

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

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

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

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

|           | CONTENIDO TEÓRICO  | ACTIVIDADES<br>(15 puntos)                  | CLASES EN DIRECTO  |
|-----------|--|---|--|
| Semana 15 | <p><b>Tema 12: El registro de dispositivos de almacenamiento masivo de información.</b></p> <p>12.1. Introducción y objetivos<br/>12.2. Circular 5/2019<br/>12.3. Utilización del Agente Encubierto en el registro remoto de equipos<br/>12.4. Medios técnicos</p> | <p><b>Test Tema 12</b><br/>(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 | <b>Semana de exámenes</b>  |   |  |

#### NOTA

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