UNIVERSIDAD DEL ATLÁNTICO MEDIO

GUÍA DOCENTE

HABILIDADDES DIGITALES PARA EL SIGLO XXI

GRADO EN DERECHO

MODALIDAD VIRTUAL

CURSO ACADÉMICO 2023-2024

ÍNDICE

RESUMEN 3
DATOS DEL PROFESORADO 3
REQUISITOS PREVIOS 3
COMPETENCIAS 4
RESULTADOS DE APRENDIZAJE 5
CONTENIDOS DE LA ASIGNATURA 6
METODOLOGÍA 8
ACTIVIDADES FORMATIVAS 9
EVALUACIÓN 9
BIBLIOGRAFÍA 11

RESUMEN

Centro	Facultad de Ciencias Sociales y Jurídicas		
Titulación	Grado en Derecho		
Asignatura	Habilidades Digitales para el Siglo XXI	**Código**	F1C1G07047
Materia	Elementos de Intensificación para el Estudio del Derecho de las TIC (virtual)		
Carácter	Optativa		
Curso	4º		
Semestre	1º		
Créditos ECTS	6		
Lengua de impartición	Castellano		
Curso académico	2023-2024		

DATOS DEL PROFESORADO

Responsable de Asignatura	
Correo electrónico	@pdi.atlánticomedio.es
Teléfono	828.019.019
Tutorías	Consultar horario de tutorías en el campus virtual. El horario de atención al estudiante se publicará al inicio de curso en el Campus Virtual. En caso de incompatibilidad con las franjas horarias establecidas pueden ponerse en contacto a través del *mail* para concertar una tutoría fuera de este horario. Se ruega que se solicite la tutoría a través del Campus Virtual o a través del correo electrónico.

REQUISITOS PREVIOS

Sin requisitos previos.

COMPETENCIAS

Competencias básicas:

CB1

Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

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.

CB5

Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

Competencias transversales:

CT1

Capacidad para la resolución de problemas y toma de decisiones

CT2

Capacidad de trabajo en equipo y en entornos diversos y multiculturales

CT3

Adquisición de conceptos vinculados a la sensibilidad hacia la diversidad y compromiso étnico.

CT4

Capacidad de tener conciencia crítica sobre las realidades sociales y las corrientes de pensamiento.

CT5

Capacidad para dominar las competencias digitales.

Competencias específicas:

CE26

Conocimiento de la informática básica en todos sus aspectos, referidos fundamentalmente al mundo del derecho. Capacidad de manejo de las bases de datos del Derecho.

RESULTADOS DE APRENDIZAJE

Cuando el estudiante supere esta asignatura será capaz de:

- Que el alumno complete su formación con la asistencia a actividades universitaria culturales, deportivas, de representación estudiantil, solidarias y de cooperación.
- Tener la capacidad de recopilar e interpretar datos e informaciones sobre las que fundamentar sus conclusiones incluyendo, cuando sea preciso y pertinente, la reflexión sobre asuntos de índole social, científica o ética en el ámbito de su campo de estudio. Ser capaces de desenvolverse en situaciones complejas o que requieran el desarrollo de nuevas soluciones tanto en el ámbito académico como laboral o profesional dentro de su campo de estudio.
- Saber comunicar a todo tipo de audiencias (especializadas o no) de manera clara y precisa, conocimientos, metodologías, ideas, problemas y soluciones en el ámbito de su campo de estudio

1. Jornada, seminarios u otras actividades universitarias culturales, deportivas, de representación estudiantil, solidarias y de cooperación.
2. Estructura del relato. Historia universal y progreso. Aceleración, revolución y utopía. Políticas de la memoria. Crisis de los metarrelatos, fin de la historia y posmodernidad. Framing y comunicación. Persona e identidad narrativa.
3. Introducción al ecosistema informático.
4. Ofimática básica: procesador de textos.
5. Ofimática básica: hoja de cálculo.
6. Ofimática básica: presentaciones eficaces.
7. Búsqueda y gestión de la información.
8. Manejo y tratamiento de imagen digital.

Estos contenidos se desarrollarán por medio del siguiente programa:

1.- Redes informáticas.

- 1.1 -Modelo OSI.
- 1.2 - Introducción al encapsulamiento.
- 1.3 - Modelo TCP/IP.
- 1.4 - Dispositivos de red.
  - 1.4.1 - Concentradores (*hubs*).
  - 1.4.2 - Conmutadores (*switches*).
  - 1.4.3 - Encaminadores (*routers*)
  - 1.4.4 - Cortafuegos (*firewall*)
  - 1.4.5 – Servidores: DHCP, DNS y proxy.
- 1.5 - Direccionamiento IP.
  - 1.5.1 - Clase de redes.
  - 1.5.2 – IPv4.
  - 1.5.3 - IPv6.
- 1.6 - Redes inalámbricas.
  - 1.6.1 - Infraestructura de redes inalámbricas.
  - 1.6.2 - Protocolos WEP, WPA, WPA2, WPA3.

2.- Sistemas operativos.

2.1 - Fundamentos de sistemas operativos.

2.2 - Funciones de un sistema operativo.

2.3 – Tipologías.

2.3.1 – MS/DOS.

2.3.2 – UNIX.

2.3.3 – Linux.

2.3.4 – Windows.

2.3.5 - MAC OS.

2.4 - Sistemas operativos móviles.

2.4.1 – iOS.

2.4.2 - Android.

2.5 - Sistemas de almacenamiento.

2.6 - Sistemas de archivos.

3.- Ciberdelincuencia y agentes de la amenaza digital.

3.1 – Ciberdelincuencia objetiva: manifestaciones de la delincuencia digital.

3.1.1 - Botnet.

3.1.2 - Business E-mail Compromise.

3.1.3 - Cartas nigerianas.

3.1.4 - Cryptojacking.

3.1.5 - Denegación de servicio.

3.1.6 - Ingeniería social.

3.1.7 - Inyección SQL.

3.1.8 - Malware.

3.1.9 - Pharming.

3.1.10 - Phishing.

3.1.11 - Spear phishing.

3.1.12 - Ransomware.

3.1.13 - Skimming.

3.1.14 - Spoofing.

3.1.15 - Spyware y Troyano.

3.2 – Ciberdelincuencia subjetiva: los cibercriminales.

3.2.1 - Crime as Service.

3.2.2 - Hacktivistas.

3.2.3 - Insider threat.

3.2.4 - APTs.

3.2.5 - Cyber Kill Chain.

4.- Dato, información e inteligencia.

4.1 - Tipologías de Inteligencia.

4.2 - Ciclo de la Inteligencia.

4.3 - Inteligencia de Fuentes Abiertas (OSINT).

4.4 - Surface Web.

4.5 - Deep Web.

4.6 - Dark Web.

4.7 – Darknet.

4.8 - Ciencia de Datos.

4.9 - Big Data.

4.10 - Cloud Computing.

5.- Seguridad de la Información.

5.1 - Ciclo de vida de la información.

5.2 – Confidencialidad de la información.

5.3 - Integridad y disponibilidad de la información.

5.4 - Sistema de gestión de la Seguridad de la Información.

5.5 - Riesgos y amenazas para la información.

6.- Ofimática básica.

6.1 – Procesador de texto

6.2 – Hoja de cálculo

6.3 – Presentaciones eficaces

6.4 – Organización y gestión de la información digital

METODOLOGÍA

- Exposición / lección magistral
- Aprendizaje constructivo y práctico
- Aprendizaje autónomo
- Estudio dirigido

ACTIVIDADES FORMATIVAS

Elaboración de informes y/o dictámenes	40,6 horas
Clases magistrales participativas	35,2 horas
Resolución de problemas o supuestos prácticos	20,2 horas
Trabajo autónomo	73 horas
Tutorías	1,4 horas

EVALUACIÓN

	% CALIFICACIÓN FINAL
Examen (teórico y/o práctico)	50 %
Evaluación de trabajos	50%

Sistemas de evaluación

A) <u>Sistema de evaluación de la convocatoria ordinaria</u>

Se aplicará el sistema de evaluación continua por asignatura donde se valorará de forma integral los resultados obtenidos por el estudiante mediante los procedimientos de evaluación indicados.

La evaluación es el reconocimiento del nivel de competencia adquirido por el estudiante y se expresa en calificaciones numéricas, de acuerdo con lo establecido en la legislación vigente.

1. **Evaluación de los conocimientos teórico-prácticos (50% de la nota final):**

   Se valorará mediante la realización de un examen final obligatorio y presencial que adoptará la forma de preguntas de desarrollo y, en su caso, de test. Constará de una parte teórica y de una parte práctica. Esta prueba comprenderá preguntas para valorar las competencias previstas en la asignatura y otra parte dedicada a la verificación del trabajo realizado en la evaluación continua (evaluación de trabajos).

2. **Evaluación de trabajos (50% de la nota final):**

   Se valorará mediante la entrega de trabajos y actividades que se propongan a lo largo del curso a través del campus virtual para la comprobación de la adquisición por parte del estudiante de las competencias descritas en esta guía docente.

B) **<u>Sistema de evaluación de la convocatoria extraordinaria</u>**

En convocatoria extraordinaria se evaluará a través del mismo sistema de evaluación que en la convocatoria ordinaria.

C) Si se hubiera superado en convocatoria ordinaria el examen final o la evaluación de los trabajos, se mantendrá la nota para la convocatoria extraordinaria. Por tanto, el alumno tendrá que realizar las pruebas que tenga pendiente de aprobación, mediante nuevos trabajos o la presentación al examen de esta convocatoria. Las calificaciones solo se guardarán para las convocatorias asociadas a la presente guía docente.

Criterios de calificación

El criterio de calificación general consiste en que cada tarea se valora con una calificación de 0 a 10. Para realizar la aplicación de los porcentajes correspondientes, será necesario obtener al menos 4 puntos en cada una de las partes. Además, para superar la asignatura es necesario obtener una calificación mínima final de 5, como resultado de la media aritmética de los sistemas de evaluación previstos.

1. **Evaluación de los conocimientos teórico-prácticos**

a) Los conocimientos teóricos se evaluarán mediante un examen con un mínimo de tres preguntas de desarrollo medio y un test de 20 preguntas.

Las preguntas de desarrollo se valorarán en su conjunto con un máximo de 2,5 puntos del examen final. Las preguntas tipo test del examen final también se valorarán en su conjunto con un máximo de 2,5 puntos.

b) Los conocimientos prácticos se evaluarán mediante la realización de dos casos prácticos del tipo de los realizados a lo largo del curso.

Cada caso práctico se valorará con un máximo de 2,5 puntos del examen final.

Para superar el examen habrá de superarse tanto la parte teórica como la parte práctica, alcanzando una nota mínima de 2,5 puntos en cada una de ellas.

2. **Evaluación de los trabajos**

Se valorará mediante la entrega de al menos dos trabajos individuales de entrega obligatoria.

BIBLIOGRAFÍA

- **Básica:**
  - Behrouz, A. Forouzan. *Transmisión de datos y redes de comunicaciones*. McGraw Hill, 2021.
  - Ortega Candel, J.M. *Ciberseguridad: manual práctico*. Paraninfo, 2021.

- **Complementaria:**
  - Santa Cruz Chao, José Manuel. *La sociedad digital. Sociología, empresa y arquitectura del mundo digital.* OMM PRESS, 2020.