Guía de aprendizaje

Gestión de Riesgos Tecnológicos

Curso: 2019 - 2020
Código: 9928001809
Profesor coordinador:
Titulación: Grado en Criminología
Escuela/ Facultad: CIENCIAS SOCIALES
Idiomas: CASTELLANO

La misión de la Universidad Europea de Valencia es proporcionar a nuestros estudiantes una educación integral, formando líderes y profesionales preparados para dar respuesta a las necesidades de un mundo global, para aportar valor en sus profesiones y contribuir al progreso social desde un espíritu emprendedor y de compromiso ético. Generar y transferir conocimiento a través de la investigación aplicada, contribuyendo igualmente al progreso y situándonos en la vanguardia del desarrollo intelectual y técnico.

Índice

1. Datos básicos de la asignatura/módulo

ECTS	6 ECTS
Carácter	OPTATIVA
Idioma/s	CASTELLANO
Modalidad	PRESENCIAL
Trimestre/Semestre	

2. Presentación de la asignatura/módulo

Esta materia pretende aportar conocimientos para la comprensión de los conceptos de ciberseguridad, así como los distintos tipos de actividad delictiva que pueden desarrollarse en la red, junto con sus características, fines, objetivos, estructura, financiación, tipología y relaciones, y mecanismos legales, jurídicos, estatales y europeos en la dirección y gestión de los diversos servicios de ciberseguridad.

El alumno manejará también conceptos relacionados con la evolución de la tecnología aplicada al ámbito de la seguridad y de la criminalidad, así como a nuevos mecanismos de comunicación, propaganda, activismo social o terrorismo.

3. Competencias y resultados de aprendizaje

Competencias básicas:

- CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
- CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

Competencias transversales:

- CT1 - Responsabilidad. Que el estudiante se capaz de asumir las consecuencias de las acciones que realiza y responder de sus propios actos.

- CT3 - Conciencia de los valores éticos. Capacidad del estudiante para sentir, juzgar, argumentar y actuar conforme a valeres morales de modo coherente, persistente y autónomo.
- CT10 - Innovación-creatividad. Que el estudiante sea capaz de idear soluciones nuevas y diferentes a problemas que aporten valor a problemas que se plantean.

Competencias específicas:

- CE 5 - Interpretar datos cuantitativos y cualitativos.
- CE 6 - Adquirir una conciencia crítica en el análisis de la criminalidad con capacidad de evaluación de resultados.
- CE 10 - Manejar las nuevas tecnologías en el ámbito criminológico y de la seguridad: bases de datos, legislación, software específico.
- CE 16 - Detectar los problemas y ofrecer las soluciones más adaptadas a la situación real planteada elaborando las estrategias de intervención más adecuadas y efectivas para cada supuesto.
- CE 17 - Analizar y comparar los sistemas de seguridad y su relación con las necesidades individuales y colectivas.
- CE 18 - Saber usar, en su caso, las fuentes de información y herramientas básicas en situaciones de seguridad y emergencia, contrastando la información y respetando la privacidad de los protocolos, directivas y registros de actuación.
- CE 19 - Valorar la eficacia de los distintos modelos de gestión de la seguridad.
- CE 20 - Conocer, en su caso, los principales sistemas de seguridad aplicables a la protección de instalaciones, las personas y la autoprotección, legislación aplicable a la seguridad privada y pública nacional, europea e internacional.
- CE 21 - Proponer, analizar, diseñar, ejecutar y evaluar estrategias en todos los ámbitos de la seguridad pública y privada, y a todos los niveles.

Resultados de aprendizaje:

- RA1: Comprensión de conceptos relacionados con la gestión de riesgos tecnológicos.
- RA2: Capacidad de análisis y diseño de estrategias.

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CB4, CT1, CT3, CE10, CE18, CE19, CE20	RA1
CB2, CB3, CT1, CT9, CT10, CE5, CE6, CE16, CE17, CE21.	RA2

A continuación, se detalla la distribución de tipos de actividades formativas y la dedicación en horas a cada una de ellas:

Tipo de actividad formativa	Número de horas
AF1. Estudio autónomo	25
AF2. Elaboración de estudio temático sobre diferentes aspectos relacionados con la Criminología.	25
AF3. Lecciones magistrales.	25
AF4. Proyectos sobre diseño de estrategias.	25
AF5. Pruebas de conocimiento.	6,3
AF6. Tutoría.	25
AF7. Búsqueda de recursos y selección de fuentes de información.	6,2
AF8. Debates y coloquios.	12,5
TOTAL	**150 h**

Para desarrollar las competencias y alcanzar los resultados de aprendizaje indicados, deberás realizar las actividades que se indican en la tabla inferior:

Resultados de aprendizaje	Actividad de aprendizaje	Tipo de actividad Formativa	Contenidos
RA1	ACT. 2 Carpeta de aprendizaje ACT. 3 Participación en debates y foros	AF3, AF7, AF8	**Unidad 1.** Introducción a la ciberseguridad y los riesgos tecnológicos.
RA1	ACT. 2 Carpeta de aprendizaje	AF3, AF7	**Unidad 2.** Marco Jurídico y político securitario español e internacional: Protección de datos y comercio electrónico
RA1	ACT. 2 Carpeta de aprendizaje, ACT. 3 Participación en debates y foros	AF3, AF7, AF8	**Unidad 3.** Seguridad de la información, redes y sistemas.
RA1, RA2	ACT. 2 Carpeta de aprendizaje, ACT. 3 Participación en debates y foros	AF3, AF7, AF8	**Unidad 4.** El ciberdelito: análisis de riesgos para los sistemas de información.
RA1, RA2	ACT. 4 Trabajos de investigación, ensayos o proyectos escritos	AF1, AF2, AF3, AF4, AF7	**Unidad 5.** Los nuevos ciberdelitos: del hacktivismo al ciberterrorismo
RA1, RA2	ACT. 1 Pruebas presenciales de conocimiento	AF1, AF5	**Todas las unidades**

En el Campus Virtual, cuando accedas a la asignatura, podrás ver en detalle los enunciados de las actividades que tendrás que realizar, así como el procedimiento y la fecha de entrega de cada una de ellas.

4. Seguimiento y evaluación

En la tabla inferior se indican las actividades evaluables, los criterios de evaluación de cada una de ellas, así como su peso sobre la calificación total de la asignatura.

Actividad evaluable	Criterios de evaluación	Peso (%)
ACT. 1 Pruebas presenciales de conocimiento	Se valorará la asunción de los contenidos de los temas por el estudiante.	40 %

ACT. 2 Carpeta de aprendizaje	Se evaluará el compendio de documentos, ejercicios, recursos seleccionados o casos que forma la carpeta, en particular la consecución de los mismos y su desarrollo	20 %
ACT. 3 Participación en debates y foros	Se evaluará la posición que cada estudiante adopta en la discusión y defensa.	10 %
ACT. 4 Trabajos de investigación, ensayos o proyectos escritos	Rúbricas y criterios se exponen en el campus virtual	30 %

4.1. Convocatoria ordinaria

En **convocatoria ordinaria**, la calificación final se realizará sumando las calificaciones de los distintos tipos de evaluación, en la ponderación que corresponda. Para superar la asignatura bastará con alcanzar un nota ponderada global de 5, que supondría superar el 50% de la asignatura. No obstante, para aplicar esta ponderación es IMPRESCINDIBLE que al menos se haya obtenido una media de 5 puntos sobre 10 en la parte correspondiente a las PRUEBAS DE CONOCIMIENTO. En caso de no llegar a esta calificación, el alumno deberá realizar nueva/s prueba/s de conocimiento en convocatoria extraordinaria, calificándose la asignatura en la convocatoria ordinaria como SUSPENSO.

Aquél alumno que no iguale u supere el 50% de la asignatura, o no alcance una calificación de 5 sobre 10 en las pruebas de conocimiento, se le calificará en la convocatoria ordinaria como "suspenso", dado que la evaluación continua impedirá considerarlo como no presentado. En consecuencia, deberá presentarse a la convocatoria extraordinaria que se fije en su momento.

Si se calificara la **asignatura** como **suspensa en ORDINARIA por falta de cumplimiento de los porcentajes de asistencia**, el profesor señalará al alumno qué pruebas, trabajos o actividades deberá realizar el alumno como complemento para poder superar la asignatura.

Asistencia: Para los estudiantes que cursen enseñanzas presenciales, se establece la obligatoriedad de justificar, al menos, el 50% la asistencia a las clases, como parte necesaria del proceso de evaluación y para dar cumplimiento al derecho del estudiante a recibir asesoramiento, asistencia y seguimiento académico por parte del profesor. A estos efectos, los estudiantes deberán utilizar el sistema tecnológico que la Universidad pone a su disposición, o el sistema de control determinado por el docente, para acreditar su asistencia diaria a cada una de sus clases. Dichos sistemas servirán, además, para garantizar una información objetiva del papel activo del estudiante en el aula. **La falta de acreditación por los medios propuestos por**

la universidad de, al menos, el 50% de asistencia, *facultará al profesor a calificar la asignatura como suspensa en la convocatoria ordinaria*, acorde al sistema de calificación previsto en el presente reglamento. Todo ello, sin perjuicio de otros requisitos o superiores porcentajes de asistencia que cada facultad pueda establecer en las guías docentes o en su normativa interna

4.2. Convocatoria extraordinaria

Para superar la asignatura convocatoria extraordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,00 de la calificación final (media ponderada de la asignatura).

Se deberan entregar las actividades no superadas en convocatoria ordinaria, tras haber obtenido las calificaciones correspondientes a las mismas por parte del profesor o bien aquellas que no fueron entregadas.

5. Bibliografía

A continuación, se indica la bibliografía recomendada:

- Bartlett, J. (2015) The Dark Net, Windmill Books, London.
- Crowell, W., Cole, E. (2011), Physical and Logical security convergence. Syngress.
- Davis, N. (2000), An information based revolution in military affairs, Arquilla, D. (Ed.) In Athena's cam: preparing for conflict in the Information Age. RAND Co: Santa Monica.
- NATO Cybersecurity Framework Manual.

6. Cómo comunicarte con tu profesor

Cuando tengas una duda sobre los contenidos o actividades, no olvides escribirla en los foros de tu asignatura para que todos tus compañeros puedan leerla. Si tienes alguna consulta exclusivamente dirigida al profesor puedes enviarle un mensaje privado desde el Campus Virtual.

Además, en caso de que necesites profundizar en algún tema, puedes acordar con tu profesor una tutoría.

Es conveniente que leas con regularidad los mensajes enviados por compañeros y profesores, pues constituyen una vía más de aprendizaje.

7. Recomendaciones de estudio

La formación universitaria exige planificación y regularidad desde la primera semana. Es muy positivo el intercambio de experiencias y opiniones con profesores y demás estudiantes, ya que permiten el desarrollo de competencias básicas como la flexibilidad, la negociación, el trabajo en equipo, y, por supuesto, el pensamiento crítico.

Por ello te proponemos una metodología general de estudio basada en los siguientes puntos:

- Seguir un ritmo de estudio constante y sistemático.
- Asistir a clase y acceder a la asignatura en el Campus Virtual de manera continuada para mantenerte actualizado sobre el desarrollo de la misma.
- Participar activamente en ella enviando opiniones, dudas y experiencias sobre los temas tratados y/o planteando nuevos aspectos de interés para su debate.
- Leer los mensajes enviados por los compañeros y/o los profesores.

Se considera de especial interés y valor académico la participación activa en las actividades del aula física y virtual. La forma en que puedes participar es muy variada: preguntando, opinando, realizando las actividades que el profesor proponga, participando en las actividades colaborativas, ayudando a otros compañeros, etc. Esta forma de trabajar supone esfuerzo, pero permite obtener mejores resultados en tu desarrollo competencia.

Anexos con información detallada en el Campus Virtual

Anexo 1. Normativa específica de la asignatura

Toda la normativa correspondiente a la Universidad Europea de Valencia el estudiante puede consultarla en el siguiente enlace: https://valencia.universidadeuropea.es/soy-alumno-uev/informacion-academica/normativa

El **plagio** total o parcial en las actividades se considera una falta grave. Como tal, aparece tipificado en el reglamento interno de la Universidad Europea, estipulándose que las sanciones aplicables oscilan desde el suspenso inmediato de la asignatura sin posibilidad de reelaboración hasta la convocatoria extraordinaria, hasta la apertura de expediente.

Anexo 2. Calendario de actividades

El calendario con fechas de entrega de actividades y eventos relevantes de la asignatura se detallará en al Campus Virtual.

Anexo 3. Rúbricas de las actividades

Las rúbricas de las actividades se detallarán en al Campus Virtual.