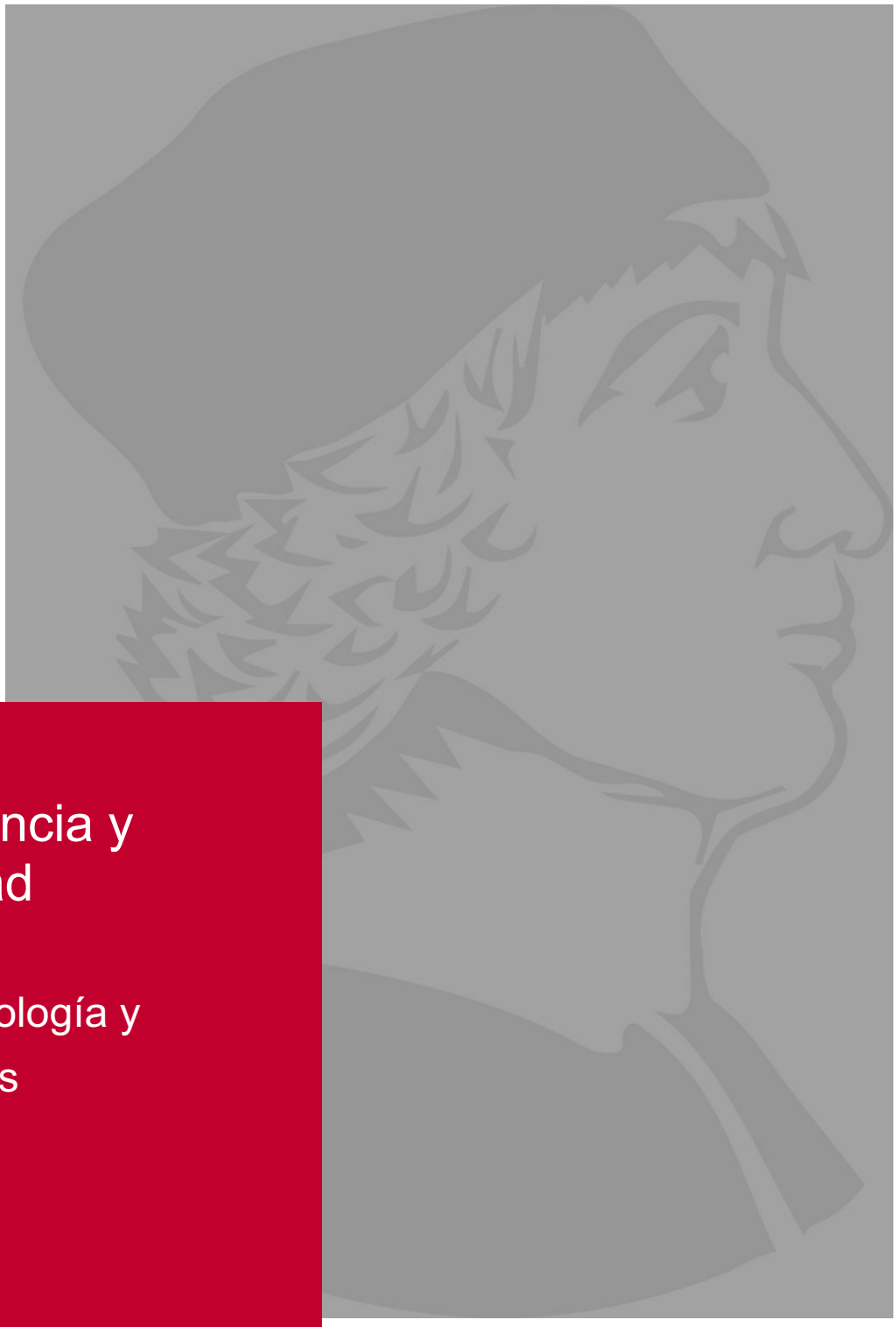

Ciberdelincuencia y Ciberseguridad

Grado en Criminología y Ciencias forenses

UNIVERSIDAD NEBRIJA

GUÍA DOCENTE

Asignatura: Ciberdelincuencia y Ciberseguridad

Titulación: Grado en Criminología y Ciencias forenses

Carácter: Obligatoria

Idioma: Castellano

Modalidad: Presencial/semipresencial/a distancia

Créditos: 6

Semestre: 2º

Profesores/Equipo Docente: D. Ivan Portillo Morales

1. CONOCIMIENTOS, HABILIDADES Y COMPETENCIAS

Conocimientos o contenidos (Knowledge)

- K1: Analizar desde un ámbito local, autonómico, nacional e internacional la delincuencia, el delincuente, la víctima y el control social.
- K2: Reunir e interpretar datos relevantes relacionados con su ámbito de conocimiento.
- K4: Transmitir, mediante un conocimiento profundo, las diferentes teorías criminológicas, para dar explicación de un fenómeno delictivo.
- K6: Describir las transformaciones y evolución de las sociedades en sus diferentes ámbitos con el objetivo de identificar patrones de conducta repetibles o mecanismos de prevención eficaces.
- K7: Enunciar la dimensión social del ser humano, desde sus procesos de socialización e influencia, evolución socio-cultural e histórico, las dinámicas de los colectivos y grupos humanos, así como las instituciones sociales fundamentales desde un punto de vista criminológico.
- K8: Listar y enumerar los fundamentos biológicos de la conducta humana y su relación con las funciones psicológicas.
- K9: Identificar desde un punto de vista empírico y multidisciplinar las distintas infracciones penales.
- K11: Conocer las diferentes políticas de protección a víctimas de un hecho delictivo, analizando el proceso de victimización y los efectos que provoca en las víctimas.

Habilidades o destrezas (Skills)

- H1: Aplicar con pensamiento crítico las principales teorías criminológicas sobre los distintos fenómenos delictivos.
- H2: Relacionar, manejar e interpretar las principales fuentes de datos sobre delincuencia y victimización y, en consecuencia, elaborar explicaciones básicas sobre las formas específicas de criminalidad.
- H3: Describir el marco jurídico penal y procesal de respuesta ante el delito, el delincuente y la desviación, así como identificar el marco legal relativo a los derechos y recursos de las víctimas.
- H5: Analizar y utilizar correctamente los métodos más adecuados para obtener información precisa, en cada caso, de víctimas, testigos y delincuentes.

Competencias (Competences)

- C1: Dar respuesta al fenómeno criminal, aplicando los conocimientos de perfilación criminal, control social, prevención y reacción delictiva, para los diferentes contextos de tipología delictiva que nos encontramos en la sociedad.
- C2: Aplicar las conclusiones técnicas de diferentes informes para ofrecer una solución específica a la prevención o reinserción de la delincuencia, así como el fomento de mecanismos de resiliencia en las víctimas.
- C5: Divulgar y comunicar de forma eficaz, entre otros, a destinatarios, profesionales, responsables institucionales y población general, los resultados obtenidos de su investigación.

2.- CONTENIDOS

2.1. Requisitos previos

Ninguno.

2.2. Descripción de los contenidos

La asignatura de Ciberdelincuencia y Ciberseguridad es una parte fundamental del Grado en Criminología, diseñada para proporcionar a los estudiantes una comprensión integral de los delitos que se cometen en el ciberespacio y las medidas de seguridad necesarias para prevenir y mitigar estos crímenes. En un mundo cada vez más digitalizado, donde las infraestructuras críticas, los datos personales y los sistemas económicos dependen de la tecnología, la ciberseguridad se ha convertido en una prioridad global. Esta asignatura combina aspectos técnicos, legales y criminológicos para formar a los estudiantes en la identificación, análisis y prevención de la ciberdelincuencia.

El curso comienza con una introducción a la ciberdelincuencia, donde se exploran las diferentes tipologías de delitos que se cometen en el entorno digital. Los estudiantes aprenderán a identificar y clasificar los delitos cibernéticos más comunes, como el hacking, el phishing, la distribución de malware, la suplantación de identidad, el ciberacoso, y el fraude digital. Se discutirán también las características específicas de los delincuentes cibernéticos y las motivaciones que los llevan a cometer estos crímenes, abarcando desde el ciberdelincuente solitario hasta las organizaciones criminales complejas que operan a escala global.

2.3. Contenido detallado

Tema 1.- Introducción a la ciberdelincuencia
Tema 2.- Motivaciones y perfiles de los ciberdelincuentes
Tema 3.- Ciberseguridad básica y medidas preventivas
Tema 4.- Marco legal y jurídico
Tema 5.- Victimología cibernética
Tema 6.- Criminología aplicada al ciberespacio
Tema 7.- Análisis y respuesta ante incidentes de seguridad informática
Tema 8.- Ingeniería social y técnicas de manipulación
Tema 9.- Infraestructuras críticas y ciberseguridad nacional
Tema 10.- Delitos cibernéticos emergentes
Tema 11.- Cooperación internacional y políticas de ciberseguridad
Tema 12.- Ética en la ciberseguridad

3. Actividades formativas

MATERIA / ASIGNATURA, CON CARÁCTER	ACTIVIDADES FORMATIVAS	Horas totales	(% presencialidad) Horas presenciales (8-12)
	A1.- Clase magistral	315	315 (100%)

PRESENCIAL	A2.- Tutorías	14	14 (100%)
	A3.- Casos prácticos	35	35 (100%)
	A4.- Clases prácticas. seminarios y talleres	35	35 (100%)
	A5.- Estudio individual y trabajo autónomo	490	0 (0%)
	A6.- Trabajos individuales o en grupo de los estudiantes	80	0 (0%)
	A7.- Actividades a través de los recursos virtuales	46	0 (0%)
	A8.- Evaluación	35	35 (100%)
	Total	**1050**	**434**
	SISTEMAS DE EVALUACIÓN		
	Convocatoria Ordinaria		
	Modalidad presencial	**MÍNIMO**	**MÁXIMO**
	S1.- Asistencia y participación	0%	15%
	S2.- Prueba parcial	0%	25%
	S3.- Examen final presencial individual	50%	60%
	S4.- Presentación de trabajos y proyectos	10%	30%
	Total	**60%**	**130%**
	Convocatoria Extraordinaria		
	Modalidad presencial	**MÍNIMO**	**MÁXIMO**
	S3.- Examen final presencial individual	50%	90%
	S4.- Presentación de trabajos y proyectos	10%	50%
	Total	**60%**	**140%**

MATERIA / ASIGNATURA, CON CARÁCTER VIRTUAL	**ACTIVIDADES FORMATIVAS**	**¿Es síncrona?**	**Horas totales**	**Horas de interactividad síncrona (4-8)**
	A1.- Clase magistral	Sí	315	158 horas (50%)
	A2.- Tutorías	Sí	14	7 horas (50%)
	A3.- Casos prácticos	Sí	35	8 horas (23%)
	A4.- Clases prácticas. seminarios y talleres	Sí	35	8 horas (23%)
	A5.- Estudio individual y trabajo autónomo	No	490	0 horas (0%)
	A6.- Trabajos individuales o en grupo de los estudiantes	No	70	0 horas (0%)
	A7.- Actividades a través de los recursos virtuales	No	70	0 horas (0%)
	A8.- Evaluación	Es presencial	21	21 (100% presencial)
	Total		**1050**	**202**
	SISTEMAS DE EVALUACIÓN			
	Convocatoria Ordinaria			
	Modalidad virtual		**MÍNIMO**	**MÁXIMO**
	S1.- Asistencia y participación		10%	20%
	S3.- Examen final presencial individual		50%	70%
	S4.- Presentación de trabajos y proyectos		15%	25%
	Total		**75%**	**115%**
	Convocatoria Extraordinaria			
	Modalidad virtual		**MÍNIMO**	**MÁXIMO**
	S3.- Examen final presencial individual		60%	80%
	S4.- Presentación de trabajos y proyectos		20%	40%
	Total		**80%**	**120%**

MATERIA / ASIGNATURA, CON CARÁCTER HÍBRIDA	**DISTRIBUCIÓN DE ASIGNATURAS POR MODALIDAD**	
	Asignaturas	**Modalidad**
	Asignatura 3.1.- Perfilación criminal	Presencial
	Asignatura 3.2.- Ciberdelincuencia y ciberseguridad	Presencial
	Asignatura 3.3.- Entrevista criminológica y psicología del testimonio	Presencial
	Asignatura 3.4.- Terrorismo y delincuencia organizada	Virtual
	Asignatura 3.5.- Delincuencia juvenil	Virtual
	Asignatura 3.6.- Criminalidad económica y de la empresa	Virtual
	Asignatura 3.7.- Violencia de género y doméstica	Virtual

ACTIVIDADES FORMATIVAS ASIGNATURAS CON MODALIDAD PRESENCIAL		Horas totales	(% presencialidad) Horas presenciales (8-12)
A1.- Clase magistral		135	135 (100%)
A2.- Tutorías		6	6 (100%)
A3.- Casos prácticos		15	15 (100%)
A4.- Clases prácticas. seminarios y talleres		15	15 (100%)
A5.- Estudio individual y trabajo autónomo		210	0 (0%)
A6.- Trabajos individuales o en grupo de los estudiantes		35	0 (0%)
A7.- Actividades a través de los recursos virtuales		19	0 (0%)
A8.- Evaluación		15	15 (100%)
Total		**450**	**186**
ACTIVIDADES FORMATIVAS ASIGNATURAS CON MODALIDAD VIRTUAL	**¿Es síncrona?**	**Horas totales**	**Horas de interactividad síncrona (4-8)**
A1.- Clase magistral	Sí	180	90 horas (50%)
A2.- Tutorías	Sí	8	4 horas (50%)
A3.- Casos prácticos	Sí	20	5 horas (25%)
A4.- Clases prácticas. seminarios y talleres	Sí	20	5 horas (25%)
A5.- Estudio individual y trabajo autónomo	No	280	0 horas (0%)
A6.- Trabajos individuales o en grupo de los estudiantes	No	40	0 horas (0%)
A7.- Actividades a través de los recursos virtuales	No	40	0 horas (0%)
A8.- Evaluación	Es presencial	12	12 (100% presencial)
Total		**600**	**116**

4. SISTEMA DE EVALUACIÓN

Sistemas de evaluación:
El sistema de calificaciones (R.D. 1125/2003, de 5 de septiembre) será el siguiente:
0 – 4,9 Suspenso (SS)
5,0 – 6,9 Aprobado (AP)
7,0 – 8,9 Notable (NT)
9,0 – 10 Sobresaliente (SB)

La mención de "matrícula de honor" se podrá otorgar a alumnos que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en la materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola "Matrícula de Honor".

SISTEMAS DE EVALUACIÓN ASIGNATURAS CURSADAS EN MODALIDAD PRESENCIAL		
Convocatoria Ordinaria		
Modalidad presencial	**MÍNIMO**	**MÁXIMO**
S1.- Asistencia y participación	0%	15%
S2.- Prueba parcial	0%	25%
S3.- Examen final presencial individual	50%	60%
S4.- Presentación de trabajos y proyectos	10%	30%
Total	**60%**	**130%**
Convocatoria Extraordinaria		
Modalidad presencial	**MÍNIMO**	**MÁXIMO**
S3.- Examen final presencial individual	50%	90%

S4.- Presentación de trabajos y proyectos	10%	50%
Total	**60%**	**140%**
SISTEMAS DE EVALUACIÓN ASIGNATURAS CURSADAS EN MODALIDAD VIRTUAL		
Convocatoria Ordinaria		
Modalidad virtual	**MÍNIMO**	**MÁXIMO**
S1.- Asistencia y participación	10%	20%
S3.- Examen final presencial individual	50%	70%
S4.- Presentación de trabajos y proyectos	15%	25%
Total	**75%**	**115%**
Convocatoria Extraordinaria		
Modalidad virtual	**MÍNIMO**	**MÁXIMO**
S3.- Examen final presencial individual	60%	80%
S4.- Presentación de trabajos y proyectos	20%	40%
Total	**80%**	**120%**

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima
En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5. BIBLIOGRAFÍA

Lastra Sánchez, Carlos, Claudio García Martorell, and Deusto Formación. 2022. *Ciberseguridad*. Segunda edición: mayo de 2022. Barcelona (España): Deusto Formación.

Pérez Bes, Francisco. 2021. *Ciberseguridad*. Madrid: Lefebvre-El Derecho.

Romeo Casabona, Carlos María, and María Ángeles Rueda Martín, eds. 2023. *Derecho Penal, Ciberseguridad, Ciberdelitos E Inteligencia Artificial*. Albolote (Granada): Comares.