: http://www.davidarroyoguardeno.blogspot.com.es/
Horario de atención al alumnado: Petición de cita previa por correo electrónico.

1.10. Objetivos del curso

Esta asignatura tiene por objetivo que el estudiante comprenda los riesgos de seguridad a los que está sometido un sistema informático y la información manipulada, y sea capaz de diseñar, desarrollar, gestionar y evaluar las medidas de defensa necesarias para minimizar esos riesgos, así como implantar y organizar un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando metodologías y estándares adecuados. Por este motivo se estudiarán los conceptos fundamentales de seguridad moderna; las vulnerabilidades de los sistemas de procesamiento y transferencia de información y de sus usuarios; y el tipo de protecciones y medidas que pueden ser incorporadas para reducir el riesgo en la explotación de las mismas. La asignatura hará especial hincapié en la naturaleza dinámica y evolutiva de los riesgos implicados, y en cómo las soluciones deben adaptarse y evolucionar consecuentemente. Además, para la implantación y organización de SGSI se requiere un conocimiento profundo de las normativas de seguridad vigentes y el empleo de estándares de seguridad informática, cuya implantación requiere conocimientos de técnicas criptográficas y de protocolos de comunicación de red. Aunque la base de la asignatura serán los principios teóricos en los que se sustenta la seguridad informática, se hará mucho énfasis en ejemplos de sistemas reales y aplicaciones prácticas, transmitiendo al estudiante el concepto fundamental de que ningún sistema informático moderno puede ser desarrollado sin considerar los aspectos de seguridad y que la gestión de esta es imprescindible.
La asignatura se ocupará entre otros de los siguientes temas: amenazas y principios de seguridad informática; metodologías para proporcionar seguridad, criptografía y autenticación; seguridad de redes y de sistemas, ataque, defensa y prevención; SGSI,

normativas, estándares, auditoria y certificación; así como, análisis forense y evidencia digital.

Las **competencias** que se persiguen adquirir con esta asignatura son:

***Competencias de formación básica o generales*:**
G2. Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa vigente y asegurando la calidad del servicio.
G3. Capacidad para dirigir, planificar y supervisar equipos multidisciplinares.
G7. Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
G8. Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.

Competencias transversales:
TR4. Capacidad para transmitir de un modo claro y sin ambigüedades a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan. Capacidad para argumentar y justificar lógicamente dichas decisiones de un modo claro y sin ambigüedades, sin dejar de considerar puntos de vista alternativos o complementarios.
TR5. Capacidad para trabajar en equipos o proyectos tecnológicos o de investigación en un contexto internacional y multidisciplinar.

Competencias específicas:
DG3. Capacidad para la dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
TI3. Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.
TI4. Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

A continuación, se especifican los objetivos generales y específicos de la asignatura *Seguridad y Auditoría de los Sistemas de Información* que pretenden alcanzarse.

OBJETIVOS GENERALES	
G1	Conocer las metodologías generales para proporcionar seguridad de

OBJETIVOS GENERALES	
	manera práctica: uso seguro de la criptografía
G2	Conocer las principales amenazas de los sistemas generales de seguridad de información
G3	Conocer los fundamentos y normativas de los sistemas generales de seguridad de información
G4	Conocer las principales técnicas de auditoría y análisis forense de los sistemas generales de seguridad de información

OBJETIVOS ESPECÍFICOS	
UNIDAD 1. Metodologías fundamentales para proporcionar seguridad	
1.1.	Conocer y estudiar las principales primitivas criptográficas para proporcionar seguridad en sistema de información
1.2.	Conocer y entender cómo utilizar de manera práctica varias primitivas criptográficas para generar aplicaciones seguras en sistemas de información
1.3.	Establecer y estudiar los principales protocolos para el uso seguro de las primitivas criptográficas en sistemas de información
1.4.	Conocer y entender cómo utilizar de manera práctica varios protocolos de seguridad para generar aplicaciones seguras en sistemas de información
UNIDAD 2. Control de acceso e identidad en sistemas de información	
2.1.	Conocer los fundamentos de las políticas de acceso a activos de un sistema de información
2.2.	Conocer las principales amenazas y riesgos asociados a las distintas metodologías de control de acceso a los activos de un sistema de información
2.3.	Establecer el grado de dependencia entre los niveles de protección de información y las expectativas de seguridad de los activos de un sistema de información
2.4.	Introducir las metodologías básicas para el registro de operaciones de acceso a información local y de la compartición de activos en un sistema de información
UNIDAD 3. Sistemas de Gestión de la seguridad e Información	
3.1.	Conocer y estudiar la normativa vigente de seguridad española
3.2.	Conocer las metodologías para la implantación de los estándares para la seguridad de los sistemas de información
3.3.	Conocer los sistemas de normalización y certificación que existen para implantar la seguridad en un sistema de información
UNIDAD 4. Seguridad de sistemas	
4.1.	Conocer y entender los principales métodos y herramientas para investigar el estado e historia de uso de los sistemas informáticos y la información que gestionan
4.2.	Conocer los principales métodos existentes para la detección de vulnerabilidades e intrusiones en un sistema informático, así como el análisis de los métodos de ataque a los mismos
4.3.	Conocer y entender el modo de operación del software malicioso, así como los principales métodos de prevención y protección.

4.4.	Entender los principios de funcionamiento de los cortafuegos de aplicación, así como su utilización para complementar la seguridad de los sistemas de información.

Contenidos del programa

Programa Sintético

UNIDAD 1. Metodologías fundamentales para proporcionar seguridad
UNIDAD 2. Control de acceso e identidad en sistemas de información
UNIDAD 3. Sistemas de Gestión de la seguridad e Información
UNIDAD 4. Seguridad de sistemas

Programa Detallado

1. **Metodologías fundamentales para proporcionar seguridad**
   - 1.1. Primitivas criptográficas
     - 1.1.1. Conceptos básicos de criptografía simétrica
     - 1.1.2. Conceptos básicos de criptografía asimétrica y manejo de claves
     - 1.1.3. Ejemplos de implementación de primitivas criptográficas con Java
   - 1.2. Uso seguro de la criptografía: Protocolos criptográficos
     - 1.2.1. Funciones resúmenes: MAC y HASH
     - 1.2.2. Firmas digitales y protocolos de autenticación simétricos y asimétricos
     - 1.2.3. Ejemplos de implementación de protocolos criptográficos con Java

2. **Control de acceso e identidad en sistemas de información**
   - 2.1. Metodologías de control de acceso
     - 2.1.1. Distribución de permisos de acceso a los activos de un sistema de información: "principio de mínimo privilegio"
     - 2.1.2. Registro de operaciones orientadas a subvertir los niveles de acceso y privilegios en un sistema de información
   - 2.2. Identificación de amenazas y riesgos
     - 2.2.1. Protección local de información
     - 2.2.2. Protección de información en tránsito
   - 2.3. Casos de estudio
     - 2.3.1. Implantación de políticas de control de acceso en sistemas Linux
     - 2.3.2. Estudio de ataques basados en desbordamiento de buffer (*Buffer OverFlow* -BOF-)

3. **Sistemas de Gestión de la seguridad e Información**

3.1. LOPD y LSSI: Estudio y análisis de casos de estudio prácticos
3.2. Arquitectura de seguridad OSI: servicios de Seguridad X.800
3.3. Auditorías: ISO/IEC 27001 y CISSP (ISC)^2
    3.3.1. Procesos de certificación, esquemas y sus competencias.

4. Seguridad de sistemas
4.1. Métodos y herramientas fundamentales de uso en auditoría y análisis forense
4.2. Detección de intrusiones
    4.2.1. Detección estática: análisis de vulnerabilidades
    4.2.2. Sistemas de detección de intrusiones (IDSs)
    4.2.3. Honeypots
4.3. Software malicioso (Malware)
    4.3.1. Comprendiendo el malware
    4.3.2. Virus, Gusanos y Troyanos
    4.3.3. Análisis de Malware: técnicas estáticas y dinámicas
4.4. Cortafuegos a nivel de aplicación (WAF)

1.11. Bibliografía

Los recursos para el aprendizaje por unidad se detallan a continuación. Se distinguen entre lecturas básicas y lecturas recomendadas.

1. W. Stallings, “Cryptography and Network Security: Principles and Practice” (Básica).
2. D. Hook, "Beginning Cryptography with Java” (Básica).
3. W. Stallings, L. Brown “Computer Security: Principles and Practice” (Básica).
4. Ross Anderson, “Security Engineering”, (Básica).
5. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography" (Complementaria).
6. Pieprzyk, J., Hardjono, T., Seberry, J., "Fundamentals of Computer Security". (Complementaria)
7. M. Sikorski, A. Honig, “Practical Malware Analysis” (Complementaria)
8. L. Spitzner, “Honeypots – Tracking Hackers” (Complementaria)
9. R. GurleyBace, “Intrusion Detection” (Básica)
10. R. Krutz, R. Dean Vines, “Advanced CISSP Prep Guide” (Complementaria)
11. K. Graves, “Certified Ethical Hacker Study Guide” (Complementaria)
12. G. Álvarez, P. Pérez, Seguridad Informática para empresas y particulares (Complementaria)
13. Michael Hale Ligh, Andrew Case, Jamie Levy. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. (Complementaria).
14. David Kennedy, Jim O’Gorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Tester’s Guide.

1.12. Metodología docente

La metodología utilizada en el desarrollo de la actividad docente incluye los siguientes tipos de actividades:

***Clases de teoría:**

Actividad del profesor

Clases expositivas simultaneadas con la realización de programas y ejercicios. Se utilizará la pizarra, combinada con la explicación en formato electrónico cuya ejecución se visualizará en la pantalla de la clase cuando se requiera.

Actividad del estudiante:

Actividad presencial: Toma de apuntes, participación activa en clase respondiendo a las cuestiones planteadas. Resolución de los ejercicios propuestos y escritura de pequeños programas durante el desarrollo de las clases.

Actividad no presencial: lectura del material bibliográfico y de apoyo, estudio de la materia y realizaciones de los cuestionarios planteados en la plataforma Moodle.

***Clases de problemas/ejercicios en aula:**

Actividad del profesor

Primera parte expositiva, una segunda parte de supervisión y asesoramiento en la resolución de los problemas por parte del alumno y una parte final de análisis del resultado y generalización a otros tipos de problemas. Se utilizará la pizarra y el proyector del aula para visualizar los algoritmos o programas propuestos.

Actividad del estudiante:

Actividad presencial: Participación activa en la resolución de los ejercicios, diseño y escritura de los programas y en el análisis de la ejecución.

Actividad no presencial: Realización de ejercicios y programas, planteados en clase o a través de la plataforma Moodle. Estudio, generalización y planteamiento de modificaciones que permitan la optimización de los programas.

***Tutorías en aula:**

Actividad del profesor:

Tutorización a toda la clase o en grupos de alumnos reducidos (8-10) con el objetivo de resolver dudas comunes plantadas por los alumnos a nivel individual o en grupo, surgidas a partir de cuestiones/ejercicios/programas señalados en clase para tal fin y orientarlos en la realización de los mismos.

Actividad del estudiante:

Actividad presencial: Planteamiento de dudas individuales o en grupo y enfoque de posibles soluciones a las tareas planteadas.

Actividad no presencial: Estudio de las tareas marcadas y debate de las soluciones planteadas en el seno del grupo.

***Prácticas:**

Actividad del profesor:

Asignar una práctica/proyecto a cada grupo de trabajo y explicar la práctica asignada a cada grupo de trabajo al comienzo de la sesión de prácticas. Supervisar el trabajo de los grupos de trabajo en el laboratorio. Suministrar el guion de prácticas a completar en el laboratorio.

Se utilizan el método expositivo tanto en tutorías como en el laboratorio con cada grupo de trabajo. Los medios utilizados son los entornos de programación editores, compiladores y los ordenadores del propio laboratorio para la ejecución y análisis de los programas realizados.

Actividad del estudiante:

Actividad presencial: Planteamiento inicial, previo al desarrollo de la práctica, sobre información contenida en el enunciado. Debate en el seno del grupo sobre el planteamiento de la solución óptima. Al finalizar la práctica se entrega un informe explicando el desarrollo de la práctica y los programas desarrollados y, además, se debe ejecutar con el profesor presente, quien hará las preguntas oportunas a cada miembro del grupo para calificar de forma individual la práctica.

Actividad no presencial: Profundizar en el enunciado de la práctica y plantear el diagrama de flujo óptimo para la resolución de la misma. Redacción del informe de la práctica.

1.13. Trabajo del estudiante

		Nº de horas	Porcentaje
Presencial	Clases teóricas	22 h (14.6%)	47 h (31.3%)
	Clases prácticas	20 h (13.3%)	
	Realización de pruebas escritas parciales y final	5 h (3.3%)	
No presencial	Estudio semanal regulado	29 h (19.3%)	103 h (68.7%)
	Realización de actividades prácticas	36 h (24%)	
	Preparación del examen (convocatoria ordinaria)	20 h (13.4%)	
	Preparación del examen (convocatoria extraordinaria)	18 h (12%)	
Carga total de horas de trabajo: 25 horas x 6 ECTS		**150 h**	

1.14. Métodos de evaluación y porcentaje en la calificación final

La calificación de la asignatura en la **convocatoria ordinaria** se hará en base a diferentes evaluaciones que se realizarán de **manera continuada a lo largo del semestre.** Estas evaluaciones continuas a lo largo del curso estarán compuestas de diversas partes prácticas, teóricas y un proyecto original realizado por el estudiante.

- Las partes, teoría, prácticas y proyecto original se puntúan sobre 10 puntos cada una de ellas.
- La nota final de la asignatura se obtiene de las notas de teoría, prácticas y un proyecto original por medio de la ecuación:

Calificación: 0.4*Prácticas + 0.4*Teoría+0.2*Proyecto Original

- Para aprobar la asignatura es obligatorio obtener una nota mayor o igual a 5 puntos, tanto en la parte de teoría como en las prácticas. En caso contrario, la nota final en actas será

Calificación: (0,4*Mín(5,Prácticas) + 0,4*Mín(5,Teoría) + 0,2*Mín(5, Proyecto Original))

La nota correspondiente a la parte de Teoría es la que resulta del promedio ponderado de las calificaciones en las diferentes pruebas escritas.

Las pruebas escritas, podrán incluir tanto cuestiones teóricas y ejercicios como el diseño y escritura de programas.

- La nota correspondiente a la parte de prácticas es la que resulta de realizar las prácticas programadas en el curso.
  - ✓ Para aprobar la parte práctica el estudiante deberá asistir, al menos, al 85% de las prácticas. En caso contrario deberá realizar unas prácticas que podrán ser de mayor complejidad a las realizadas en el curso. En este último supuesto la nota de prácticas implica la evaluación del material entregado y un examen sobre el trabajo realizado.
  - ✓ La calificación de la parte práctica tendrá en cuenta la calidad de los diseños realizados y el nivel de los resultados obtenidos. También se valorará la validez de los resultados obtenidos en cada uno de los apartados que se hayan establecido para su realización en los guiones de las prácticas.
- La nota de teoría se conserva (convalida) sólo para la convocatoria extraordinaria del mismo curso académico.
- La nota de prácticas se conserva (convalida) sólo para la convocatoria extraordinaria del mismo curso académico.
- La nota del proyecto original se conserva (convalida) sólo para la convocatoria extraordinaria del mismo curso académico.
- Para aquellos estudiantes que deban hacer uso de la **convocatoria extraordinaria** de junio habrá un único examen de la parte de teoría. Además el mismo día del

examen los estudiantes deberán presentar las prácticas de la asignatura y el proyecto original escogido. La ponderación de las tres partes se hará de acuerdo con la misma expresión utilizada en la convocatoria ordinaria.

ATENCIÓN: Cualquier copia descubierta que se haya realizado a lo largo del curso, tanto en cualquiera de las actividades de teoría desarrolladas, como en cualquiera de los apartados de las prácticas, serán penalizadas con rigor.

1.15. Planificación / Cronograma

Semana	Contenido
1	**UNIDAD 1.Metodologías fundamentales para proporcionar seguridad: Tema 1.1**
2	**UNIDAD 1.Metodologías fundamentales para proporcionar seguridad: Tema 1.1**
3	**UNIDAD 1.Metodologías fundamentales para proporcionar seguridad: Tema 1.2**
4	**UNIDAD 1.Metodologías fundamentales para proporcionar seguridad: Tema 1.2**
5	**UNIDAD 2. Control de acceso e identidad en sistemas de información: Tema 2.1**
6	**UNIDAD 2.Control de acceso e identidad en sistemas de información: Tema 2.2**
7	**UNIDAD 2.Control de acceso e identidad en sistemas de información: Tema 2.2**
8	**UNIDAD 2.Control de acceso e identidad en sistemas de información: Tema 2.3**
9	**UNIDAD 3.Sistemas de Gestión de la seguridad e Información**
10	**UNIDAD 4. Métodos y herramientas fundamentales de uso en auditoría y análisis forense: Tema 4.1**
11	**UNIDAD 4. Detección de intrusiones: Tema 4.2**
12	**UNIDAD 4. Software malicioso y Cortafuegos a nivel de aplicación: Temas 4.3 y 4.4**
13	**Intensificación y presentación de proyectos**
14	**Intensificación y presentación de proyectos**