20-21

GRADO EN CRIMINOLOGÍA
CUARTO CURSO

GUÍA DE ESTUDIO PÚBLICA



CRIMINALIDAD Y SEGURIDAD INFORMÁTICA

CÓDIGO 66044186

UNED

20-21

CRIMINALIDAD Y SEGURIDAD INFORMÁTICA

CÓDIGO 66044186

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN
REQUISITOS Y/O RECOMENDACIONES PARA CURSAR LA ASIGNATURA
EQUIPO DOCENTE
HORARIO DE ATENCIÓN AL ESTUDIANTE
TUTORIZACIÓN EN CENTROS ASOCIADOS
COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE
RESULTADOS DE APRENDIZAJE
CONTENIDOS
METODOLOGÍA
SISTEMA DE EVALUACIÓN
BIBLIOGRAFÍA BÁSICA
BIBLIOGRAFÍA COMPLEMENTARIA
RECURSOS DE APOYO Y WEBGRAFÍA

Nombre de la asignatura	CRIMINALIDAD Y SEGURIDAD INFORMÁTICA
Código	66044186
Curso académico	2020/2021
Departamento	DERECHO PENAL Y CRIMINOLOGÍA
Título en que se imparte	GRADO EN CRIMINOLOGÍA
Curso	CUARTO CURSO
Periodo	SEMESTRE 1
Tipo	OBLIGATORIAS
Nº ETCS	6
Horas	150.0
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

La asignatura Criminalidad y Seguridad Informática es una asignatura obligatoria de cuarto curso, primer semestre, del Grado en Criminología.
Esta asignatura se incluye en la materia de Criminología y se imparte por el Departamento de Derecho penal y Criminología de la UNED.
La asignatura está relacionada con muchas de las asignaturas de la materia Criminología que integran el Grado, como por ejemplo Programas de prevención y tratamiento de la delincuencia, o Políticas de Seguridad y de Prevención del Delito, pero también con las materias referidas a los Fundamentos de la responsabilidad penal y a la Parte especial del Derecho penal , en cuanto que aporta los fundamentos para la compresión del ciberdelito, y ofrece un enfoque para el control y prevención del delito.
La asignatura contribuye al perfil profesional ofreciendo una base científica para la toma de decisiones, así como una formación básica imprescindible para afrontar los retos de la criminalidad a través de las TIC.
En una sociedad en la que el conocimiento es un valor cada vez más preciado, tanto para el funcionamiento de las organizaciones (estados, empresas, etc.) como para la realización de los individuos, las nuevas tecnologías han supuesto un salto cualitativo espectacular, una verdadera revolución, en tanto nos posibilitan una recopilación, almacenamiento y procesamiento masivo de datos y su transformación en información a través de complejos procesos de contextualización, categorización, cálculo, corrección o condensación. Resulta evidente que ante esta nueva realidad las posibles formas de ataque a la información y las consiguientes necesidades de protección han cambiado notablemente.
Pero además las TIC han modificado para siempre las relaciones económicas, políticas y sociales a nivel planetario. De esta manera entran en el radio de acción de las nuevas tecnologías, y con ello en el de sus peligros, bienes jurídicos como la intimidad y la propia imagen, el patrimonio, la libertad e indemnidad sexual, la propiedad intelectual e industrial, el honor, la libertad, el estado civil, el orden público...
En estos ámbitos las nuevas tecnologías han supuesto en algunas ocasiones nuevas formas de ataque antes desconocidas a viejos bienes jurídicos, y en otras han facilitado y multiplicado los efectos de formas de ataque que ya nos eran también conocidas.
Por todo ello resulta imprescindible para un criminólogo conocer este nuevo y creciente ámbito de criminalidad que denominamos Cibercriminalidad. Y ello presupone la necesaria

adquisición de unos conocimientos básicos o fundamentos de tecnología y seguridad informática.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR LA ASIGNATURA

No se exigen requisitos especiales más allá de los necesarios para cursar el grado.

EQUIPO DOCENTE

Nombre y Apellidos	SERGIO CAMARA ARROYO (Coordinador de asignatura)
Correo Electrónico	scamara@der.uned.es
Teléfono	
Facultad	FACULTAD DE DERECHO
Departamento	DERECHO PENAL Y CRIMINOLOGÍA

Nombre y Apellidos	DANIEL FERNANDEZ BERMEJO
Correo Electrónico	daniel.fernandez@der.uned.es
Teléfono	
Facultad	FACULTAD DE DERECHO
Departamento	DERECHO PENAL Y CRIMINOLOGÍA

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	ALFREDO LIÑAN LAFUENTE
Correo Electrónico	alinan@der.uned.es
Teléfono	
Facultad	FACULTAD DE DERECHO
Departamento	DERECHO PENAL Y CRIMINOLOGÍA

Nombre y Apellidos	RAFAEL PASTOR VARGAS
Correo Electrónico	rpastor@dia.uned.es
Teléfono	91398-8383
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	RAFAEL PASTOR VARGAS
Correo Electrónico	rpastor@scc.uned.es
Teléfono	91398-8383
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	ANTONIO ROBLES GOMEZ
Correo Electrónico	arobles@scc.uned.es
Teléfono	91398-8480
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	MARIA DE LOS LLANOS TOBARRA ABAD
Correo Electrónico	llanos@scc.uned.es
Teléfono	91398-9566
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	NOELIA MARIA CORRAL MARAVER
Correo Electrónico	noeliamaraver@der.uned.es
Teléfono	
Facultad	FACULTAD DE DERECHO
Departamento	DERECHO PENAL Y CRIMINOLOGÍA

HORARIO DE ATENCIÓN AL ESTUDIANTE

La atención a los alumnos del Curso se realizará por el equipo docente a través de los siguientes medios:
- Foros en la plataforma aLF: el método preferente de consultas será el uso de los foros de la asignatura habilitados en la plataforma aLF.
- Atención telefónica y presencial: se realizará en los horarios indicados para cada profesor.
En el **Departamento de Derecho penal y Criminología** de la UNED –Facultad de Derecho de la UNED, C/ Obispo Trejo, 2, planta 3ª, 28040 MADRID–:
Prof. Dra. D.ª Alicia Gil Gil: Despacho 3.41 (martes 10:00-14:00), tel: (+34) 91 398 61 46
Prof. Dr. D. Sergio Cámara García. Despacho 3.52 (martes 10:00-14:00 - guardia del departamento martes 16:00-20:00), tel.: (+34) 91 398 80 54.
Prof. Dra. D.ª Ascensión García Ruiz. Despacho 3.40 (martes de 10 a 14:00 horas) guardia del departamento martes de 15:30 a 19:30 horas. Tef.: 913987004.
Prof. D. Daniel Fernández Bermejo. Despacho 3.48. (martes de 11:00 a 14:00 horas) Tef.: 91 398 6948.
Prof. Alfredo Liñán Lafuente. Miércoles lectivos de 16:30 a 19:30 horas, tel.: 91 398 7004
- Correo electrónico: pueden por último realizarse consultas por correo electrónico en la siguiente dirección:
alumnos.criminologia@der.uned.es

Y en el **Departamento de Sistemas de Comunicación y Control**
C/ Juan del Rosal 16. 28040. Madrid

Prof. Dra. D.ª María de los Llanos Tobarra Abad
Horario: Miércoles de 10:00 a 14:00 horas.
Email: llanos@scc.uned.es
Tfno: 913989566

Prof. Dr. D. Roberto Hernández
Horario martes de 15.00 a 19.00 h
Email: roberto@scc.uned.es
Tfno: 913957198

D. Antonio Robles Gómez
Lunes de 10:00 a 14:00 horas

Como criterio general obligatorio, la comunicación y relación con los alumnos se realizará exclusivamente desde el correo de alumno UNED.

TUTORIZACIÓN EN CENTROS ASOCIADOS

En el enlace que aparece a continuación se muestran los centros asociados y extensiones en las que se imparten tutorías de la asignatura. Estas pueden ser:

•**Tutorías de centro o presenciales**: se puede asistir físicamente en un aula o despacho del centro asociado.

•**Tutorías campus/intercampus**: se puede acceder vía internet.

Consultar horarios de tutorización de la asignatura 66044186

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

CE. 33 - Ser capaz de analizar interdisciplinariamente las causas, factores y consecuencias de la delincuencia, así como las nuevas formas de criminalidad, los contextos en los que se realiza y las medidas destinadas a su prevención.

CE. 34 - Ser capaz de conocer las técnicas y métodos para el análisis de las diferentes muestras de interés criminalístico, la correcta interpretación de los resultados y la elaboración de informe forenses.

CE. 35 - Ser capaz de conocer la relación entre contexto y vulnerabilidad social, delito y delincuente.

CG. 01 - Fortalecer la capacidad de aprendizaje autónomo y de adaptación a nuevos desarrollos de la actividad delictiva y su prevención y tratamiento.

CG. 03 - Conocer y comprender los lenguajes jurídico, sociológico, psicológico y técnico necesarios para el manejo correcto de los conceptos utilizados en las diversas disciplinas, así como sus repercusiones en el ámbito propio de la criminología.

CG. 04 - Saber integrar las diversas perspectivas de análisis del fenómeno delictivo (jurídica, psicológica, sociológica, etc.) para una comprensión plena del mismo, como es propia de la criminología, pudiendo desarrollar respuestas

CG. 05 - Comprender la complejidad y diversidad del fenómeno criminal en un mundo globalizado.

CG. 06 - Ser capaz de utilizar los diversos conocimientos adquiridos en los distintos sectores de la criminología, tanto desde una perspectiva teórica como práctica, sabiendo manejar igualmente perspectivas explicativas o predictivas, descriptivas o normativas

CG. 07 - Desarrollar la capacidad de iniciativa y motivación para el desempeño profesional en el ámbito de la Criminología.

CG. 08 - Conformar la capacidad para la crítica y autocrítica constructivas, tanto respecto a planteamientos teóricos como normativos y prácticos relacionados con la criminología.

CG. 09 - Ser capaz de desarrollar trabajo en equipo con otros profesionales de la actividad criminológica, desarrollando habilidades de liderazgo y coordinación.

CG. 10 - Saber gestionar y organizar la información tanto respecto a la recogida de datos, como al manejo de bases de datos y su presentación, fortaleciendo la utilización de las TIC como herramienta básica en el ámbito de la criminología.

CG. 11 - Saber poner en práctica las visiones sociológica, psicológica y jurídica en los ámbitos profesionales relacionados con el fenómeno delictivo.

CG. 12 - Ser capaz de elaborar estrategias de prevención e intervención en el ámbito criminológico, victimológico, marginalidad, etc., garantizando la seguridad ciudadana, los derechos fundamentales y la solución de los conflictos sociales.

RESULTADOS DE APRENDIZAJE

Al finalizar el curso el estudiante deberá
-Conocer los fundamentos de seguridad en tecnología informática
-Conocer las particularidades de la criminalidad relacionada con las TIC
-Conocer los cibercrímenes en particular.
-Conocer los retos del futuro en el ámbito de la cribercriminalidad
-Ser capaz de aplicar los conocimientos adquiridos a la resuolución de supuestos prácticos.

CONTENIDOS

Índice

Parte I: Fundamentos de seguridad en tecnología informática

En este bloque se trasmiten al estudiante los conceptos básicos e ideas clave relativos a la seguridad y a la tecnología informática para que sea capaz después de comprender las especiales condiciones, mecanismos y carácterístias de la criminalidad cometida a través de las TIC

1.

La Seguridad informática

I. LA ESTANDARIZACIÓN

II. LA SEGURIDAD

III. AMENAZAS, VULNERABILIDADES, ATAQUES (*HACKING*) Y GESTIÓN DE RIESGOS

2.

Fundamentos de tecnología informática

I. FUNDAMENTOS DE COMPUTADORES

II. FUNDAMENTOS DE REDES

III. CÓDIGOS MALICIOSOS

IV. REDES SOCIALES E INTERNET

Parte 2. Aspectos penales y criminológicos de la criminalidad relacionada con las TIC. Cuestiones generales

En este bloque nos adentramos en cuestiones criminológicas generales propias de la cibercriminalidad, así como en otros aspectos comunes a estos delitos, como la legislación aplicable o las particularidades que presenta la prueba en este ámbito delictivo.

3.

Particularidades de la criminalidad relacionada con las TIC

I. INTRODUCCIÓN

II.LOS SISTEMAS DE INFORMACIÓN Y SUS FUNCIONES COMO OBJETO DE PROTECCIÓN

III. LAS NUEVAS TECNOLOGÍAS COMO NUEVAS FORMAS DE ATAQUE A BIENES JURÍDICOS TRADICIONALES
IV. EL CIBERDELINCUENTE
V. PERFIL VICTIMOLÓGICO
VI. LA PRUEBA EN EL CIBERCRIMEN

4.

El cibercrimen. Definición, clasificación y marco legislativo

I. TERMINOLOGÍA
II. CLASIFICACIÓN DE LOS CIBERCRÍMENES
III. MARCO LEGISLATIVO

Parte 3. Los cibercrímenes en particular.

En este bloque analizamos las particularidades penales y criminológicas de cada uno de la ciberdelitos.

5.

Cibercrímenes en sentido estricto

I. HACKING
II. MALWARE INFORMÁTICO

6.

Cibercrímenes en sentido amplio

I. NUEVAS TIPOLOGÍAS DELICTIVAS
II. NUEVAS MODALIDADES DE COMISIÓN PARA DELITOS CLÁSICOS

7.

Los retos del futuro

I. RELATIVOS A LA INFORMACIÓN
II. RELATIVOS A LA CRIPTOGRAFÍA
III. OTROS

METODOLOGÍA

Para afrontar el estudio de *Criminalidad y Seguridad Informática* es conveniente seguir el orden previsto en el Programa.
La metodología de aprendizaje es a distancia y se utilizará la plataforma como complemento del estudio de los textos básicos. Así, habrá trabajo de tipo teórico (estudio de los materiales didácticos, en concreto la bibliografía básica de obligado conocimiento) y de tipo práctico (aprendizaje autorregulado). En la plataforma se abrirán diversos foros para la interacción de los estudiantes.
Se recomienda seguir los siguientes pasos para el estudio de la asignatura y de cara a la preparación de los exámenes:
a) Lectura detenida comprensiva de las lecciones del programa empleando para ello el texto básico recomendado y siguiendo el orden del mismo.

b) Resolución de los ejercicios de autoevaluación que aparecen al final de cada lección y de los supuestos prácticos.
c) Consulta de las dudas que puedan surgir de dicha lectura y de la realización de los ejercicios en el foro de la lección correspondiente de la plataforma y en las tutorías presenciales en caso de que el estudiante asista a las mismas.
d) Memorización de contenidos una vez que se hayan comprendido en su totalidad. Repaso/s de cara a la prueba presencial en función de las necesidades de cada estudiante.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen tipo test
Preguntas test	20
Duración del examen	60 (minutos)

Material permitido en el examen

Ninguno

Criterios de evaluación

El examen consiste en 20 preguntas tipo test que versarán sobre la materia del programa y podrán ser de tipo teórico propiamente dicho o referidas a pequeños supuestos o casos prácticos.

% del examen sobre la nota final	100
Nota del examen para aprobar sin PEC	5
Nota máxima que aporta el examen a la calificación final sin PEC	10
Nota mínima en el examen para sumar la PEC	7,5

Comentarios y observaciones

La prueba presencial consistirá en la realización de un test de 20 preguntas. Cada una de las preguntas tendrá 4 posibles respuestas, de las que solo una será correcta. Cada pregunta respondida correctamente puntuará 0,5; cada respuesta errónea descontará 0,1; las preguntas que no se contesten no descontarán puntuación.

La prueba tendrá una duración de 60 minutos.

Para superar la asignatura es necesario obtener una calificación mínima de 5 .

Revisiones de exámenes:

Las revisiones de exámenes deberán realizarse siguiendo la normativa establecida por la Universidad publicada en la página de la Facultad de Derecho.

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?	Si

Descripción

Las pruebas de evaluación continua (PEC) forman parte de la actividad formativa del estudiante. Su realización permitirá que éste evalúe el avance de su proceso de aprendizaje y podrá incidir en la calificación final.

La prueba consistirá en la realización de varias preguntas tipo test, propuestas a partir de un supuesto práctico, texto legal, fragmento de resolución judicial, etc.

La realización de estas actividades es voluntaria.

La PEC es una prueba no presencial. Se realizará en la plataforma el día y hora que el equipo docente de la asignatura determinará. Fuera de la plataforma virtual no es posible realizar las PEC.

Criterios de evaluación

La nota de la PEC solo sube la calificación final de la asignatura, nunca la baja. La nota de la PEC solo se suma a la nota del examen si la PEC se ha aprobado y en el examen se ha obtenido una calificación de 7.5 o superior.

La PEC será valorada con un máximo de 2,5 puntos.

Para hacer el cómputo de la nota, las respuestas se valoran sobre 10, de manera que si se formulan 5 preguntas cada respuesta correcta se computará con 2 puntos, y a cada fallo corresponderá un descuento de 0,5, y el resultado final se divide por 4 para ajustarlo al valor final de 2,5.

Ponderación de la PEC en la nota final	Cada una de las PEC servirá; SOLO para subir la nota del examen parcial correspondiente siempre que se den los siguientes requisitos: 1.-Calificación de la PEC: Se debe aprobar la PEC, esto es, se debe obtener un mínimo de 1,25 puntos sobre los 2,5 posibles; y ·2.- Nota de corte en la prueba presencial: Es preciso alcanzar en la prueba presencial correspondiente al menos 7,5 puntos de los 10 posibles. Se guarda la nota de la PEC para septiembre.
Fecha aproximada de entrega	Se publicará en la plataforma aLF
Comentarios y observaciones	

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?	No
Descripción	
Criterios de evaluación	
Ponderación en la nota final	
Fecha aproximada de entrega	
Comentarios y observaciones	

¿CÓMO SE OBTIENE LA NOTA FINAL?

La calificación final de la asignatura se realizará teniendo en cuenta las siguientes posibilidades:

A) Si únicamente se realizan la prueba presencial:

Si el estudiante decide no realizar la evaluación continua, la calificación final de la asignatura será la nota de la prueba presencial .

B) Si se opta por la realización de la PEC:

Si el estudiante opta por la evaluación continua y realiza la PEC, la nota de esta servirá solo para sumar, hasta una puntuación máxima de 10 , siempre que la PEC se haya aprobado (es decir, se haya alcanzado en la misma una puntuación de 1.25, de los 2.5 puntos posibles) y en el examen se haya alcanzado la puntuación mínima de 7.5.

De esta manera, por ejemplo:

-Un estudiante que haya obtenido 7.5 en el examen y 2.5 en la PEC obtendrá la calificación final de 10.

-Un estudiante que haya obtenido un 8 en el examen y 1.25 en la PEC obtendrá la calificación final de 9.25.

-Un estudiante que haya obtenido un 7 en el examen y 2.5 en la PEC obtendrá la calificación final de 7.

La PEC no servirá para adjudicar las matrículas de honor, que se asignarán teniendo en cuenta la nota del examen.

BIBLIOGRAFÍA BÁSICA

ISBN(13):9788413242699
Título:CIBERCRIMINALIDAD, 2019
Autor/es:Roberto Hernández Berlinches (Coords.) ; Alicia Gil Gil ;
Editorial:: DYKINSON

BIBLIOGRAFÍA COMPLEMENTARIA

Se proporcionará al estudiante en el curso virtual.

RECURSOS DE APOYO Y WEBGRAFÍA

Los medios de apoyo que podrá utilizar el estudiante son, además del curso virtual:
Las tutorías que se imparten en los centros asociados de la UNED.
La red de bibliotecas de la UNED.
Posibles programas radiofónicos, que se anunciarán a lo largo del curso.
Otros recursos disponibles en internet.
El uso de estos recursos forma parte del conjunto formativo y de adquisición de habilidades.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.