1. Identificación

1.1. De la Asignatura

Curso Académico	2017/2018
Titulación	GRADO EN INGENIERIA INFORMÁTICA
Nombre de la Asignatura	GESTIÓN DE LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN
Código	3888
Curso	CUARTO
Carácter	OPTATIVA
N.º Grupos	1
Créditos ECTS	6
Estimación del volumen de trabajo del alumno	150
Organización Temporal/Temporalidad	Segundo Cuatrimestre
Idiomas en que se imparte	ESPAÑOL
Tipo de Enseñanza	Presencial

1.2. Del profesorado: Equipo Docente

<table>
<tr><td rowspan="8">Coordinación de la asignatura
LORENZO FERNANDEZ MAIMO
Grupo de Docencia: 1
Coordinación de los grupos:1</td><td>Área/Departamento</td><td colspan="4">INGENIERÍA Y TECNOLOGÍA DE COMPUTADORES</td></tr>
<tr><td>Categoría</td><td colspan="4">PROFESORES TITULARES DE ESCUELAS UNIVERSITARIAS</td></tr>
<tr><td>Correo Electrónico / Página web / Tutoría electrónica</td><td colspan="4">lfmaimo@um.es
http://ditec.um.es/personal/8
Tutoría Electrónica: SÍ</td></tr>
<tr><td rowspan="3">Teléfono, Horario y Lugar de atención al alumnado</td><td>Duración</td><td>Día</td><td>Horario</td><td>Lugar</td></tr>
<tr><td>Primer Cuatrimestre</td><td>Martes</td><td>10:30- 12:00</td><td>868884651, Facultad de Informática B1.3.033</td></tr>
<tr><td>Primer Cuatrimestre</td><td>Martes</td><td>17:00- 18:30</td><td>868884651, Facultad de Informática B1.3.033</td></tr>
<tr><td rowspan="4">RAFAEL MENENDEZ-BARZANALLANA ASENSIO
Grupo de Docencia: 1</td><td>Área/Departamento</td><td colspan="4">INFORMÁTICA Y SISTEMAS</td></tr>
<tr><td>Categoría</td><td colspan="4">PROFESORES TITULARES DE ESCUELAS UNIVERSITARIAS</td></tr>
<tr><td>Correo Electrónico / Página web / Tutoría electrónica</td><td colspan="4">barzana@um.es
http://www.um.es/docencia/barzana
Tutoría Electrónica: SÍ</td></tr>
<tr><td rowspan="3">Teléfono, Horario y Lugar de atención al alumnado</td><td>Duración</td><td>Día</td><td>Horario</td><td>Lugar</td></tr>
<tr><td>Anual</td><td>Lunes</td><td>08:00- 11:00</td><td>868884856, Aulario de la Merced B2.1.006</td></tr>
<tr><td>Anual</td><td>Viernes</td><td>16:00- 18:00</td><td>868884856, Aulario de la Merced B2.1.006</td></tr>
</table>

2. Presentación

CONTENIDOS Y OBJETIVOS FORMATIVOS:

Los marcos europeos y mundial.

- Analizar los antecedentes de la seguridad de los sistemas de información, de su marco europeo y mundial así como de su situación en España

Niveles de gestión de seguridad.

- Conocer los distintos modelos escalonados o niveles de gestión de la seguridad de los Sistemas de Información

Metodología de análisis y gestión de riesgos: MAGERIT.

- Conocer los fundamentos y elementos de la Metodología de Análisis y Gestión de Riesgos en Sistemas de Información (MAGERIT) del Ministerio de Administraciones Públicas
- Entender la realización y estructuración de un proyecto de análisis y gestión de riesgos de acuerdo con MAGERIT

Herramientas de soporte de la metodología.

- Manejar la herramienta informática de apoyo a la metodología MAGERIT Procedimiento Informático y Lógico para el Análisis de Riesgos (PILAR) del Centro Criptológico Nacional, para el estudio de un caso de uso y para la realización de un caso práctico de aplicación de la metodología MAGERIT y de utilización de la herramienta informática PILAR

Seguridad de los Sistemas TIC: Políticas, Normalización, Acreditación, Organización y gestión, herramientas.

- Conocer el establecimiento e implantación de una organización de la seguridad como estructura para el mantenimiento y gestión de la seguridad de los sistemas de información, identificar las diferentes actividades y definir las responsabilidades, figuras y roles en la gestión de la seguridad
- Conocer la tipología y clasificación de las herramientas de seguridad existentes
- Revisar los requisitos relativos a la selección, aprobación, implementación, uso y mantenimiento de las herramientas de seguridad en los sistemas de información

Aspectos legales: Legislación: LOPD, delito informático, fraude informático, prueba pericial.

- Abordar el marco legal de la Seguridad Informática, el régimen jurídico de la firma electrónica, de los delitos informáticos y, especialmente, la protección de datos personales y las medidas de seguridad aplicables a ficheros y tratamientos

Respuesta a incidentes.

- Ser capaces de identificar un incidente y establecer los requisitos que debe cumplir un equipo de respuesta a incidentes dentro de la empresa.
- Conocer metolodogías de reacción ante un incidente y las implicaciones que puede tener para la organización.
- Mecanismos de detección de intrusiones y los indicadores de compromiso (IOC).

Informática Forense. Peritajes. Evidencia digital.

- Conocer los objetivos de la informática forense, las metodologías que utiliza y los procedimientos técnicos y legales
- El papel del perito. Informe pericial
- Conocer los detalles de bajo nivel que son de importancia a la hora de enfrentarse a un escenario forense
- Extraer de forma adecuada las evidencias digitales por medio de herramientas forenses aplicadas a pequeños retos prácticos, fundamentalmente en sistemas operativos Windows.

3. Condiciones de acceso a la asignatura

3.1 Incompatibilidades

No consta

3.2 Recomendaciones

Para la parte de informática forense, se recomienda un conocimiento básico de sistemas de ficheros y administración de sistemas operativos.

4. Competencias

4.1 Competencias Básicas

No disponible

4.2 Competencias de la titulación

· CGUM6. Capacidad para trabajar en equipo y para relacionarse con otras personas del mismo o distinto ámbito profesional.
· CGII1. Capacidad de análisis y síntesis.
· CGII2. Capacidad de organización y planificación.
· CGII3. Comunicación oral y escrita en la lengua nativa.
· CGII4. Conocimiento de una lengua extranjera.
· CGII7. Resolución de problemas.
· CGII9. Trabajo en equipo.
· CGII10. Trabajo en un equipo de carácter interdisciplinar.
· CGII16. Aprendizaje autónomo.
· CEII10. Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos de informática.

4.3 Competencias transversales y de materia

· Competencia 1. 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.
· Competencia 2. SI5. Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.
· Competencia 3. SI6. Capacidad para comprender y aplicar los principios y las técnicas de gestión de la calidad y de la innovación tecnológica en las organizaciones.
· Competencia 4. Capacidad de enfrentarse al escenario de un delito digital con las habilidades necesarias para extraer pruebas, analizarlas y emitir un informe; todo ello de forma forense.

5. Contenidos

Bloque 1: Gestión de la Seguridad, Análisis de Riesgos y Legislación

TEMA 1. Introducción a la Seguridad en los Sistemas de Información

1. Información y Seguridad.
2. Un ejemplo trivial.
3. Evolución de la Seguridad de los Sistemas de Información.
4. Los marcos de seguridad europeo y mundial.
5. Situación en España.

TEMA 2. Niveles de gestión de la seguridad

1. Nivel 0: el sentido común.
2. Nivel 1: salvaguardas preventivas mínimas. Cumplimiento de la legislación obligatoria.
3. Nivel 1,5: salvaguardas adicionales mínimas. Legislación administraciones públicas. Esquema Nacional de Seguridad.
4. Nivel 2: gestión del proceso de seguridad. Estándares y normas europeas y españolas. Certificación.
5. Nivel 3. gestión global de la seguridad.
6. Nivel 4. certificación de componentes y de sistemas.

TEMA 3. Metodología de Análisis y Gestión de Riesgos en Sistemas de Información MAGERIT

1. Introducción a MAGERIT versión 2.
2. Realización del análisis y la gestión de riesgos (AGR).
3. Estructuración del proyecto de AGR.
4. Herramienta de AGR: PILAR (Procedimiento Informático y Lógico para el Análisis de Riesgos).
5. Técnicas aplicables al AGR: técnicas generales y específicas.
6. Catálogo de elementos
7. Aplicación del AGR al desarrollo de sistemas de información.

TEMA 4. Aspectos legales de la seguridad en los Sistemas de Información

1. Protección de datos personales.
2. El régimen jurídico de la firma electrónica.
3. Aspectos jurídico penales.

Bloque 2: Respuesta a incidentes e Informática Forense

TEMA 5. El incidente de seguridad en la organización

1. Definición y caracterización del incidente.
2. Preparación previa al incidente. Creación del grupo de respuesta a incidentes y su papel en la organización.

3. Recolección y manejo de evidencias tanto en vivo como post-mortem. Conocimientos básicos para tal fin: Sistemas de ficheros, logs del sistema, etc.
4. Análisis forense de datos.
5. Aspectos legales del análisis forense. Terminología. La figura del perito. Leyes a tener en cuenta.
6. Casos de estudio
7. El informe pericial

TEMA 6. Herramientas de Seguridad en los Sistemas de Información

1. Herramientas utilizadas en los incidentes de seguridad: análisis de las más comunes.
2. Requisitos para la selección, aprobación, implementación, uso y mantenimiento de las herramientas de seguridad en los Sistemas de Información.
3. Aplicación de las herramientas analizadas a casos prácticos sencillos.

TEMA 7. Introducción a la informática forense

PRÁCTICAS

Práctica 1. Manejo de la herramienta PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos) de apoyo a la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: *Relacionada con los contenidos Tema 3*

- ESTUDIO DE UN CASO DE USO. Tomando como punto de partida el caso práctico del proyecto de una UNIDAD ADMINISTRATIVA de la herramienta PILAR, estudiar el caso de uso de la GUIA DE SEGURIDAD DE LAS TIC DEL CENTRO CRIPTOLÓGIOCO NACIONAL.
- TRABAJO PRÁCTICO DE APLICACIÓN DE MAGERIT USANDO PILAR. Elaboración de un proyecto de análisis y gestión de riesgos con ayuda de la herramienta PILAR de apoyo a la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de acuerdo al enunciado que se facilitará.

Práctica 2. Manejo de algunas distribuciones Linux LiveCD de informática forense (HELIX, CAINE) y otras herramientas propietarias para ejercitar técnicas de análisis forense, reto forense, peritajes informáticos e informes: *Relacionada con los contenidos Bloque 2*,*Tema 5*,*Tema 6 y Tema 7*

- Herramientas: Autopsy, OSForensics, Redline.
- Obtención de una imagen de disco duro, hash del mismo y análisis en búsqueda de información trabajando con la copia del mismo.
- Extracción y análisis de metadatos y generación de líneas de tiempo para correlacionar actividades en el sistema.
- Resolución retos forense. Ejemplo de reto forense: Dada una llave USB, métodos y técnicas para localizar cierta información de manera que se admita como prueba pericial.
- Elaboración de un informe pericial informático.

6. Metodología Docente

Actividad Formativa	Metodología	Horas Presenciales	Trabajo Autónomo	Volumen de trabajo
A1	Actividades con grupo grande de alumnos entre las que se encuentran la presentación en el aula de los conceptos propios de la materia mediante metodología expositiva con lecciones magistrales participativas y medios audiovisuales. También se contemplan en este grupo las actividades de evaluación teórico prácticas.	20	30	50
A2	Actividades en el aula de resolución de problemas, seminarios, aprendizaje orientado a proyectos, exposición y discusión de trabajos y simulaciones relativas al seguimiento individual y/o grupal de adquisición de las competencias.	10	15	25
A3	Actividades en el laboratorio relacionadas con la componente práctica de las asignaturas, desarrollo de trabajos con equipo técnico especializado, desarrollo de programas, etc	30	45	75
	Total	60	90	150

7. Horario de la asignatura

http://www.um.es/informatica/index.php?pagina=planificacion&subseccion=horarios

8. Sistema de Evaluación

Métodos / Instrumentos	Examen teórico-práctico. En este instrumento incluimos desde el tradicional examen escrito o tipo test hasta los exámenes basados en resolución de problemas, pasando por los de tipo mixto que incluyen cuestiones cortas o de desarrollo teórico junto con pequeños problemas. También se incluye aquí la consideración de la participación activa del alumno en clase, la entrega de ejercicios o realización de pequeños trabajos escritos y presentaciones.
Criterios de Valoración	Evaluación de las capacidades y competencias adquiridas respecto a los aspectos de gestión de la seguridad, metodologías y estándares, auditoría y peritaje de los sistemas de información y los relativos a la legislación vigente.
Ponderación	50
Métodos / Instrumentos	Informe técnico. En este instrumento incluimos los resultados de actividades prácticas, o de laboratorio, junto con sus memorias descriptivas. Los resúmenes del estado del arte o memorias de investigación sobre temas concretos. Y la posibilidad de realizar entrevistas personales o presentaciones de los trabajos realizados también entran en esta categoría.
Criterios de Valoración	Evaluación de las capacidades y competencias adquiridas respecto a los aspectos de manejo de técnicas y herramientas informáticas de análisis y gestión de riesgos y de informática forense.
Ponderación	50

Fechas de exámenes

http://www.um.es/informatica/index.php?pagina=planificacion&subseccion=examenes

9. Resultados del Aprendizaje

Objetivos Formativos

- Analizar los antecedentes de la seguridad de los sistemas de información, de su marco europeo y mundial así como de su situación en España.
- Conocer los distintos modelos escalonados o niveles de gestión de la seguridad de los Sistemas de Información.

- Conocer los fundamentos y elementos de la Metodología de Análisis y Gestión de Riesgos en Sistemas de Información (MAGERIT) del Ministerio de Administraciones Públicas.
- Entender la realización y estructuración de un proyecto de análisis y gestión de riesgos de acuerdo con MAGERIT.
- Manejar la herramienta informática de apoyo a la metodología MAGERIT Procedimiento Informático y Lógico para el Análisis de Riesgos (PILAR) del Centro Criptológico Nacional, para el estudio de un caso de uso y para la realización de un caso práctico de aplicación de la metodología MAGERIT y de utilización de la herramienta informática PILAR.
- Conocer el establecimiento e implantación de una organización de la seguridad como estructura para el mantenimiento y gestión de la seguridad de los sistemas de información, identificar las diferentes actividades y definir las responsabilidades, figuras y roles en la gestión de la seguridad.
- Abordar el marco legal de la Seguridad Informática, el régimen jurídico de la firma electrónica, de los delitos informáticos y, especialmente, la protección de datos personales y las medidas de seguridad aplicables a ficheros y tratamientos.
- Conocer el proceso de implantación y certificación del estándar para la seguridad de la información ISO/IEC 27001 en una organización.
- Ser capaz de definir las áreas y fases de la auditoría de la seguridad de los sistemas de información.
- Manejar las directrices oficiales más comunes para la recolección y manejo de evidencias.
- Conocer los objetivos de la informática forense, las metodologías que utiliza y los procedimientos técnicos y legales.
- Desarrollar un plan de acción como respuesta a un incidente, así como tratar con los diferentes agentes que intervienen en la respuesta.
- Extraer y analizar indicios y pruebas sobre el incidente de una manera forense.
- Redactar un informe con los resultados y defenderlo.

10. Bibliografía

Bibliografía Básica

Marcelo Cocho, Julián. “Riesgo y Seguridad de los Sistemas Informáticos”. Ed. UNIVERSIDAD POLITÉCNICA DE VALENCIA. 2003. ISBN: 9788497053303. Nº Título:497015.

Metodología MAGERIT v 3. MINISTERIO DE ADMINISTRACIONES PÚBLICAS. 2012

Centro Criptológico Nacional. Herramienta PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos)

Jason T. Luttgens, Matthew pepe. "Incident Response & Computer Forensics". 3ª ed. McGraw Hill. ISBN: 978-0-07-179868-6. Nº Título: 602195

Cory Altheide, Harlan Carvey. "Digital Forensics with Open Source Tools." Ed. Elsevier. ISBN 978-1-59749-586-8. Nº Título:576774

García Rambla, Juan Luis. Un forense llevado a juicio. Sidertia. Bajo licencia Creative Commons

Bibliografía Complementaria

Varios autores. Seguridad de las Tecnologías de la Información. La construcción de la confianza para una sociedad conectada. Ed. AENOR. 2003. ISBN: 9788481433678

11. Observaciones y recomendaciones

La asignatura consta de dos partes bien diferenciadas de 7 semanas cada una, con su propia evaluación. La nota final será la media de ambas partes.

Los criterios para establecer la nota final a partir de cada parte son los siguientes:

- Si el alumno no se presenta al examen de teoría ni realiza ninguna entrega de prácticas, su calificación será "No Presentado"
- Si el alumno supera una parte y no se presenta a la otra, su calificación será "No Presentado"
- Si el alumno suspende una parte y no se presenta o aprueba la otra, su calificación será "Suspenso" con la nota de esa parte.
- Cuando el alumno aprueba o suspende las dos partes, su calificación será resultado de aplicar los pesos establecidos para cada parte.
- Si el alumno aprueba ambas partes, la nota final será la media de las dos notas.