

Programación semanal

En la programación semanal te presentamos un **reparto del trabajo de la asignatura** a lo largo de las semanas del cuatrimestre.

	CONTENIDO TEÓRICO	ACTIVIDADES (15 puntos)	CLASES EN DIRECTO
Semana 1	<p>Tema 1. La informática forense. Nuevas tecnologías aplicadas a la prevención e investigación del ciberdelito.</p> <p>1.1. Introducción y objetivos 1.2. Fases de la informática forense 1.3. Herramientas informáticas forenses 1.4. La informática forense como medida preventiva.</p>	<p>Asistencia a 2 clases en directo a elegir a lo largo del cuatrimestre (0.15 puntos cada una)</p> <p>Test Tema 1 (0.1 puntos)</p>	<p>Presentación de la asignatura y clase del tema 1</p>
Semana 2	<p>Tema 2. Herramientas de ciberdelincuencia y ciberseguridad</p> <p>2.1. Introducción y objetivos 2.2. CCN-CERT 2.3. SAT-INET 2.3 SAT-SARA 2.5 SAT-ICS</p>	<p>Test tema 2 (0.1 puntos)</p>	<p>Clase del tema 2</p>
Semana 3	<p>Tema 2. Herramientas de ciberdelincuencia y ciberseguridad. (continuación)</p> <p>2.6 Niveles de Ciberinteligencia 2.7 OSINT y HUMINT</p>	<p>Actividad. Investigación en fuentes abiertas de un ciberdelito (5.25 puntos)</p>	<p>Clase del tema 2 y presentación de la actividad Investigación en fuentes abiertas de un ciberdelito</p>
Semana 4	<p>Tema 3. Huella digital y rastro de navegación. Fuentes de extracción de información. Dirección IP.</p> <p>3.1. Introducción y objetivos 3.2. La huella digital ¿Qué datos “regalamos”? ¿Quién y para qué se usan esos datos? 3.3. Protección de nuestra huella digital. 3.4. Derecho de supresión “al olvido” 3.5. Fuentes de extracción de información 3.6. Footprinting</p>	<p>Test Tema 3 (0.1 puntos)</p>	<p>Clase del tema 3</p>

	CONTENIDO TEÓRICO	ACTIVIDADES (15 puntos)	CLASES EN DIRECTO
Semana 5	<p>Tema 4. Derechos fundamentales e investigación criminal. Cooperación internacional en la investigación</p> <p>4.1. Introducción y objetivos 4.2. Definiciones 4.3. Historia de ciberdelitos y consideraciones previas. 4.4. Acuerdos y resoluciones internacionales respecto de la ciberseguridad en el ciberespacio. 4.5 Derechos fundamentales del investigado. 4.6 Cooperación Internacional. Órganos y directrices. 4.7. La Orden Europea de Investigación</p>	<p>Test Tema 4 (0.1 puntos)</p>	<p>Clase del tema 4</p>
Semana 6	<p>Tema 5. Medidas de investigación realizadas por las Fuerzas y Cuerpos de Seguridad contra la ciberdelincuencia. Requisitos generales. Presupuestos y requisitos comunes a todas las medidas.</p> <p>5.1. Introducción y objetivos 5.2. Órganos competentes especializados en la persecución de conductas ciberdelictivas. 5.3 Medidas de investigación como garantía de legalidad en el proceso de obtención de las pruebas. 5.4. Artículo 588 bis de la LECrim. Jurisprudencia.</p>	<p>Test Tema 5 (0.1 puntos)</p>	<p>Clase del tema 5</p>
Semana 7	<p>Tema 6. Entradas y registros: preparación para llevarlas a cabo, formalidades, búsqueda de información y análisis de dispositivos.</p> <p>6.1. Introducción y objetivos 6.2. Orden de entrada y Registro. 6.3. Proceso de recogida de los dispositivos digitales 6.4 Análisis de los dispositivos digitales incautados en un registro. 6.5. Cadena custodia. Ejemplo práctico.</p>	<p>Actividad Grupal. Preparación de un dispositivo de entrada y registro (3 puntos)</p> <p>Test Tema 6 (0.1 puntos)</p>	<p>Clase del tema 6 y presentación de la actividad grupal Preparación de un dispositivo de entrada y registro</p>

	CONTENIDO TEÓRICO	ACTIVIDADES (15 puntos)	CLASES EN DIRECTO
Semana 8	<p>Tema 7. Evidencia digital. Concepto y características de la prueba electrónica. El hacking legal. Respeto a los derechos fundamentales.</p> <p>7.1. Introducción y objetivos 7.2. Norma ISO/IEC 27037:2012 7.3. Como se obtiene una evidencia digital. 7.4. Hacking legal (Art. 588 septies). 7.5. Uso del hacking legal por las Unidades de Investigación de las FyCSE. 7.6. Derechos fundamentales del afectado.</p>	<p>Test Tema 7 (0.1 puntos)</p>	<p>Clase del tema 7 y resolución de la actividad Investigación en fuentes abiertas de un cibercrimen</p>
Semana 9	<p>Tema 8. Agente encubierto informático.</p> <p>8.1. Introducción y objetivos 8.2. Creación y regulación de la figura del AEI (Agente Encubierto Informático) 8.3. Autorización judicial y control de la actuación del AEI</p>	<p>Actividad Solicitud y creación de un AEI (5.25 puntos)</p> <p>Test Tema 8 (0.1 puntos)</p>	<p>Clase del tema 8 y presentación de la actividad Solicitud y creación de un AEI</p>
Semana 10	<p>Tema 9: La interceptación de las comunicaciones telefónicas y telemáticas.</p> <p>9.1. Introducción y objetivos 9.2. Requisitos legales (artículo 588.bis.b) y control de la medida (artículo 588.ter.f).</p>	<p>Test Tema 9 (0.1 puntos)</p>	<p>Clase del tema 9</p>
Semana 11	<p>Tema 9: La interceptación de las comunicaciones telefónicas y telemáticas (continuación).</p> <p>9.3 SITEL (Sistema Integral de Interceptación de Comunicaciones) 9.4 Colaboración de las operadoras de servicios de telefonía e ISP.</p>		<p>Clase del tema 9</p>

	CONTENIDO TEÓRICO	ACTIVIDADES (15 puntos)	CLASES EN DIRECTO
Semana 12	<p>Tema 10. La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.</p> <p>10.1. Introducción y objetivos 10.2. Grabación de Conversaciones 10.3. ¿Es la grabación una prueba válida? 10.4. Hacking Legal. 10.5. Captación de correos electrónicos y mensajería en la empresa. 10.6. Captación y grabación de conversaciones mediante dispositivos electrónicos por parte de los FCCSS. 10.7. Balizamiento.</p>	<p>Test Tema 10 (0.1 puntos)</p>	<p>Clase del tema 10</p>
Semana 13	<p>Tema 11. La utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen. Supuestos de aplicación y métodos empleados. Espacios públicos y privados y relación con la intimidad.</p> <p>11.1. Introducción y objetivos 11.2. Concepto de Videovigilancia: fines de utilización. 11.3. Legitimación en el ejercicio de la videovigilancia: Regla general.</p>		<p>Clase del tema 11</p>
Semana 14	<p>Tema 11. La utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen. Supuestos de aplicación y métodos empleados. Espacios públicos y privados y relación con la intimidad (continuación).</p> <p>11.4. Legitimación en el proceso penal por FCCSE de utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. 11.5. Ejemplos de medios técnicos utilizados para la videovigilancia.</p>	<p>Test Tema 11 (0.1 puntos)</p>	<p>Clase del tema 11 y resolución de la actividad grupal Preparación de un dispositivo de entrada y registro</p>

	CONTENIDO TEÓRICO	ACTIVIDADES (15 puntos)	CLASES EN DIRECTO
Semana 15	<p>Tema 12: El registro de dispositivos de almacenamiento masivo de información.</p> <p>12.1. Introducción y objetivos 12.2. Circular 5/2019 12.3. Utilización del Agente Encubierto en el registro remoto de equipos 12.4. Medios técnicos</p>	<p>Test Tema 12 (0.1 puntos)</p>	<p>Clase del tema 12 y resolución de la actividad Solicitud y creación de un AEI</p> <p>Sesión de explicación del modelo de examen</p>
Semana 16	Semana de exámenes		

NOTA

Esta **Programación semanal** puede ser modificada si el profesor lo considera oportuno para el enriquecimiento de la asignatura.