
INSTITUTO UNIVERSITARIO
DE SEGURIDAD
DE LA CIUDAD

Diplomatura en Investigación de Delitos Informáticos y Evidencia Digital

1. Identificación:

1.1. Denominación de la diplomatura: Investigación de Delitos Informáticos y Evidencia Digital

1.2. Título a otorgar: Diplomado en Investigación de Delitos Informáticos y Evidencia Digital

1.3. Carga horaria total: 90 horas

1.4. Ubicación de la estructura: Secretaria de Extensión, Transferencia e Investigación

1.5. Modalidad: Presencial

2. Características de la diplomatura

2.1. Titulación: Diplomado en Investigación de Delitos Informáticos y Evidencia Digital

2.3. Objetivos de la carrera:

Objetivos:

- Analizar la influencia de la informática y las telecomunicaciones en los principios generales del sistema penal, tanto en el derecho penal de fondo como en el proceso penal y en los sistemas de cooperación internacional en materia penal.
- Analizar las características típicas y los problemas jurídicos que presentan los delitos informáticos previstos en nuestra legislación y en el Derecho Comparado.
- Proveer a los participantes de los conocimientos tecnológicos básicos que resultan necesarios para la investigación de delitos en entornos digitales (conceptos básicos sobre informática, distintos soportes de almacenamiento de datos, estructura y funcionamiento de internet, telefonía móvil, herramientas de geo localización y otros dispositivos de tecno vigilancia).
- Proveer conocimientos básicos necesarios de informática forense.
- Utilización práctica de programa de informática forense.

2.4. Perfil del egresado

- Estudiar los mecanismos para obtener evidencia digital alojada en servidores ubicados en extraña jurisdicción, ya sea mediante la cooperación interprovincial, internacional o mediante requerimientos a las empresas del sector privado nacionales y extranjeras.
- Analizar las herramientas procesales necesarias para la obtención y posterior utilización válida en un proceso penal de la evidencia digital.

2.5. Requisitos de admisión: Jueces, Fiscales y Funcionarios de la justicia Nacional, Federal y Provincial. Policías y otras fuerzas de seguridad. Abogados penalistas y profesionales especialistas en Seguridad Informática y en criminalística. Peritos e investigadores de delitos o siniestros corporativos, empresariales y/o de compañías de seguros. Auditores o jefes de seguridad en entidades bancarias o financieras.

3. Organización de la diplomatura: se preveen clases teóricas y prácticas, con examen parcial y un examen final integrador.

3.1. Asignación Horaria:

COD.	ESPACIO CURRICULAR	CARGA HORARIA SERMANAL	CARGA HORARIA TOTAL	CANTIDAD DE CLASES
1	Aspectos básicos de informática.	3	9	3
2	Las conductas definidas como delitos informáticos en la legislación nacional y en el derecho comparado.	3	15	5
3	Proceso penal: aspectos teóricos y prácticos de la investigación en entornos digitales.	3	15	5
4	Herramientas tecnológicas para la investigación	3	15	5
5	Aspectos básicos de informática forense y evidencia digital	3	12	4
6	Principales problemas de cooperación internacional y su reflejo en el proceso penal.	3	6	2
7	Demostración de experiencias prácticas en investigación de casos reales.	3	12	3
8	Seminarios y conferencias especiales.	3	12	3
	TOTAL		**90**	**30**

3.1. Espacios Curriculares

- *Aspectos básicos de informática.*

Glosario de términos. Hardware y software. Datos de tráfico y datos de contenido. Tipos de soporte de almacenamiento de datos. Funcionamiento de internet. Asignación de dominios, direcciones IP, Correos electrónicos. Telefonía móvil.

- *Las conductas definidas como delitos informáticos en la legislación nacional y en el derecho comparado.*

Análisis de la Ley 26.388. La convención de Budapest. Acceso ilegítimo a sistemas informáticos. Daño informático (acciones de denegación de servicio). Fraude informático. Distribución de pornografía infantil. Grooming. Falsificación de documentos electrónicos. Suplantación de identidad. El denominado "phishing" y el pharming. Los delitos cometidos por medios informáticos. Especial referencia a las amenazas, hostigamientos, contenidos ilegales. El denominado ciber- terrorismo.

- *Proceso penal: aspectos teóricos y prácticos de la investigación en entornos digitales.*

Principios generales del proceso penal y estructura del proceso. Las distintas etapas del proceso penal. Los nuevos mecanismos de investigación tecnológicos y su relación con el derecho a la intimidad. Análisis de las garantías en el ámbito de investigaciones que involucran evidencia digital. Ley de protección de datos personales. Conceptos generales de evidencia. La prueba en el proceso penal. El principio de libertad probatoria y sus límites. La utilización analógica de las normas procesales que regulan los medios de prueba pensados para la evidencia física en la obtención de la evidencia digital. Problemas prácticos.

Necesidad de nuevos instrumentos procesales para la obtención de evidencia digital:

- Aseguramiento rápido de datos.
- Leyes de retención de datos de tráfico de comunicaciones.

- Registro y secuestro de datos informáticos.
- Intercepción de datos de tráfico y de datos de contenido.
- Remote forensic software: El secuestro de información digital sin necesidad de allanamiento a espacios físicos.

- *Aspectos básicos de informática forense y evidencia digital.*

Obtención de evidencia en diferentes entornos (qué se puede obtener y de qué manera). Herramientas informáticas para el aseguramiento y el análisis de evidencia contenida en soportes digitales (hardware y software). Estándares para la obtención de evidencia. Cadena de custodia en materia de evidencia digital. Aspectos prácticos. Programas informáticos especiales de investigación criminal e informática forense. Especial referencia al Encase. Análisis forense de teléfonos móviles. Investigación criminal en redes sociales. Técnicas de ingeniería social.

- *Principales problemas de cooperación internacional y su reflejo en el proceso penal.*

Problemas de jurisdicción y ley penal aplicable. Las dificultades de la cooperación internacional en delitos cometidos en el entorno digital. Especial referencia a la computación en las nubes (cloud computing) y su significación jurídica. La convención de Budapest y las recomendaciones de la OEA. La relación con autoridades extranjeras y distintas redes de cooperación internacional. Las redes 24/7. Interpol y las redes policiales de unidades especiales en delitos tecnológicos. El acceso transfronterizo de datos.

- *Demostración de experiencias prácticas en investigación de casos reales.*

Unidades especiales de la Policía Federal. Telemática de la Policía de la Ciudad. Fiscalía Especial de Delitos Informáticos de la CABA. Interpol. Fuerzas federales

- *Seminarios y conferencias especiales.*

Con el objetivo de cubrir las áreas funcionales y sectores dentro de la actividad profesional, se contempla asistencia a conferencias, seminarios, cursos y talleres de casos, aportando valor a las personas a través de acciones formativas de alto impacto y aplicación práctica.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S

Hoja Adicional de Firmas
Anexo

Número: IF-2019-07268025-GCABA-IUS

Buenos Aires, Viernes 1 de Marzo de 2019

Referencia: "Diplomatura en Investigación de Delitos Informáticos y Evidencia Digital"

El documento fue importado por el sistema GEDO con un total de 6 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.03.01 13:09:35 -03'00'

MARCELA DE LANGHE
Rector
INSTITUTO UNIVERSITARIO DE SEGURIDAD
MINISTERIO DE JUSTICIA Y SEGURIDAD

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.03.01 13:09:37 -03'00'