**PROGRAMA EXPERTO EN INFO FORENSE**

| U T | Eje Temático | Contenido |
| --- | --- | --- |
| 1 | Introducción a la problemática de la informática forense | El delito informático, su evolución en la última década, su proyección futura.  El surgimiento de la informática forense, su inserción social, judicial y tecnológica.  La acción de hacker’s y cracker’s.  El espionaje industrial y comercial, los activos informáticos y sus vulnerabilidades.  La labor conjunta legislativa, gerencial y tecnológica (Informática y Criminalística), para asegurar la privacidad como libertad individual y su preservación. |
| 2 | Informática aplicada | Medios de procesamiento, almacenamiento y distribución de información, centralizados, descentralizados, públicos y privados.  Características a preservar en los activos informáticos: integridad, disponibilidad, confidencialidad (privacidad), autenticidad, control de accesos (política del mínimo nivel y tiempo acotado) y confiabilidad (no repudio) de los datos.  La auditoría informática como medio para controlar la preservación de los activos informáticos |
| 3 | Ataques a los activos informáticos | El fraude informático, motivaciones delictivas, tipología, prevención y detección del fraude.  Virus, gusanos, hacker’s y cracker’s, consecuencias de su accionar sobre los activos informáticos.  Ataques pasivos a la confidencialidad de la información: intercepción, lectura del mensaje, análisis de tráfico.  Ataques activos a la información: Interrupción (disponibilidad), modificación (integridad), fabricación (integridad).  Criptoanálisis: Análisis de tráfico, detección de claves (de acceso y de cifrado) y textos cifrados.  Desencriptado de textos a partir de:   1. el algoritmo y el texto cifrado, 2. un texto en claro y 1. 3. un par cifrado plano y 1. 4. la clave privada y 1. 5. la clave privada y 2. o 3.   La ingeniería social (inversa) y las normas de seguridad. |

|  |  |  |
| --- | --- | --- |
| 4 | Seguridad Informática | Protagonistas: la gerencia, los propietarios/usuarios, los responsables informáticos, la administración de seguridad, los auditores informáticos.  Diseño, desarrollo e implementación de mecanismos de protección para los activos informáticos.  Concepto de propietario de la información, política de control de acceso y autenticación.  La auditoría informática, como medio de supervisión de la seguridad informática.  Protección ante riesgos de personal: errores, omisiones, hurto sabotaje, fraude.  Protección ante intrusos a través de los distintos medios de comunicación y transmisión de la información, disponibles.  Criptografía, diferentes técnicas de cifrado de la información *(DES, IDEA, RSA, PGP, Kerberos, SHA, SNMPv2, DSS)*  Implementación de mecanismos de autenticación y firma digital públicos y privados.  La interacción gerencial, informática y administrativa como política de protección de activos informáticos. |
| 5 | Principios de Derecho Informático | El sistema jurídico argentino, fuentes del derecho.  La Constitución Nacional, los Códigos de forma y de fondo.  Ramas del derecho, público y privado.  El derecho y las nuevas tecnologías.  Sistema judicial argentino, organización y competencias.  El sistema probatorio en uso, pertinencia de la prueba informático forense. |
| 6 | Legislación vigente y en estudio | Derecho de propiedad intelectual e industrial.  Derecho de autor, régimen legal argentino, convenios internacionales.  Protección del *software*, compilaciones y bases de datos, datos no originales, otras protecciones legales.  Registro de obras, formalidades, titularidad del *software* y de la información, trabajadores en relación de dependencia.  Patentes, derecho marcario.  Habeas data y protección de datos personales.  Delitos informáticos, estafa, hurto, espionaje, violación de secretos, acceso ilegítimo, falsedad informática, denegación de servicio, preconización de actividades terroristas, estupefacientes, pornografía infantil y otros delitos por Internet.  Regulaciones en Internet, casinos, comercio, martilleros, turismo, conflictos legales y de jurisdicción.  Ley de Firma digital, autoridades certificantes, almacenamiento y transmisión de la firma digital, validez del correo electrónico como medio de prueba |
| 7 | Criminalística y la prueba indiciaria | La criminalísta y sus disciplinas integradoras.  La prueba indiciaria como resultado evolutivo de las pruebas divina, personal, confesional y testimonial.  El delito informático como resultado de la explosión computacional de fines del siglo XX.  El concepto de prueba indiciaria aplicado a las huellas de los soportes digitales vigentes.  La aplicación de la metodología Criminalística a la prueba indiciaria informática. |
| 8 | La informática forense como prueba indiciaria | La escena del crimen, las evidencias, la cadena de pruebas.  Detección, revelado, protección y análisis de los indicios probatorios informáticos obtenidos en el lugar del hecho.  Detección de intrusos, ataques Mitnick, *exploits*, denegación de servicio, detección de reunión de información, el problema de las RPC (llamadas a procedimientos remotos), filtros de detección y protección (*TCP dump*, enmascaramiento), respuesta manual y automática a la intrusión.  Seguimiento y trazado de intrusos. Análisis y recuperación de archivos en distintos soportes. Herramientas de análisis informático forense (*the Coroner’s Toolkit, Task y Autopsy, Chrootkit*, Encase, Norton y otras) |
| 9 | Metodología de la Investigación Científica aplicada al Trabajo Final Integrador | El método científico - El estudio exploratorio - La selección de tema, hipótesis y variables - La planificación de la demostración lógica - El informe monográfico - La defensa oral |
| 10 | Práctica Pericial | Empleo de las herramientas informáticas en la investigacion informático forense. Planificiación, ejecución y defensa de un informe pericial modelo. |