CUATRO CLASES VIRTUALES

DELINCUENCIA INFORMÁTICA Y EVIDENCIA DIGITAL

6, 13, 19 y 26 DE OCTUBRE

Horario: 16 a 19 hs.

CURSO ABIERTO Y GRATUITO PARA TODO EL PERSONAL DEL PODER JUDICIAL DE SANTA CRUZ

DIRIGIDO ESPECIALMENTE AL FUERO PENAL

ACTIVIDAD CON PUNTAJE

Dentro de los términos del R.P.P. Art. 11° Inc. 2

ESCUELA DE CAPACITACIÓN Y PERFECCIONAMIENTO JUDICIAL

INSCRIPCIÓN HASTA EL 04/10/21 EN

bit.ly/inscripdelincuenciainformática

CONTENIDO DEL CURSO

Estructura: Dos módulos, uno de delincuencia informática y otro sobre informática forense y evidencia digital. Cada módulo requiere de 2 clases virtuales que se dan cada una dividida en dos bloques de 90 minutos.

MÓDULO 1: DELINCUENCIA INFORMÁTICA Y SU CONSIDERACIÓN JURÍDICA

DICTAN: MARCELO ALFREDO RIQUERT / CARLOS CHRISTIAN SUEIRO

Clase del 6 DE OCTUBRE MARCELO RIQUERT

1° bloque (16 a 17.30):

1. Derecho penal y nuevas tecnologías. Técnicas jurídicas de evitación de la impunidad: cooperación, asimilación, armonización y unificación. Antecedentes históricos de los delitos informáticos en general y de la ley 26.388 en particular. Convención de Budapest contra la Ciberdelincuencia. Protocolo Adicional al Convenio (Estrasburgo, 28/1/03): Penalización de Actos de Índole Racista y Xenófoba Cometidos por medio de Sistemas Informáticos.

2. Intimidad en la era de la extimidad. Bien jurídico: intimidad, privacidad y autodeterminación informativa. Panóptico tecnológico y los derechos humanos como criterios limitadores. Violencia institucional tecnológica: monitoreo electrónico del espacio privado; videovigilancia del espacio público. Agentes encubiertos. Violencia en el ámbito empresarial. Responsabilidad de los proveedores de servicios de Internet (ISP). Tipicidad, Big Data e Inteligencia Artificial. Robótica y atribución de resultados lesivos. ICC: dispositivos interfaz cerebro/computadoras no invasivos.

2° bloque (17.30 a 19):

3. Violencia de género en sus distintas variantes y redes sociales. Normativa nacional e internacional genérica y específica. Violencia contra niñas, niños y adolescentes. Normativa nacional e internacional. Violencia intrafamiliar. Hostigamiento, agresión o maltrato (Ciberbullying). Victimización infantil sexual online (VISO): explotación sexual comercial; solicitud sexual; exposición a contenido sexual. Tecnología y jóvenes autores.

4. El delito de ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil. Tenencia simple (cf. Ley 27436) y tenencia con fines de distribución. Problemas que advierte en el tipo penal del artículo 128 del Código Penal (supuestos de tenencias, bien jurídico protegido y pornografía virtual, otro tipo de representaciones en las que no se utiliza menores reales). Descripción de los verbos típicos. Nuestra legislación y las demandas de tipificación de la Convención de Budapest y del Protocolo facultativo de la Convención sobre los derechos del niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (ONU, 2000; Ley 25763/03).

5. Tipo penal de grooming. Elementos y posibles problemas de aplicación. La escala penal en comparación a otros delitos del mismo título dentro del Código Penal. Nuevas tipicidades: El delito de "revenge porn" (porno-venganza). Distintas variantes de acoso (ciberstalking): seguimiento y geolocalización, videovigilancia, hackeo y espionaje. Suplantación de Identidad en la red. Sexting y difusión de imágenes o grabaciones en la red inconsentidas.

Clase del 13 DE OCTUBRE CARLOS SUEIRO

1° bloque (16 a 17.30):

1. Violación de secretos y privacidad. El delito de acceso ilegítimo a la correspondencia electrónica. Acceso ilegítimo a sistemas y datos informáticos. Publicación indebida de comunicaciones electrónicas. Antecedentes legislativos. Tipos de acción en estos delitos. La utilización de los mails corporativos como prueba en el proceso penal, postura de los tribunales locales y el derecho comparado.

CONTENIDO DEL CURSO

2. El delito de Interrupción de comunicaciones. Regulación. Verbos Típicos. Modalidades. El delito de Destrucción de medios de prueba. Bien jurídico protegido. Regulación e importancia. Verbos típicos.
3. Daño Informático. Regulación en el derecho comparado y su inclusión al derecho argentino. El bien jurídico protegido. Las distintas modalidades para su comisión. Programas o virus maliciosos. El daño informático agravado: distintas circunstancias calificantes. ¿Qué es un ataque de denegación de servicios? Otros ataques informáticos. Hurto de datos: discusiones sobre su tipificación. Tenencia de herramientas de hackeo (Hacking tools).

2° bloque (17.30 a 19):
4. Fraude informático. Antecedentes. El nuevo texto legal. Modalidades de estafas informáticas. Alteración de registros informáticos. Uso no autorizado de tarjetas y claves falsas o sustraídas o de sus datos. Pharming, Phishing y robo de identidad. Estafas en mercados virtuales o con medios de pago virtuales. Evasión tributaria y previsional: afectación de bases de datos (art. 11, Ley 27430). Criptomonedas y lavado de activos de origen delictivo.

MÓDULO 2: INFORMÁTICA FORENSE Y EVIDENCIA DIGITAL
DICTAN: ANA H. DI IORIO / BRUNO CONSTANZO / SANTIAGO TRIGO / ROSALÍA GRILLO

Clase del 19 DE OCTUBRE
1° bloque (16 a 17.30) **- Ana Di Iorio Introducción a la Informática Forense y a la Evidencia Digital**
Ciberseguridad. Seguridad Informática. Seguridad de la Información.
Evidencia digital e informática forense. Clasificación. Tipos de Evidencia.
Principios Forenses. Protocolos y Guías de Actuación nacionales e internacionales.
Conceptos técnicos. Elementos que pueden investigarse en un sistema informático.
Roles del Informático Forense en el Proceso Penal. Proceso PURI.

2° bloque (17.30 a 19) **- Santiago Trigo Actuar Metodológico en la actuación Informático Forense**
Procedimientos de recolección, adquisición, preservación, análisis, presentación y validación de la evidencia digital.
Relevamiento. Identificación. Recolección de Evidencia digital.
Imágenes Forenses: Utilidad y Necesidad. Extracción, Análisis y Presentación de la evidencia. Análisis Forense de Datos (Investiga). Análisis Forense de Comunicaciones: Correo electrónico, Mensajería Instantánea y Redes Sociales.

Clase del 26 DE OCTUBRE
1° bloque (16 a 17.30) **- Bruno Constanzo Análisis Forense de Archivos y Contenido Multimedia**
Análisis forense de almacenamiento masivo. Búsqueda de elementos eliminados. Búsquedas simples y complejas de palabras clave.
Análisis Forense de Archivos Multimedia. Metadatos EXIF. DVR.
Triage en la escena del hecho y en el análisis.

2° bloque (17.30 a 19) **- Rosalía Grillo Análisis de Dispositivos Móviles**
Recolección, Cadena de Custodia, Extracción y Análisis de Dispositivos Móviles. UFED. UFED Reader. Pericia irreproducible. Pericia Informática e informe técnico. Objetivos de una pericia informática. Cuestionarios periciales.