

DELITOS INFORMÁTICOS (CIBERCRIMEN)

CÓDIGO CURSO: 216

OBJETIVO GENERAL

Al finalizar el curso, el alumno deberá ser capaz de conocer, comprender y analizar las fuentes de las normas sobre delincuencia informática, en el marco del Derecho sustantivo, especialmente la Ley N° 19.223 y Ley N° 20.009, como de los principios aplicables a la disciplina.

Asimismo, el alumno estará en condiciones de aplicar a la resolución de un asunto concreto dichas normas y principios.

OBJETIVOS ESPECÍFICOS

- Que los participantes adquieran conocimientos para comprender los fundamentos y bases del derecho de la informática y del derecho penal aplicables a la resolución de conflictos de relevancia jurídico penal en el área informática.
- Que los participantes adquieran las destrezas que les permitan analizar el fenómeno de la delincuencia informática y los distintos delitos configurados en derecho nacional y comparado desde la óptica de los bienes jurídicos protegidos tradicionales y tecnológicos.
- Desarrollar en los participantes los conocimientos para comprender y aplicar los delitos de espionaje y sabotaje informático regulados en la Ley N° 19.223.
- Desarrollar en los participantes los conocimientos para comprender y aplicar en situaciones concretas cada uno de los tipos penales contemplados en la Ley N° 20.009.

- Que los participantes adquieran conocimientos y destrezas para solicitar y analizar las pruebas presentadas en la investigación de un delito informático, ponderarlas y apreciarlas en pos de lograr un grado de convicción al respecto.

CONTENIDOS

Análisis de los principios de derecho penal y derecho de la informática aplicables a la comprensión de la delincuencia informática, análisis de las figuras delictivas relativas a la informática vigentes en derecho nacional y de los principales medios probatorios aptos para su acreditación.

MÓDULO I: Principios del Derecho aplicables al Derecho Informático.

Objetivo específico: Al finalizar el módulo el alumno estará en condiciones de comprender los fundamentos y bases del derecho de la informática y del derecho penal aplicables a la resolución de conflictos de relevancia jurídico penal en el área informática.

Contenidos:

Unidad 1: Análisis Criminológico del la Delincuencia Informática.

1. La informática como medio comisivo y como objeto del delito.
2. Principales características de la delincuencia informática:
 - a. Desde el punto de vista del autor.
 - b. Desde la óptica tecnológica: breve análisis del funcionamiento y partes de un sistema de tratamiento de la información.
 - c. Problemas ligados a la persecución de los delitos informáticos.

3. La víctima en los delitos informáticos.
4. los problemas de persecución de los delitos informáticos.
5. Los tratados internacionales de colaboración en la persecución de delitos informáticos.

Unidad 2: Principios de Derecho Informático y principios de Derecho Penal aplicables a la Materia.

1. Principios de Derecho Penal:
 - a. Legalidad y la tipificación de los delitos informáticos.
 - b. Culpabilidad y el dolo en los delitos informáticos.
2. Principios de Derecho Informático:
 - a. Neutralidad tecnológica.
 - b. Equivalencia Funcional.

MÓDULO II: El Bien Jurídico protegido en los Delitos Informáticos, Situación Nacional y Derecho Comparado.

Objetivo específico: Al finalizar el módulo el alumno estará en condiciones de analizar el fenómeno de la delincuencia informática y los distintos delitos configurados en derecho nacional y comparado desde la óptica de los bienes jurídicos protegidos tradicionales y tecnológicos.

Contenidos:

Unidad 1: El Bien Jurídico Protegido en Derecho Comparado.

1. Los delitos informáticos contra el patrimonio.
2. Las falsedades documentales y la fe pública.
3. La privacidad y las interceptaciones e interferencias de comunicaciones electrónicas.

4. La propiedad intelectual y las copias ilegales de programas computacionales.

Unidad 2: El Bien Jurídico Protegido en Chile.

1. 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.
2. Atentados contra la privacidad a través de las tecnologías de la información y las comunicaciones.
3. La propiedad intelectual frente a la informática.
4. La fe pública y las falsedades documentales.
5. Atentados contra la propiedad cometidos por medios informáticos.

MÓDULO III: Figuras Contenidas en la Ley N° 19.223 sobre Delitos Informáticos.

Objetivo Específico: Al finalizar este módulo el alumno estará en condiciones de comprender y aplicar los delitos de espionaje y sabotaje informático regulados en la Ley N° 19.223.

Contenidos:

Unidad 1: Sabotaje Informático.

1. Naturaleza y Justificación en relación al bien jurídico protegido.
2. Elementos del tipo:
 - a. Modalidades de la conducta.
 - b. La pena.
 - c. Elementos subjetivos del tipo.
3. Iter críminis.
4. Concursos y circunstancias modificatorias de responsabilidad.

Unidad 2: Delito de Espionaje Informático.

1. Naturaleza y Justificación en relación al bien jurídico protegido.
2. Elementos del tipo:
 - a. Modalidades de la conducta.
 - b. La pena.
 - c. Elementos subjetivos del tipo.
3. Iter críminis.
4. Concursos y circunstancias modificatorias de responsabilidad.

MÓDULO IV: Tipos Penales relativos a la Informática contenidos en otros Cuerpos Normativos.

Objetivo específico: Al finalizar este módulo el alumno estará en condiciones de comprender y aplicar en situaciones concretas cada uno de los tipos penales contemplados en la Ley N° 20.009.

Contenidos:

Unidad 1: Uso Fraudulento de Tarjetas de Crédito o Débito. Ley N° 20.009.

1. Naturaleza y Justificación en relación al bien jurídico protegido.
2. Elementos del tipo:
 - a. Modalidades de la conducta.
 - b. La pena.
 - c. Elementos subjetivos del tipo.
3. Iter críminis.
4. Concursos y circunstancias modificatorias de responsabilidad.

Unidad 2: La Piratería Informática. Art. 80 Ley N° 19.733.

1. Naturaleza y Justificación en relación al bien jurídico protegido.
2. Elementos del tipo:
 - a. Modalidades de la conducta.
 - b. La pena.
 - c. Elementos subjetivos del tipo.
3. Iter críminis.
4. Concursos y circunstancias modificatorias de responsabilidad.

Unidad 3: Pornografía Infantil realizada por Medios Informáticos. Art. 366 quinquies Código Penal, introducido por Ley N° 19.927.

1. Naturaleza y Justificación en relación al bien jurídico protegido.
2. Elementos del tipo:
 - a. Modalidades de la conducta.
 - b. La pena.
 - c. Elementos subjetivos del tipo.
3. Iter críminis.
4. Concursos y circunstancias modificatorias de responsabilidad.

MÓDULO V: Problemas relacionados a la Prueba de los Delitos Informáticos.

Objetivo específico: Realizado este módulo el alumno podrá analizar las pruebas presentadas en la investigación de un delito informático, ponderarlas y apreciarlas en pos de lograr un grado de convicción al respecto.

Contenidos:

Unidad 1: Problemas relativos a la Conservación de Pruebas en los Delitos Informáticos.

1. La responsabilidad de los ISP en la conservación de pruebas.
2. La informática forense y la pesquisa de pruebas del delito informático:
 - a. Concepto de informática forense.
 - b. Importancia de la informática forense en la pesquisa de pruebas del delito informático.
 - c. La evidencia Digital: el grabado de información, la lectura y conservación de información, la recuperación de datos.

Unidad 2: El Peritaje Informático.

1. Concepto y oportunidad.
2. El sistema de tratamiento de la información como objeto de pericia.
3. El informe de perito informático, su estructura, interpretación y aplicación en la pesquisa de delitos informáticos.

METODOLOGÍA

El diseño metodológico del curso deberá integrar dos modalidades: **Curso y Taller.**

El curso (orientado a los conocimientos) se estructura sobre la base de una pedagogía participativa. Para ello, las clases presenciales se desarrollarán sobre la base de lecturas dirigidas, discusiones informadas y planteamiento de problemas relevantes en cada una de las materias que se aborde. En este contexto se estimulará el análisis práctico de los temas fundamentales de la disciplina, a través del análisis crítico y reflexivo de los textos leídos, análisis de casos teóricos y prácticos y, muy especialmente, estudio de la jurisprudencia nacional.

El equipo docente deberá entregar, con anterioridad, material escrito de modo que las sesiones se centren en la reflexión, intercambio entre docentes y participantes, análisis y exposición de casos prácticos.

El taller (orientado al desarrollo de habilidades y aptitudes) supone la utilización de técnicas como observación participante, participación en procesos simulados, discusiones en grupo y otros que puedan resultar conducentes a los objetivos buscados.

DESTINATARIOS

Jueces de Garantía, Jueces de Tribunal de Juicio Oral en lo Penal, Jueces de Juzgados de Letras y Garantía, Secretarios de Juzgados de Letras y Garantía, Ministros, Secretarios y Fiscales Judiciales de Cortes de Apelaciones.

DURACIÓN

24 horas.

CUPOS

Mínimo 15 y máximo 25 participantes.

NÚMERO DE CURSOS

1 curso.

LUGARES Y FECHAS

El curso durará 3 días.

Cód. Ciudad 1 Santiago 07 - 09 septiembre