



UNIVERSIDAD  
DEL ESTE  
LA PLATA

Actividades de Extensión



## DIPLOMATURA CIBERCRIMEN

Modalidad Virtual

### Cronograma de Trabajo Cohorte 2022

Fecha	Temario propuesto	Contenidos
<b>17 de marzo</b> Primer encuentro	<b>Módulo bienvenida y presentación.</b>	Propuesta y metodología de trabajo. Presentación del equipo docente y los alumnos. Charla acerca de la importancia del estudio de la temática y de sus abordajes prácticos e interdisciplinarios.
<b>31 de marzo</b> Semanas 1 y 2	<b>Las nuevas modalidades delictivas del mundo globalizado (Módulo introductorio).</b>	La Sociedad de la información. La relación entre el Derecho y la tecnología. Política criminal. Políticas preventivas. Seguridad informática. Perfil criminológico del delincuente informático. Inmigrantes y nativos digitales. La supuesta neutralidad de la tecnología. El uso de las TIC`s. Las redes sociales: caja de resonancia. Las neurociencias: neuroinformática. Multitarea (multitasking). Delitos informáticos y pandemia. El hacker ético.

Fecha	Temario propuesto	Contenidos
<p><b>14 de abril</b> Semanas 3 y 4</p>	<p><b>Unidad 1: Conceptualización del cibercrimen.</b></p>	<p>Definiciones, aplicabilidad y clasificación de los Delitos informáticos. Sujetos en el Delito informático (Sujeto Activo y Pasivo). Bienes jurídicos protegidos. Interpretación en cuanto Objeto / medio. Cibercrimen o delitos informáticos. Otras denominaciones. Clasificación de los modos de ejecución de los ciberdelitos (visión fenomenológica de la ciberdelincuencia). Derecho aplicable al Derecho Informático. Criminalidad informática.</p>
<p><b>28 de abril</b> Semanas 5 y 6</p>	<p><b>Unidad 2: Derecho Penal y Derecho Informático.</b></p>	<p>¿Derecho Penal Informático? El derecho informático y la informática jurídica. Principio de legalidad vs. Principio de neutralidad tecnológica y principio de equivalencia funcional. La neutralidad en las redes.</p>
<p><b>5 de mayo</b> Semanas 7 y 8</p>	<p><b>Unidad 2: Derecho Penal y Derecho Informático (Continuación).</b></p>	<p>Las características particulares de los delitos informáticos frente a los principios e institutos generales del Derecho Penal. Los problemas de la autoría y la participación. La criminalidad organizada. Vulnerabilidad de las víctimas. Problemas de Persecución. Ámbito espacial y principios. La problemática territorial. Lugar del hecho real (LHR). Lugar del hecho virtual impropio (LHVI). Lugar del hecho virtual propio (LHVP). La reformulación de las garantías. Fuentes constitucionales y los dilemas del derecho.</p>
<p><b>19 de mayo</b> Semanas 9 y 10</p>	<p><b>Unidad 3: El contexto normativo internacional.</b></p>	<p>El Convenio de Budapest. Cooperación internacional. Jurisprudencia internacional. Tipos de clasificación de los Delitos informáticos internacional. Delitos Informáticos – Clasificación reconocida por las Naciones Unidas: Fraudes cometidos mediante manipulación de computadoras. Falsificaciones informáticas. Daños o modificaciones de programas o datos computarizados. Acceso no autorizado a servicios y sistemas informáticos. Delitos Informáticos – Clasificación complementaria: Delitos cometidos por medio de Internet.</p>

Fecha	Temario propuesto	Contenidos
<p><b>2 de junio</b> Semanas 11 y 12</p>	<p><b>Unidad 4: La legislación argentina en materia de cibercrimen.</b></p>	<p>Los Delitos informáticos en el Derecho Penal Argentino: en el Código Penal y en leyes complementarias. Anteproyectos de reforma integral. Formas de tipificación y técnica legislativa. Marco Legal. Ley 26.388. Estudios estadísticos sobre cibercrimen en Argentina. La regulación en el Título específico sobre “Delitos Informáticos” Anteproyecto de Código Penal de 2018-2019.</p>
<p><b>16 de junio</b> Semanas 13 y 14</p>	<p><b>Unidad 4: La legislación argentina en materia de cibercrimen (Cont.)</b></p>	<p>El Convenio sobre Ciberdelito del Consejo de Europa (Convenio de Budapest) y su aprobación por el Estado Argentino -ley 27411-. Reservas a la Ley 27.411 Convenio de Budapest. Incidencias a nivel local y reformas legales. Las definiciones del art. 77 del Código Penal.</p>
<p><b>30 de junio</b> Semanas 15 y 16</p>	<p><b>Unidad 5: Protección de datos personales y Propiedad intelectual.</b></p>	<p>Registros de obras, marcas, señales y diseños. Copyleft. Marcos legales de protección de la dignidad y los datos personales. Ley 11.723 Propiedad Intelectual. Ley 25.326 de protección de datos personales. Constitución Nacional. Código civil y comercial. Delitos contra la dignidad (honor, intimidad, privacidad, secreto, etc). Ley 14.214 Provincia de Bs As. Las implicancias de la modificación del Código Civil y Comercial en el Derecho Penal, el Derecho a la Dignidad. La imagen y la reputación. Perfiles. Usuarios. Mail. Redes sociales. El documento electrónico y las firmas electrónica y digital (Ley 25.506). Nuevas formas de reconocimientos: reconocimiento facial y biométrico. El uso de la IA en el tratamiento de los datos y la big data.</p>
<p><b>14 de julio</b> Semanas 17 y 18</p>	<p><b>Unidad 6: Hurto, fraude y daño informático:</b></p>	<p>Hurto. Daño. Phishing. Fraude informático. Estafas informáticas. Estafas telefónicas. Atentado por medios informáticos. Sabotaje informático. Secuestro extorsivo. Hacking. Piratería. Piratas informáticos. Acceso no autorizado. Malware, virus, gusanos, troyanos, hijackers, keyloggers, hoax, jokes, spyware, adware, phishing, zombies.</p>

Fecha	Temario propuesto	Contenidos
<p><b>11 de agosto</b> Semanas 19 y 20</p>	<p><b>Unidad 7: Delitos informáticos en el ámbito financiero y económico.</b></p>	<p>Criptomonedas y su uso en los delitos informáticos. Blockchain. Estafas electrónicas. Transferencias de fondos. Delitos informáticos en el ámbito financiero y económico. Cryptojacking. Análisis del ocultamiento de rastros en la ruta del dinero, utilizando las criptomonedas. Lavado de activos utilizando técnicas informáticas. Grandes fraudes. Ataques informáticos a gran escala. Responsabilidad penal de las personas jurídicas.</p>
<p><b>25 de agosto</b> Semanas 21 y 22</p>	<p><b>Unidad 8: Delitos contra la integridad sexual en el contexto informático:</b>  <b>Tenencia de pornografía infantil.</b></p>	<p>Tenencia de pornografía infantil, Convenio Europeo de protección de los NNA. Producción, ofrecimiento, distribución y tenencia de pornografía infantil. Modalidades relacionadas con la pornografía infantil. Recolección de la evidencia digital. Pericias. Directrices de Luxemburgo. La protección de los menores en la Sociedad de la Información.</p>
<p><b>8 de septiembre</b> Semanas 23 y 24</p>	<p><b>Unidad 8 (Continuación):</b> <b>Ciberacoso (Grooming)</b></p>	<p>Ciberacoso (<i>Grooming</i>). Análisis de la figura delictiva del art. 131 del Código Penal. Políticas preventivas.</p>
<p><b>22 de septiembre</b> Semanas 25 y 26</p>	<p><b>Unidad 8 (Continuación):</b> <b>Sexting, pornovenganza (Revenge-porn) y sextorsión. Otros abusos: Hostigamiento (Stalking) y Cyberbullying.</b></p>	<p>Sexting, pornovenganza (<i>Revenge-porn</i>) y sextorsión. Otros abusos: Hostigamiento (<i>Stalking</i>) y Cyberbullying. Políticas preventivas. Antecedentes. Convenciones internacionales. Ley 26.388. Ley 26.904. Reforma de la ley 27.436. Explotación Infantil. NMEC.</p>
<p><b>6 de octubre</b> Semanas 27 y 28</p>	<p><b>Unidad 9: Informática forense</b></p>	<p>Investigaciones en entornos digitales. Obtención, preservación y tratamiento de evidencia digital. Las particularidades en el "levantamiento de rastros" y en "la escena del crimen". Cuestiones procesales relacionadas con la evitación de nulidades: Levantamiento de rastros, evidencias y efectos.</p>
<p><b>20 de octubre</b> Semanas 29 y 30</p>	<p><b>Unidad 9: Informática forense (Cont.)</b></p>	<p>Cadena de custodia, protocolos de actuación. Sistema PURI. Protocolo Provincia de Buenos Aires. Protocolos. RES 234/16. Guía de obtención, preservación y tratamiento de evidencia digital. RES PGN 3743/15.</p>

Fecha	Temario propuesto	Contenidos
<b>10 de noviembre</b> Semanas 31 y 32	<b>Unidad 10: Análisis Forense Digital</b>	La prueba pericial, técnicas OSINT, demostraciones prácticas. Herramientas y software utilizado para realizar pericias informáticas. Técnicas correctas para la realización de pericias informáticas. Análisis Forense Digital.
<b>24 de noviembre</b> Semanas 33 y 34	<b>Unidad 10: Análisis Forense Digital (Cont.)</b>	La prueba pericial en el proceso penal de la provincia de Buenos Aires. Pericias Informáticas. Uso de técnicas OSINT para investigaciones digitales penales. Demostración práctica de herramientas forenses. Alternativas Open Code de herramientas para realizar pericias y análisis. Casos prácticos: Uso del Sistema de Investigación MAN/u en casos de Grooming. Causa investigada "Casi Ángeles s/ Abuso de menores". Evidencia digital. Seguridad informática. Dirección IP. Identificación por radiofrecuencia.
<b>1 de diciembre</b> Semanas 35 y 36	<b>Unidad 11: La internet oculta</b> <b>Unidad 12: Inteligencia Artificial</b>	La internet oculta: Clearnet, Deep web, Dark web y Darknet y su posible uso en delitos informáticos. Dep Weeb y Dark Weeb en el entorno de los Delitos informáticos. Espionaje. Terrorismo. Narcotráfico. Tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, etc.  Inteligencia Artificial y el sistema jurídico. Internet de las cosas. La responsabilidad penal y la IA. Casos Prácticos. Reglamento del Parlamento Europeo y del Consejo de Normas Armonizadas en materia de inteligencia artificial.
<b>15 de diciembre</b> Semanas 37 y 38	<b>Cierre: evaluación final.</b>	Pautas del trabajo final para la acreditación del curso y debate de propuestas.

**Carga horaria total:** 60 horas *online* (encuentros sincrónicos) y 132 horas virtuales (asincrónicas a través del campus virtual) totalizando 192 horas reloj.

**Modalidad:** Virtual (sincrónica y asincrónica).

**Lugar:** Campus virtual UDE – FCH / Zoom / fchumanas@ude.edu.ar

**Email de contacto:** [ciberkrimencursos@gmail.com](mailto:ciberkrimencursos@gmail.com)