



FRD.UTN

CIBERDELITOS

“El impacto en la educación y justicia, cómo prevenirlos y su tratamiento pericial”




DOCENTES:


Dr. Roberto Uzal
 Mg. Walter Fabián Agüero
 Dr. y Mg. candidata Viviana Petralcini
 Dr. Santiago Salomón Calderon
 Dr. Eduino Alessio
 Per. José Anello

DURACIÓN: 66 horas totales divididas en 15 horas asincrónicas y 51 horas sincrónicas con clases en vivo. Quedará distribuido en 17 encuentros de 3h los días viernes de 18 a 21h

OBJETIVOS:

El objetivo de la capacitación es dar a conocer las distintas modalidades del Ciberdelito y el impacto en la comunidad educativa, sociedad en general; y, principalmente en los auxiliares y miembros de la justicia. Se darán a conocer acciones de prevención y establecerá un protocolo a seguir en caso que el ciberdelito suceda (ámbito escolar y privado) y conservación de la prueba y su análisis como parte de un procedimiento pericial ante la justicia.

 /cursosutncampana

 www.frd.utn.edu.ar

 cursosadistancia@frd.utn.edu.ar

CIBERDELITOS

“El impacto en la educación y justicia, cómo prevenirlos y su tratamiento pericial”

DESTINATARIOS: Abogados, comunidad educativa (Docentes, directivos, padres, etc.), miembros y auxiliares de la justicia, miembros de las fuerzas de seguridad, alumnos de carreras de informática y público en general.

No es necesario tener conocimiento previos en computación o legal para cursar esta diplomatura.

Requisitos previos:

El único requisito para realizar este curso es contar con manejo básico de una computadora/Notebook, sistema operativo Windows o Linux, correo electrónico, navegación por internet.

CIBERDELITOS

“El impacto en la educación y justicia, cómo prevenirlos y su tratamiento pericial”

PROGRAMA

- INICIAL
- CAPITULO 1: Introducción al proceso judicial
- CAPITULO 2: Cibercrimen I
- Capítulo 3: Cibercrimen II
- CAPITULO 4: Cibercrimen III
- CAPITULO 5: Pericia Informático oficial
- CAPITULO 6: Evidencia Digital y perito de parte
Taller: Se realizará un taller en laboratorio y se proveerá del software para comprender los puntos mencionados



CERTIFICADO: Certificado de Asistencia.
Importante: Es requisito indispensable asistir a un mínimo de 80% de las clases.

**APTO CRÉDITO FISCAL PARA CAPACITACIÓN:
SOMOS UCAP**

POLÍTICAS DE CANCELACIÓN: La reserva de la vacante con el porcentaje asignado se reintegrará si el curso es suspendido. Si el curso confirma su apertura, antes de las 96 hs de la fecha estipulada de inicio, debe abonarse sin excepción el resto del valor del curso. Si esto no ocurre, se retendrá lo abonado previa notificación vía teléfono o, en su defecto, mail. Si el curso no se realizara, el inscripto podrá retirar el dinero en el período de hasta un mes de la fecha de cancelación del curso. Si participaste de nuestros cursos durante 2019, tenés un 15% (*) de descuento en nuestros cursos del ciclo 2020 **¡NO TE LO PIERDAS!** Solicitá información en Extensión Universitaria. (*) Aplicable únicamente para el pago completo.



PROGRAMA DETALLADO:

INICIAL

Presentación de la Diplomatura en Ciberdelitos y Peritaje Informático a cargo del Mg. Walter Agüero
Clase: Rastro y evidencia digital ciberseguridad y ciberdefensa
Clase magistral del Dr. Roberto Uzal, director de la Maestría en Ciberseguridad y Ciberdefensa de la Universidad de Buenos Aires

CAPITULO 1: Introducción al proceso judicial

Procedimiento legal. Partes del proceso judicial. Etapas e instancias procesales. Tipos de juzgados. Carátula de expediente. Nombre, funciones y roles de los involucrados en el proceso judicial. Peritos, su función. Características, deberes y derecho del perito. Perito de parte y oficial. Marco legal. Cuando se los convoca a los peritos y su incidencia en el juicio. Pilares de autenticidad de lo informado por el perito. Perito informático, su función. Prueba, adquisición física. Experiencia en algunos casos.
Cohorte a cargo del Dr. Eduardo Alessio

CAPITULO 2: Ciberdelito I

Ciberdelitos. Delitos informáticos en todas sus modalidades. Leyes nacionales y marco legal nacional. Grooming, Ciberacoso. Denuncias. Procedimiento que sigue a la denuncia. Evidencia digital, extracción física, lógica, duplicable, modificable, eliminable. Cadena de custodia. Experiencia en algunos casos.
Cohorte a cargo Dr. Santiago Salomón Calderón

Capítulo 3: Ciberdelitos II

Ciberespacio y características de los ciberdelitos. Introducción al marco legal, estructura de cada ley y lenguaje. Convenio de Cibercrimen de Budapest. Garantías penales y su importancia. Medidas procesales internacionales del Convenio de Ciberdelincuencia de Budapest.
Cohorte a cargo de la Dra. Viviana Estela Petracini Cerdeiro

CAPITULO 4: Ciberdelito III

Vocabulario y definiciones. Estado del arte de ciberdelitos cometidos en Argentina y el Mundo. Tipos de ciberdelitos. Estafas y ciberestafas. Robo en cuentas bancarias. Vulnerabilidades informáticas. Redes sociales. Phishing. Suplantación de identidad digital. Robo de cuentas de Facebook, Instagram y WhatsApp. Pornografía infantil Cooperación internacional. Violación de correspondencia electrónica. Pentesting, Ethical Hacking. Sexting. Extracción de Pruebas, su custodia.
Se realizará talleres prácticos en materia forense para la extracción de pruebas en peritajes forenses.
Cohorte a cargo: Mg. Walter Agüero

CAPITULO 5: Pericia Informático oficial

Perito informático: Designación en el cargo. Formas de notificación. Plazo para aceptar del cargo. Aceptando el cargo. Caso Práctico: Aceptando una Causa. Tipos de escritos judiciales. Solicitando en préstamo el expediente. Solicitando adelanto de gastos. Solicitando prórroga de plazos procesales. Fijando fechas de pericia. Fijando Fecha. Solicitando aclaraciones sobre puntos periciales. El informe pericial. Impugnaciones, Observaciones, Aclaraciones y Explicaciones Sentencia y notificación. Honorarios del perito. Experiencia en algunos casos.
Cohorte a cargo: Perito oficial José Anello

CAPITULO 6: Evidencia Digital y perito de parte

Evidencia digital: Ransomware y daño informático. Grooming, Cyberbullying y Bullying. Legislación y preservación de pruebas. Protocolo Cyberbullying. Ciberseguridad: Cómo implementarlas en cada uno de nuestros dispositivos. Virtual Private Network (VPN). Antivirus con Inteligencia Artificial. Firewall. Protección de la información. Criptografía simétrica y asimétrica. Firma Digital. Estenografía. Encriptación de nuestros datos. Blockchain y su arquitectura. Criptomonedas. Tipos de redes y su peligro de compartir o conectarse a una red WiFi ajena.
Cohorte a cargo: Mg. Walter Agüero

Taller: Se realizará un taller en laboratorio y se proveerá del software para comprender los puntos mencionados