ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001013 - Sistemas de gestión de seguridad de la información

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001013 - Sistemas de gestión de seguridad de la información
No de créditos	3 ECTS
Carácter	Optativa
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	09AW - Master universitario en ciberseguridad
Centro en el que se imparte	09 - Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Jesus Sanchez Lopez (Coordinador/a)	ETSISI -1117	jesus.sanchezl@upm.es	Sin horario.
Carolina Gallardo Perez	ETSISI - 1209	carolina.gallardop@upm.es	Sin horario.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Competencias y resultados de aprendizaje

3.1. Competencias

CB07 - 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

CB09 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - 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

CG01 - Proporcionar al alumno los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, dotándole de la capacidad para definir estrategias, políticas y normas para la seguridad corporativa

CG05 - Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia

CT05 - Gestión de la información

CT11 - Razonamiento crítico

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

3.2. Resultados del aprendizaje

RA20 - Diseñar un Sistema de Gestión de Seguridad de la Información que permita la monitorización de la estrategia y política de ciberseguridad y la validación de los controles necesarios para ello

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

La asignatura Sistemas de Gestión de la Seguridad de la Información capacita al alumno para conocer los conceptos, estándares, normativa, regulación y buenas prácticas de uso más extendido en la gestión de la seguridad de la información: ISO 27001, Esquema Nacional de Seguridad (ENS), etc., así como practicar sobre supuestos para utilizar algunas de las herramientas comerciales de implantación de SGSIs (tales como PILAR y GlobalSuite) más usadas en este sector profesional tanto en España como fuera de ella.

El sector profesional de relacionado con esta asignatura, en sus vertientes de Consultoría y de Auditoría, es novedoso y de interés creciente. Las ofertas de empleo son de naturaleza muy diversa y proceden tanto de las propias Organizaciones, con necesidades de cubrir perfiles de seguridad de la información (no solo / necesariamente TIC's): [CSO], CIO, CISO, etc. y de auditor interno (primera parte), como de empresas que facilitan a otras servicios de consultoría y auditoría externa (tercera parte).

El objetivo general de la asignatura es conocer los aspectos relacionados con los sistemas de gestión de la seguridad de la información (SGSI) tanto en sus vertientes de implementación (consultoría) como de evaluación (auditoría). Se contemplan los siguientes objetivos específicos:

- Identificar los conceptos y enfoques actuales en el ámbito de la Seguridad de la Información.
- Capacitar al alumno para realizar el análisis y la planificación de la seguridad de la información aplicando un procedimiento sistemático basado en el seguimiento de normas y estándares nacionales e internacionales.
- Saber establecer y utilizar métricas para medir el grado de implantación, y en su caso la eficacia, de los controles que se establezcan.
- Aprender una metodología para la realización de auditorías de los sistemas de información.
- Conocer las aproximaciones más habituales para recuperarse frente a desastres y permitir la continuidad de las operaciones (negocio).

NOTA: En esta asignatura **no se aborda** la problemática de la **Gestión** (Evaluación y Tratamiento) **de Riesgos**

dado que este aspecto es motivo de otra específica, de carácter obligatorio.

4.2. Temario de la asignatura

1. La Organización y su Sistema de Información
    1.1. El Departamento de Sistema de Información.
    1.2. Tecnologías para el Sistema de Información.
    1.3. Gestión del Sistema de Información.
    1.4. Marcos de referencia y contexto profesional.
2. Estándares internacionales. La familia ISO 27k.
    2.1. Enfoque orientado a la normalización.
    2.2. Definición de SGSI. Norma ISO 27001.
    2.3. Código de buenas prácticas. Norma ISO 27002.
3. El marco español. Esquema Nacional de Seguridad (ENS)
    3.1. Estructura del Esquema Nacional de Seguridad.
    3.2. Medidas de seguridad.
    3.3. Política de seguridad.
    3.4. Responsabilidades y funciones.
4. Auditoría del SGSI.
    4.1. Conceptos y definiciones.
    4.2. Programa de auditoría.
    4.3. Herramientas para la auditoría.
5. Continuidad de negocio y recuperación frente a desastres.
    5.1. Organización para la gestión de incidentes.
    5.2. Análisis de impacto al negocio (BIA).
    5.3. El Sistema de Gestión de la Continuidad del Negocio. Norma ISO 22301.
    5.4. Aspectos de seguridad de la información para gestión de la continuidad del negocio. Norma ISO 27002, Dominio 17

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	**La Organización y su Sistema de Información** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Sondeo del sector profesional** Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas	**Participación en foro colaborativo y elaboración de conclusiones** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 04:00
2	**Estándares internacionales. La familia ISO 27k** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
3	**El marco español. Esquema Nacional de Seguridad.** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Identificación de medidas de seguridad (ENS)** Duración: 02:00 PR: Actividad del tipo Clase de Problemas	
4		**Utilización del programa PILAR para el Esquema Nacional de Seguridad.** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		**Aplicabilidad de medidas del Esquema Nacional de Seguridad.** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 06:00
5	**Medición y auditoría del SGSI.** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
6	**Medición y auditoría del SGSI.** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Herramienta GlobalSuite para la gestión del SGSI.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
7	**Continuidad de negocio y recuperación frente a desastres.** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Conferencia: Las profesiones de Consultor y Auditor de SGSI.** Duración: 02:00 OT: Otras actividades formativas	**Cuestionario general.** ET: Técnica del tipo Prueba Telemática Evaluación continua Duración: 02:00 **Utilización de herramientas de soporte al SGSI.** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 10:00
8				
9				
10				
11				
12				

13				
14				
15				
16				**Examen final** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 03:00
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Participación en foro colaborativo y elaboración de conclusiones	ET: Técnica del tipo Prueba Telemática	No Presencial	04:00	10%	0 / 10	CB09 CT05 CT11
4	Aplicabilidad de medidas del Esquema Nacional de Seguridad.	ET: Técnica del tipo Prueba Telemática	No Presencial	06:00	25%	3 / 10	CB07 CB10 CG05
7	Cuestionario general.	ET: Técnica del tipo Prueba Telemática	Presencial	02:00	40%	3 / 10	CB07 CB09 CG01 CT11
7	Utilización de herramientas de soporte al SGSI.	TI: Técnica del tipo Trabajo Individual	No Presencial	10:00	25%	5 / 10	CG01 CT12

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
16	Examen final	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	5 / 10	CB07 CB09 CB10 CG01 CG05 CT05 CT11 CT12

6.1.3. Evaluación convocatoria extraordinaria

No se ha definido la evaluación extraordinaria.

6.2. Criterios de evaluación

El mecanismo de evaluación está orientado a valorar el resultado de aprendizaje **RA20 - Diseñar un Sistema de Gestión de Seguridad de la Información que permita la monitorización de la estrategia y política de ciberseguridad y la validación de los controles necesarios para ello.**

Para ello se ha diseñado el conjunto de actividades de evaluación indicado en el apartado anterior, constituido por **tres actividades práctica**s y **un cuestionario genera**l, aplicable tanto para **Evaluación Continua** como para **Evaluación sólo por Prueba Final**. En el primer caso la realización y entrega de las (3) actividades prácticas seguirá el secuenciamiento temporal indicado en el cronograma, en tanto que para el segundo el alumno gestionará libremente su tiempo debiendo hacer entrega de los resultados con anterioridad a la fecha de celebración del examen final.

NOTA: La primera de las actividades prácticas: **Participación en foro colaborativo y elaboración de conclusiones**, requirá una adaptación para Evaluación solo por Prueba Final dado que en este caso no se realizará como actividad colaborativa.

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Plataforma Moodle	Recursos web	Se utilizará la plataforma Moodle de la UPM (https://moodle.upm.es/titulaciones/oficiales/) tanto para el alojamiento de contenidos como para la gestión de actividades (incluida evaluación) y comunicación interpersonal

8. Otra información

8.1. Otra información sobre la asignatura

OBSERVACIÓN:

En la memoria aparecen las siguientes **competencias** que se pretende que el alumno consiga con la asignatura optativa Sistemas de Gestión de la Seguridad de la Información, pero **que no puedo ver en Gauss:**

- CE -10 Capacidad para establecer una estrategia de continuidad de negocio y hacer resiliente a la organización ante cualquier tipo de ataques, dotándola de capacidades predictivas y prescriptivas.
- CE-11 Capacidad de definir el plan estratégico de ciberseguridad de una organización, incluyendo la normativa, procesos de implantación y valoración del impacto en el negocio.