2023

# Diplomatura en Delitos Informáticos y Ciberseguridad

Derecho y Ciencias Políticas

UAI

Facultad de

DERECHO Y CIENCIAS POLÍTICAS

Universidad Abierta Interamericana (UAI)

Extensión Universitaria

INFORMES

De lunes a viernes de 9:00 a 18:00 Hs.

+54 9 11 2660 3030 // +54 9 11 5594 9903

## Duración:

**120 horas**.

## Días y horarios:

Del 15 de marzo al 22 de noviembre de 2023.
**Miércoles de 18:00 a 21:00 Hs.**

## Modalidad y localización:

**Virtual.**

## Aranceles:

**Externos:**
Matrícula: $ 4.000.-
Contado: $180.000.- o 9 cuotas de $20.000.-

**Comunidad UAI:**
Matrícula: $ 4.000.-
Contado: $126.000.- o 9 cuotas de $14.000.-

**Operadores de justicia, agentes de la administración pública:**
Matrícula: $ 4.000.-
Contado: $144.000.- o 9 cuotas de $16.000.-

**Extranjeros no residentes en Argentina*:**
Matrícula: USD 100.-
Contado: USD 3.200.- o 9 cuotas de USD 356.-

(*) Los aranceles de la actividad comprenden únicamente los conceptos de matrícula y cuota. Todo impuesto, tasa o contribución asociada a los pagos en dólares estadounidenses que pudiera ser aplicada por el país de origen, así como cualquier otra suma que se adicione en virtud de las tarifas vigentes en la entidad bancaria al momento de realizar la transacción, queda a exclusivo cargo del alumno.

## Dirigido a:

Estudiantes y profesionales del área de las ciencias sociales y jurídicas, sociología, abogacía, informática, ciencias de la comunicación social, criminología, criminalística; operadores de justicia, agentes de la administración pública, investigadores vinculados a la temática y al público en general.

## Objetivos:

Conocer los diferentes delitos informáticos y las dimensiones de la problemática de la ciberseguridad desde un enfoque criminológico y el abordaje de la seguridad informática, el Derecho, la protección de los datos personales y el peritaje informático forense, con el objetivo de brindar herramientas que permitan el diseño y ejecución de medidas de prevención y políticas para el sector, tanto a nivel público como privado.

## Impacto:

Al terminar el Diplomado los estudiantes tendrán la capacidad de:
a) Comprender el Marco Jurídico relacionado con Internet, así como los desafíos que representa su regulación.
b) Asesorar en la prevención de delitos contra la integridad de niños, niñas y adolescentes.
c) Elaborar diagnósticos en ciberseguridad, detección de vulnerabilidades, evaluación de ciberriesgos.
d) Diseñar planes de acción para intervenir y prevenir ataques cibernéticos en organizaciones públicas y privadas.
e) Asesorar en casos vinculados a delitos informáticos y el peritaje forense.
f) Comprender el funcionamiento del Blockchain y las criptomonedas y su relación con las actividades delictivas.
g) Realizar estudios científicos del fenómeno criminal en el ciberespacio.
h) Analizar junto a equipos multidisciplinarios los diferentes escenarios de la cibercriminalidad para orientar en la identificación de los autores.
i) Conocimiento de herramientas forenses y entrenamiento en prueba digital.

## Fundamentación:

El aumento del uso de las tecnologías en la última década ha generado un aumento exponencial en la innovación y en el desarrollo de los países. La red de información electrónica conectada constituye una parte importante de la vida cotidiana de muchas personas. Cada año se van sumando diferentes tipos de organizaciones como instituciones médicas, financieras y educativas utilizando la red para funcionar de forma eficaz. Esta red es utilizada en líneas generales para recopilar, procesar, almacenar y compartir grandes cantidades de información digital. A medida que se recopila y se comparte cada vez más información digital, su protección se vuelve imprescindible para la seguridad nacional y la estabilidad económica.

La Pandemia causada por el virus SARS-Cov-2 conocida por el acrónimo en inglés COVID-19 (coronavirus 2019) dejó en evidencia la vulnerabilidad de numerosas instituciones y organizaciones que no estaban preparadas para hacer una migración al teletrabajo, lo que significó el aumento de diferentes ataques por parte de la ciberdelincuencia.

La Organización de Estados Americanos (OEA) estima que las consecuencias económicas del ciberdelito ascienden a unos 90.000 millones de dólares, razón por la cual se invierte una importante

cantidad de recursos en la capacitación de operadores en los sistemas de justicia para perseguir las modalidades delictivas que se generan mediante el uso de la tecnología (OEA, 2009).

El Diplomado en Delitos Informáticos y Ciberseguridad de la Universidad Abierta Interamericana tiene como propósito promover la protección de los sistemas de red y todos los datos contra el uso no autorizado y los daños que estas acciones causan a nivel personal, corporativo y de estado.

## Diseño curricular:

**Módulo I: Marco Jurídico de Internet:** Introducción al marco legislativo existente sobre la regulación de internet, las leyes que rigen la materia en Argentina y su proceso de construcción, límites y desafíos en la era digital.

**Módulo II: Delitos Informáticos:** Delitos contra la integridad de niños, niñas y adolescentes: Principales instrumentos jurídicos en la materia, Pornografía infantil y Grooming, modalidades delictivas, prevención.

**Módulo III: Fundamentos de la seguridad informática:** Introducción y conceptos básicos de la seguridad informática, historia de la seguridad informática, principios y ciclos de la seguridad informática, ciclo de la seguridad informática, amenazas y sus tipos, vulnerabilidades, métodos y técnicas de intrusión.

**Módulo IV: Ciberseguridad en las organizaciones:** La infraestructura. Diseño de políticas y normativa, control de acceso, las copias de seguridad, protección antimalware, actualizaciones, seguridad de la red, la información de tránsito, gestión de soportes, registro de actividad, protocolos de actuación, equipamiento básico.

**Módulo V: Diseño y evaluación de planes de prevención en ciberseguridad:** Elaboración de diagnósticos en ciberseguridad, detección de vulnerabilidades, evaluación de ciberriesgos, elaboración de planes de acción, los recursos humanos y financieros, supervisión de los procesos, evaluación de los resultados.

**Módulo VI: Investigación Criminal y peritaje forense en delitos informáticos:** La evidencia digital, las pericias informáticas, la cadena de custodia de evidencias digitales, aspectos generales de la informática forense, etapas del peritaje, el laboratorio de informática forense.

**Módulo VII: Introducción sobre el Ethical Hacking:** Tipos de análisis de seguridad, reconocimiento pasivo, reconocimiento activo, tipos de ataques puro y consolidado, informe técnico.

**Módulo VIII: Blockchain y criptomonedas:** La metodología del cálculo de Blockchain, el Blockchain y la transformación digital, el minado de monedas, las criptomonedas limitaciones y potencialidades, billeteras digitales y transacciones de criptomonedas, la actividad delictiva y las criptomonedas.

**Módulo IX: Cibercriminología y Criminología Cyborg:** El estudio del fenómeno criminal en el ciberespacio. El impacto de la tecnología en el comportamiento humano, enfoque transdisciplinar en el estudio del ciberespacio, diferentes desviaciones relacionadas al ciberespacio (adicción, disfunciones cibersexuales, entre otras) teorías criminológicas en el estudio del ciberespacio. Investigaciones criminológicas en el ciberespacio.

**Módulo X: La Técnica de Perfilación Criminal Aplicada a Delincuentes Informáticos.** El ciberprofiling, la técnica del profiling criminal y su aplicación en la cibercriminalidad, enfoque inductivo y deductivo, la victimología, características de la escena del cibercrimen.

**Módulo XI: taller herramientas forenses:** Herramientas forenses utilizadas en la investigación de delitos informáticos y análisis de dispositivos.

**Módulo XII: La cooperación internacional, los daños informáticos y las fuentes abiertas:** Clases prácticas de investigación en redes abiertas: Grooming (vinculación con la pornografía infantil y el con el abuso sexual). Ciberbullying. Sexting. Revenge Porn. Sextorsion. El rol de Interpol en Investigaciones. Cooperación Internacional. Daño informático. Ransomware, DNS, Phishing. Análisis de casos. Análisis de la información de fuentes abiertas.  Análisis de WhatsApp y Telegram Análisis de Facebook y Twitter.

**Módulo XIII: Proyecto Final.** Presentación escrita de un trabajo individual de diez cuartillas en letra Times New Roman tamaño 12, con la aplicación de las Normas APA, donde se amplíe, analice, interrogue, o se debata alguna de las temáticas abordadas y que sea de especial interés para el estudiante.

## Metodología:

El presente diplomado está organizado en campos temáticos. Se dictarán clases virtuales y se complementarán con actividades prácticas en entornos web como Classroom. Al finalizar, se espera que entreguen un trabajo escrito donde profundicen un área específica, se responda una pregunta pertinente o se realice un análisis crítico sobre una de las temáticas abordadas.

## Evaluación Formativa:

La evaluación del Diplomado se realizará mediante la producción de un  trabajo  final individual. Se tratará de la realización de un análisis crítico, una discusión, o la respuesta a una pregunta clave de uno de los temas desarrollados en el curso. Los temas a desarrollar serán escogidos por los participantes previa consulta con el Director. En cada uno de los análisis los estudiantes deberán dialogar con los planteos realizados en clase. El trabajo final no podrá superar las diez páginas (A4, letra 12, Times New Roman, a espacio y medio).

## Recursos académicos:

**1- Clases virtuales:** Con la ayuda de plataformas como Google Meat, se realizarán encuentros virtuales equivalentes a clases presenciales con la participación del profesor, el director de la diplomatura y los estudiantes, donde tendrán la posibilidad de intervenir y realizar preguntas.

**2- Presentaciones:** Cada profesor diseñará una presentación para cada encuentro con la finalidad de facilitar datos o contenido relevante. Las presentaciones se diseñarán de acuerdo con el criterio de cada profesor en diferentes plataformas como PowerPoint, Prezi, Emaze, Slide Share, Knovio, entre otras.

**3- Videos tutoriales:** En este Diplomado se utilizarán como un recurso interactivo para reforzar la formación de conceptos, además de fortalecer la comprensión, asociación y consolidación de aprendizajes. De esta forma, los estudiantes estarán reforzando conceptos presentados en el curso de una forma más espontánea y con fundamento teórico aprobado por el docente. Algunos recursos que se utilizarán se encuentran en TED, Academic Earth, y Youtube.

**4- Foros de debate:** Con el apoyo de la plataforma Classroom se utilizará este recurso para dar dinamismo al espacio virtual. Esta herramienta de participación permitirá la interacción que genera un debate, consenso de ideas y construcción compartida de conocimiento, todo ello aporta un valor agregado al aprendizaje. El profesor estará presente en los foros, facilitando la construcción de conocimientos de forma autónoma y colaborativa.

## Calendario de encuentros:

**Módulo I:** Marco Jurídico de Internet.
**Fecha:** 15, 22, 29 y 05/04/2022 **Hora:** 18:00 a 21:00 Hs. (12hs).

**Módulo II:** Delitos contra la integridad de niños, niñas y adolescentes.
**Fecha:** 12, 19, 26, 03/05/2023 **Hora:** 18:00 a 21:00 Hs. (12hs).

**Módulo III:** Fundamentos de la seguridad informática.
**Fecha:** 10, 17, 24/05/2021 **Hora:** 18:00 a 21:00 Hs. (9hs).

**Módulo IV:** Ciberseguridad en las organizaciones: La infraestructura.
**Fecha:** 31/5 y 17/06/2023y 14/06. **Hora:** 18:00 a 21:00 Hs. (9hs).

**Módulo V:** Diseño y evaluación de planes de prevención en ciberseguridad.
**Fecha:** 28/6, 05/07/2023. **Hora:** 18:00 a 21:00 Hs. (6hs).

**Módulo VI:** Investigación criminal y peritaje forense en delitos informáticos.
**Fecha:** 12/07, 19/07, 26/07 y 2/08 **Hora:** 18:00 a 21:00 Hs. (12hs).

**Módulo VII:** Introducción sobre el Ethical Hacking.
**Fecha:** 09/08, 16/08 ,23/08/2021, 30/8/2021 (12hs) **Hora:** 18:00 a 21:00 Hs.

**Módulo VIII:** Blockchain y criptomonedas.
**Fecha:** 06/09, 13/09/23, 20/09/23 **Hora:** 18:00 a 21:00 Hs. (9hs).

**Módulo IX:** Cibercriminología y Criminología Cyborg: El estudio del fenómeno criminal en el ciberespacio.
**Fecha:** 27/09 y 04/10/2023 **Hora:** 18:00 a 21:00 Hs. (6hs).

**Módulo X:** La Técnica de Perfilación Criminal Aplicada a Delincuentes Informáticos.
**Fecha:** 11/10 y 18/10/2023. **Hora:** 18:00 a 21:00 Hs. (6hs).

**Módulo XI:** Taller de Herramientas Forenses.
**Fecha:** 25/10 y 01/11/2023. **Hora:** 18:00 a 21:00 Hs. (6hs).

**Módulo XII:** La cooperación internacional, los daños informáticos y las fuentes abiertas.
**Fechas:** 08/11, 15/11, 22/11.(12hs)

**Módulo XIII:** Proyecto Final.
**Fecha:** 29/11. **Hora:** 18:00 a 21:00 Hs. (3hs).

## Docentes participantes:

**Lic. Selene Vázquez.** Lic. Kinesiología y Fisioterapia. Ciencias de la Salud.

**Med-. Diego Mejía.** Médico. Ciencias de la Salud.

## Contacto:

uai.extension@uai.edu.ar

Envianos un mensaje en WhatsApp:

**Módulo VII:** Introducción sobre el Ethical Hacking.
**Fecha:** 09/08, 16/08 ,23/08/2021, 30/8/2021 (12hs) **Hora:** 18:00 a 21:00 Hs.

**Módulo VIII:** Blockchain y criptomonedas.
**Fecha:** 06/09, 13/09/23, 20/09/23 **Hora:** 18:00 a 21:00 Hs. (9hs).

**Módulo IX:** Cibercriminología y Criminología Cyborg: El estudio del fenómeno criminal en el ciberespacio.
**Fecha:** 27/09 y 04/10/2023 **Hora:** 18:00 a 21:00 Hs. (6hs).

**Módulo X:** La Técnica de Perfilación Criminal Aplicada a Delincuentes Informáticos.
**Fecha:** 11/10 y 18/10/2023. **Hora:** 18:00 a 21:00 Hs. (6hs).

**Módulo XI:** Taller de Herramientas Forenses.
**Fecha:** 25/10 y 01/11/2023. **Hora:** 18:00 a 21:00 Hs. (6hs).

**Módulo XII:** La cooperación internacional, los daños informáticos y las fuentes abiertas.
**Fechas:** 08/11, 15/11, 22/11.(12hs)

**Módulo XIII:** Proyecto Final.
**Fecha:** 29/11. **Hora:** 18:00 a 21:00 Hs. (3hs).

## Cuerpo Docente:

**Mg. Carlos Avendaño.** Docente UAI. Criminólogo. Magister y Doctorante en Ciencias Sociales UNGS-IDES. Políticas Criminal y Psicología del comportamiento delictivo.

**Abg. Hugo Daniel Sorbo.** Docente. Abogado. Especialista en Derecho Informático UBA. Derecho Informático e informática Forense.

**Tec. Marcelo Romero.** Docente. Técnico superior en Seguridad Pública. Especialista en Informática Forense. Especialista en Informática Forense.

## Contacto:

uai.extension@uai.edu.ar

E-MAIL

Envianos un mensaje en WhatsApp:

**+ 54 9 11 5594 9903**

**+ 54 9 11 2660 3030**