

utdt.edu/ele

PRUEBAS INFORMÁTICAS

DIRECCIÓN ACADÉMICA: GUSTAVO PRESMAN Y DANIEL MONASTERSKY



**PROGRAMA
ABIERTO**

**DURACIÓN
5 ENCUENTROS**

**CURSADA
JUEVES 15, 22 Y 29
DE AGOSTO, Y 5 Y
12 DE SEPTIEMBRE**

DE 19 A 22H

La informática forense ayuda a abogados y jueces a identificar, preservar y analizar datos almacenados en medios magnéticos y transacciones electrónicas en un litigio judicial o extrajudicial. En el contexto actual, la mayoría de las comunicaciones y actividades comerciales involucran redes digitales, por lo que es indispensable tener un enfoque multidisciplinario que combine conocimientos informáticos con conocimientos legales. Esto es especialmente importante en una esfera en la que la prueba reviste vital importancia, sin que las normas procesales y de fondo hayan sido todavía adecuadamente actualizadas para contemplar desarrollos tecnológicos recientes de gran relevancia.

En este curso se examina el camino que se inicia con la recolección de evidencia digital, prosigue con su posterior análisis y concluye con la incorporación de dicha evidencia a los diversos procesos judiciales o con su uso interno en la empresa. También serán analizadas cuestiones transnacionales.

PLAN DE ESTUDIOS

MÓDULO 1 | LOS DELITOS INFORMÁTICOS I

- › Introducción a los delitos informáticos. Modificaciones al Código Penal mediante la Ley 26.388.
- › Ley de Grooming 26.904.
- › Antecedentes. Evolución legislativa.
- › Modalidades delictivas aún no contempladas.

MÓDULO 2 | INTRODUCCIÓN A LA EVIDENCIA DIGITAL

- › Informática forense y evidencia digital.
- › Distintos tipos de evidencia digital.
- › Evidencia en computadoras, en teléfonos celulares, en la nube y en Internet of Things (IoT).
- › Recolección y preservación: imágenes forenses.
- › Tratamiento de evidencia digital en el ámbito civil y penal.
- › Preconstitución de prueba informática.

MÓDULO 3 | LOS DELITOS INFORMÁTICOS II

- › Difusión de contenido íntimo sin consentimiento.
- › Calumnias e injurias a través de medios digitales.
- › Robo de identidad.
- › Desafíos actuales en materia de delitos informáticos.
- › Análisis de jurisprudencia.
- › Casos prácticos.

MÓDULO 4 | PRUEBA PERICIAL INFORMÁTICA

- › La pericia informática en el ámbito civil y penal.
- › ¿Qué cosas se pueden investigar en la evidencia digital?
- › Cómo pedir una pericia informática.
- › Medidas de prueba anticipada sobre evidencia digital.

MÓDULO 5 | ASPECTOS JURÍDICOS DE LA PRUEBA INFORMÁTICA

- › Prueba en el proceso penal.
- › La prueba en el proceso civil y comercial, y laboral.
- › Convenio de Cibercrimen de Budapest.
- › Diligencias preliminares. Medidas de prueba anticipada.

Se entregarán certificados de asistencia a quienes completen el 80% del programa.

La UTDT se reserva el derecho de modificar los módulos, sus contenidos y los profesores, garantizando la calidad de los mismos.

METODOLOGÍA

A través de la resolución de trabajos prácticos y la lectura de jurisprudencia, se pretende introducir a los asistentes en el tratamiento de la evidencia digital.

AUDIENCIA

El curso está dirigido a abogados, *compliance officers*, peritos judiciales, auditores, consultores en seguridad informática, y abogados internos de empresas y organismos de gobierno.

CUERPO DE PROFESORES

Gustavo Presman.

Master Executive en Tecnologías de la Información y las Comunicaciones, Programa GADEX. Ingeniero Electrónico, UBA. Especialista certificado internacionalmente en técnicas de Informática Forense. Profesor de Informática Forense en la Maestría en Seguridad Informática de la UBA. Perito judicial de parte y consultor técnico en la especialidad. Miembro del Consejo Profesional de Ingeniería Electrónica, Telecomunicaciones y Computación (jurisdicción nacional) y del Colegio de Ingenieros de la Provincia de Buenos Aires.

Daniel Monastersky.

Abogado, UMSA. Especialista en delitos informáticos, robo de identidad, reputación *online* y protección de datos personales. Director de la Diplomatura en Gestión y Estrategias en Ciberseguridad, UCEMA. Al frente de su estudio Identidad Robada, es desde 2016 uno de los nueve integrantes del Consejo Asesor del Foro Global de Especialistas en Ciberseguridad (impulsado por el gobierno de los Países Bajos y conformado por ONU, OEA y el