ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001011 - Gestión de riesgos y operaciones en ciberseguridad

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	93001011 - Gestión de riesgos y operaciones en ciberseguridad
No de créditos	6 ECTS
Carácter	Obligatoria
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 *
Jose Antonio Mañas Argemi	B-202	joseantonio.manas@upm.es	X - 12:00 - 13:00
Victor Abraham Villagra Gonzalez (Coordinador/a)	B-217	victor.villagra@upm.es	X - 14:00 - 15:00
Irene Cristina Romero Ibañez	B-423	irenecristina.romero@upm.es	X - 14:00 - 15:00 Contactar por correo electronico

Joaquin Luciano Salvachua Rodriguez	C-220	joaquin.salvachua@upm.es	X - 14:00 - 15:00
Gabriel Huecas Fernandez-Toribio	C-219	gabriel.huecas@upm.es	X - 14:00 - 15:00

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

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Ciberseguridad: contexto y amenazas

- Protección de la información

- Protección de sistemas y servicios

- Servicios de control de acceso

- Servicios de seguridad en red

- Auditoría técnica de seguridad

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Servicios de Seguridad en Redes, Servicios y Sistemas de Telecomunicación

- Tecnologías de Ciberseguridad

4. Competencias y resultados de aprendizaje

4.1. Competencias

CB06 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

CB08 - 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

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

CE03 - Capacidad para realizar un análisis y evaluación de los riesgos de una organización, con un enfoque de gestión de riesgos enmarcado en un Sistema de Gestión de Seguridad de la Información

CE07 - - Capacidad para diseñar un centro de gestión y operación de ciberseguridad, con la combinación adecuada de servicios preventivos, de detección y de respuesta a incidentes

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

CG02 - Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización

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

CT03 - Creatividad

CT04 - Organización y planificación

CT05 - Gestión de la información

CT10 - Resolución de problemas

CT11 - Razonamiento crítico

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

4.2. Resultados del aprendizaje

RA17 - Conocer los componentes de un riesgo, y saber aplicar las metodologías para la realización de un análisis de riesgos

RA18 - Conocer los distintos componentes organizativos y tecnológicos de un Centro de Gestión de Ciberseguridad, y ser capaz de realizar su diseño

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Los objetivos de esta asignatura se articulan en dos grandes temas:

- Análisis y Gestión de Riesgos de Ciberseguridad
- Gestión y Operación de la Seguridad en Corporaciones

El primer tema tiene como objetivo que el alumno conozca la problemática asociada a la implantación de una política de seguridad en una organización, siendo capaz de realizar una planificación y diseño de la misma, a nivel de estrategia corporativa, y su análisis de riegos. Se verán las distinas aproximaciones al análisis y gestión de riesgos, con casos de estudio que permitan el diseño de distintos análisis de riesgos de determinadas organizaciones.

El segundo tema trata sobre la problemática de la gestión y monitorización de incidentes de ciberseguridad en una

organización, tratando los servicios necesarios a implantar en un Centro de Operaciones de Ciberseguridad (SOC), y los modelos de gestión existentes para estos centros,. En este tema se tratará de forma especial las tecnologías y modelos de Big Data y Machine Learning aplicados a la gestión de incidentes en ciberseguridad.

La asignatura incluirá trabajos personales de los alumnos de casos de estudio de situaciones muy cercanas a casos reales en dichos temas.

5.2. Temario de la asignatura

1. Analisis y Gestión de Riesgos
2. Gestión y Operación de la Ciberseguridad
   - 2.1. Servicios de un Centro de Operación de Ciberseguridad
   - 2.2. Diseño de un Centro de Operación de Ciberseguridad
   - 2.3. Técnicas de Machine Learning y Big Data en Ciberseguridad

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1				
2				
3				
4				
5				
6	**Clases Teóricas de Análisis y Gestión de Riesgos** Duración: 10:00 LM: Actividad del tipo Lección Magistral **Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 10:00 LM: Actividad del tipo Lección Magistral			
7	**Clases Téoricas de Análisis y Gestión de Riesgos** Duración: 10:00 LM: Actividad del tipo Lección Magistral **Clases Teóricas de Gestión de Operaciones en Ciberseguridad** Duración: 06:00 LM: Actividad del tipo Lección Magistral	**Desarrollo de Casos de Estudio de Análisis y Gestrión de Riesgos** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
8	**Clases Téoricas de Big Data y Machine Learning aplicado a la Ciberseguridad** Duración: 04:00 LM: Actividad del tipo Lección Magistral	**Casos de Estudio de Sistemas SIEM de Operaciones en Ciberseguridad** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
9		**Casos de Estudio de Big Data y Machine Learning aplicado a la Ciberseguridad** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio **Casos de Estudio de Sistemas SIEM de Operaciones en Ciberseguridad** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación de Trabajos de Análisis de Riesgos** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 02:00 **Evaluación de Trabajos de Gestión de Operaciones** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 02:00 **Evaluación de Trabajos de Machine Learning y Big Data** PG: Técnica del tipo Presentación en Grupo Evaluación continua Duración: 02:00

				Examen Final EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00 **Evaluacion de Trabajos** PG: Técnica del tipo Presentación en Grupo Evaluación sólo prueba final Duración: 04:00 **Examen Final** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00
10				
11				
12				
13				
14				
15				
16				
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.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
9	Evaluación de Trabajos de Análisis de Riesgos	PG: Técnica del tipo Presentación en Grupo	Presencial	02:00	20%	4 / 10	CB06 CB07 CB08 CB09 CB10 CG01 CG02 CG05 CT03 CT04 CT05 CT10 CT11 CT12 CE03
9	Evaluación de Trabajos de Gestión de Operaciones	PG: Técnica del tipo Presentación en Grupo	Presencial	02:00	20%	4 / 10	CB07 CB08 CB09 CB10 CG01 CG02 CG05 CT03 CT04 CT05 CT10 CT11 CT12 CE07
9	Evaluación de Trabajos de Machine Learning y Big Data	PG: Técnica del tipo Presentación en Grupo	Presencial	02:00	10%	4 / 10	CB06 CB07 CB08 CB09 CG01 CG05 CT03 CT04 CT05 CT10 CT11

							CT12 CE07
9	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	50%	4 / 10	CE03 CE07

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
9	Evaluacion de Trabajos	PG: Técnica del tipo Presentación en Grupo	Presencial	04:00	50%	4 / 10	CB06 CB07 CB08 CB09 CB10 CG01 CG02 CG05 CT03 CT04 CT05 CT10 CT11 CT12 CE03 CE07
9	Examen Final	EX: Técnica del tipo Examen Escrito	Presencial	02:00	50%	4 / 10	CE03 CE07

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen Final Extraordinario	EX: Técnica del tipo Examen Escrito	Presencial	04:00	100%	5 / 10	CB06 CB07 CB08 CB09 CB10 CG01 CG02 CG05 CT03 CT04 CT05 CT10 CT11 CT12

						CE03 CE07

7.2. Criterios de evaluación

Los estudiantes serán evaluados, por defecto, mediante evaluación continua. El estudiante que desee renunciar a la evaluación continua y optar a la evaluación por prueba final (formada por una o más actividades de evaluación global de la asignatura), deberá comunicarlo por escrito formalizado en el registro de la ETSI Telecomunicación y dirigido al Coordinador de la Asignatura antes del final del primer mes desde el comienzo de la asignatura. La presentación de este escrito supondrá la renuncia automática a la evaluación continua.

La evaluación comprobará si los estudiantes han adquirido las competencias de la asignatura. Por tanto, la evaluación mediante prueba final usará los mismos tipos de técnicas evaluativas que se usan en la evaluación continua (EX, ET, TG, etc.), y se realizarán en las fechas y horas de evaluación final aprobadas por la Junta de Escuela para el presente curso y semestre..

CONVOCATORIA ORDINARIA: MODALIDAD EVALUACIÓN CONTINUA

La asignatura se aprobará cuando se obtenga una calificación mayor o igual a 5 puntos sobre un total de 10. La nota final se obtendrá:

- Examen escrito de todos los temas: 50%
- Prácticas de Analisis y gestión de Riesgos: 20%
- Prácticas de Gestión de Operaciones: 20%
- Prácticas de Machine Learning y Big Data: 10%

Deberá sacar más de un 4 en cada trabajo y un 5 en total para poder ser evaluado en esta modalidad. En caso contrario, deberá presentarse al examen final. En caso de inasistencia o no entrega de alguno de los componentes de cada actividad, se considerará que el alumno no se ha presentado y no podrá seguir la evaluación continua, debiendo optar por evaluación única

CONVOCATORIA ORDINARIA: EVALUACIÓN MEDIANTE UNA ÚNICA PRUEBA FINAL

El 100% de la calificación de los alumnos que presenten el escrito arriba referido se otorgará en función de una única prueba final en la que presentarán asimismo los trabajos de la asignatura.

CONVOCATORIA EXTRAORDINARIA

La evaluación de la asignatura en su convocatoria extraordinaria se realizará mediante una única prueba final, con independencia de la opción elegida en la convocatoria ordinaria.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Moodle	Recursos web	Servidor Moodle de la Asignatura
Equipamiento	Equipamiento	Aula, Laboratorio, Sala de Trabajo en Grupo
Referencias	Bibliografía	Bibliografía