

# Delitos informáticos.

**Código: 216**

## **Descripción:**

El curso busca combinar el aporte teórico y discusión conceptual tras lo cual los participantes se concentrarán en la resolución de casos utilizando las herramientas adquiridas.

## **Destinatarios:**

Escalafón primario.

### **1. De los objetivos del curso:**

#### **A. Objetivo general:**

El curso pretende que al finalizar, los participantes sean capaces de resolver causas en que se juzgan delitos informáticos, delitos que se cometen por medios informáticos y puedan apreciar y ponderar la prueba informática, empleando los conocimientos técnicos y jurídicos, además de las destrezas adquiridas en el curso.

#### **B. Objetivos específicos:**

- Adquirir conocimientos para comprender los fundamentos y las bases del derecho de la informática y del derecho penal aplicables a la resolución de conflictos de relevancia jurídico penal en el área informática.
- Clasificación y utilización de destrezas que permitan analizar el fenómeno de la delincuencia informática y los distintos delitos configurados en el derecho nacional y comparado desde la óptica de los bienes jurídicos protegidos tradicionales y tecnológicos.
- Analizar y ponderar las pruebas de carácter informático.

### **2. Los contenidos del curso son:**

Unidades de aprendizaje	Contenido
<b>MÓDULO 1: Principios del derecho aplicables al derecho penal informático</b>	
<b>A. Análisis de la delincuencia informática</b>	<ul style="list-style-type: none"> <li>• La informática como medio comisivo y como objeto del delito.</li> <li>• Principales características de la delincuencia informática:               <ul style="list-style-type: none"> <li>○ Desde el punto de vista del autor.</li> <li>○ Desde la óptica tecnológica: breve análisis del funcionamiento y partes de un sistema de tratamiento de la información.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ Problemas ligados a la persecución de los delitos informáticos.</li> <li>● La víctima en los delitos informáticos.</li> <li>● Los problemas de persecución de los delitos informáticos.</li> <li>● Los tratados internacionales de colaboración en la persecución de delitos informáticos.</li> </ul>
<b>B. Principios de derecho informático y principios de derecho penal aplicables a la materia.</b>	<ul style="list-style-type: none"> <li>● Principios de derecho penal: <ul style="list-style-type: none"> <li>○ Legalidad y la tipificación de los delitos informáticos.</li> <li>○ Culpabilidad y el dolo en los delitos informáticos.</li> </ul> </li> <li>● Principios de derecho informático: <ul style="list-style-type: none"> <li>○ Neutralidad tecnológica.</li> <li>○ Equivalencia funcional.</li> <li>○ Equivalencia de soportes.</li> <li>○ Mínima afectación de las instituciones jurídicas tradicionales.</li> </ul> </li> </ul>
<b>MÓDULO 2: El bien jurídico protegido en los delitos informáticos. Derecho nacional y comparado</b>	
<b>A. El bien jurídico protegido en derecho comparado.</b>	<ul style="list-style-type: none"> <li>● Los delitos informáticos contra el patrimonio.</li> <li>● Las falsedades documentales y la fe pública.</li> <li>● La privacidad y las interceptaciones e interferencias de comunicaciones electrónicas</li> <li>● La propiedad intelectual y las copias ilegales de programas computacionales</li> </ul>
<b>B. El bien jurídico protegido en Chile.</b>	<ul style="list-style-type: none"> <li>● La pureza de la información contenida en sistemas de tratamiento de la información como nuevo bien jurídico protegido recogido en la ley N° 19.223.</li> <li>● Atentados contra la privacidad a través de las tecnologías de la información y las comunicaciones.</li> <li>● La propiedad intelectual frente a la informática.</li> <li>● La fe pública y las falsedades documentales.</li> <li>● Atentados contra la propiedad cometidos por medios informáticos.</li> </ul>
<b>MÓDULO 3: Figuras contenidas en la ley N° 19.223 sobre delitos informáticos y figuras relacionadas en el Código Penal.</b>	
<b>A. Sabotaje informático.</b>	<ul style="list-style-type: none"> <li>● Naturaleza y justificación en relación al bien jurídico protegido.</li> <li>● Elementos del tipo: <ul style="list-style-type: none"> <li>○ Modalidades de la conducta.</li> <li>○ Elementos subjetivos del tipo.</li> </ul> </li> <li>● Iter críminis.</li> <li>● Concursos y circunstancias modificatorias de responsabilidad.</li> <li>● Penalidad.</li> </ul>
<b>B. Delito de espionaje informático</b>	<ul style="list-style-type: none"> <li>● Naturaleza y justificación en relación al bien jurídico protegido.</li> <li>● Elementos del tipo: <ul style="list-style-type: none"> <li>○ Modalidades de la conducta.</li> <li>○ Elementos subjetivos del tipo.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Iter críminis.</li> <li>• Concursos y circunstancias modificatorias de responsabilidad.</li> <li>• Penalidad.</li> </ul>
<b>C. Análisis de las figuras de la ley N° 19.223 en concordancia con las figuras generales del Código Penal.</b>	<ul style="list-style-type: none"> <li>• Los delitos informáticos y la violación de correspondencia.</li> <li>• Delitos informáticos y falsificaciones documentales.</li> <li>• Delitos informáticos y estafas, fraudes y otros engaños.</li> </ul>
<b>MÓDULO 4: Tipos penales relativos a la informática contenidos en otros textos normativos</b>	
	<ul style="list-style-type: none"> <li>• Uso fraudulento de tarjetas de crédito o débito. Ley N° 20.009.</li> <li>• La piratería informática. Art. 80 de la ley N° 17.336 sobre protección de la propiedad intelectual.</li> <li>• Pornografía infantil realizada por medios informáticos. Art. 366 quinquies del Código Penal, introducido por ley N° 19.927.</li> <li>• Ilícitos contenidos en la legislación de telecomunicaciones.</li> <li>• Ley N° 20.601 que agrega el artículo 443 bis al Código Penal que aumenta las penas del delito de robo de cajeros automáticos.</li> </ul>
<b>MÓDULO 5: La persecución penal del delito informático.</b>	
<b>A. Problemas probatorios asociados a los delitos informáticos</b>	<ul style="list-style-type: none"> <li>• Cifra negra y delincuencia tecnológica.</li> <li>• Los medios de prueba aplicados a la acreditación de los hechos constitutivos de delito informático: especialidades de los medios de prueba tradicionales y nuevos medios de prueba, especiales referencias a la presentación de documentos electrónicos como medios de prueba en juicio penal.</li> </ul>
<b>B. Particularidades de los medios de prueba tecnológicos en la prueba de los delitos informáticos</b>	<ul style="list-style-type: none"> <li>• Lenguaje técnico informático en apoyo al análisis de los medios probatorios en los delitos informáticos.</li> <li>• Principios de seguridad informática aplicables a la producción y conservación de pruebas en los delitos informáticos.</li> <li>• Reglas básicas y método de informática forense y su aplicación en el proceso penal.</li> </ul>
<b>C. Procedimientos especiales de información asociados a la pesquisa y prueba de los delitos informáticos</b>	<ul style="list-style-type: none"> <li>• La responsabilidad de los proveedores de servicios de Internet frente a los delitos contra la propiedad intelectual.</li> <li>• Procedimientos de interceptación de comunicaciones electrónicas previstos en leyes especiales.</li> </ul>
<b>D. Problemas asociados a la</b>	<ul style="list-style-type: none"> <li>• El Tratado de Budapest sobre ciberdelincuencia.</li> <li>• Los delitos informáticos en el Derecho Europeo.</li> </ul>

**transnacionalidad de los delitos informáticos.**

- Los delitos informáticos en otros países de Latinoamérica.
- Los delitos informáticos en la órbita de las Naciones Unidas.

**MÓDULO 6: Taller de resolución de casos (método taller, destinado a la etapa presencial)**

- El taller, de 14 horas de duración distribuidos en dos jornadas de trabajo, debe contemplar la resolución, en grupos de no más de 6 ni menos de 3 participantes, de casos complejos que involucren la aplicación de textos positivos, doctrina y jurisprudencia. Los resultados del trabajo en grupo serán llevados a plenario. El mínimo de casos a resolver por cada grupo será de seis. Podrá usarse un mismo caso para varios grupos si trabajan simultáneamente y comparten su discusión en sesión plenaria. La resolución del caso deberá proponerse como parte resolutoria de un fallo, y deberán aportarse los principales fundamentos de la decisión adoptada por cada grupo, en su caso, con sus votos disidentes.

### 3. Metodología:

Curso presencial, para grupos de hasta 30 alumnos, que combinan en su metodología lecciones expositivas, con la interacción entre docentes y alumnos y la ejercitación de conocimientos relevantes.

### 4. Evaluación:

De acuerdo a lo señalado en el artículo 68 del Reglamento General de la Academia Judicial, "Los cursos del programa de perfeccionamiento serán objeto de evaluación de reacción y de aprendizaje".

Las evaluaciones de aprendizaje tendrán por finalidad únicamente retroalimentar al alumno, a los docentes y a la propia Academia respecto del proceso de aprendizaje."

Asimismo, sobre aprobación de los cursos, el artículo 67 del citado Reglamento señala que "Para aprobar un curso del programa de perfeccionamiento, se requiere acreditar la participación efectiva en todas las actividades presenciales que éste contemple o haber completado todas las que integran uno virtual."

### 5. Duración y distribución horaria del curso:

La duración del curso será de 24 horas. El curso deberá desarrollarse en 3 días.

### 6. Del cupo:

El número de alumnos no será superior a **30** ni inferior a **15**.