**Delitos Informáticos**

**Concepto**

Los delitos informáticos, también conocidos como ciberdelitos, son aquellas actividades ilegales realizadas mediante el uso de tecnologías de la información y la comunicación (TIC). Estos delitos pueden implicar el acceso no autorizado a sistemas informáticos, la modificación de datos, el robo de información, el fraude en línea, entre otros.

**Clases**

Los delitos informáticos se pueden clasificar en varias categorías, entre ellas:

1. **Acceso no autorizado:** Ingreso a sistemas informáticos sin permiso.

2. **Intercepción de datos:** Captura de datos en tránsito sin autorización.

3. **Daño o alteración de datos:** Modificación, borrado o deterioro de datos sin autorización.

4**. Fraude informático:** Uso de computadoras para cometer fraudes financieros.

5. **Delitos contra la privacidad:** Robo de información personal y violación de la privacidad.

6. **Piratería de software:** Copia, distribución y uso no autorizado de software protegido por derechos de autor.

7. **Phishing:** Suplantación de identidad para obtener información sensible.

8. **Distribución de malware:** Creación y propagación de virus, troyanos y otros tipos de software malicioso.

**Figuras y Modalidades**

Las figuras delictivas y modalidades en delitos informáticos incluyen:

**- Hackeo (hacking):** Acceso no autorizado a sistemas informáticos con el fin de robar, modificar o destruir datos.

**- Cracking:** Similar al hacking, pero con la intención de causar daño o realizar actividades ilegales.

**- Phishing:** Engaños a través de correos electrónicos o sitios web falsos para obtener información confidencial.

**- Spyware:** Software que recoge información sobre una persona u organización sin su conocimiento.

**-** **Ransomware:** Software que bloquea el acceso a los datos de una víctima y exige un rescate para desbloquearlos.

**Marco Legal**

En Argentina, la legislación sobre delitos informáticos incluye varias leyes y artículos del Código Penal que abordan específicamente este tipo de delitos.

1. **Ley 26.388 (Delitos Informáticos):** Esta ley modifica el Código Penal para incluir delitos específicos relacionados con la informática, tales como el acceso indebido a sistemas y la interceptación de comunicaciones.

2. **Ley 11.723 (Ley de Propiedad Intelectual):** Protege los derechos de autor, incluidos los derechos sobre software.

**Protección Legal del Software (Ley 25.036)**

La **Ley 25.036** de Argentina, sancionada en 1999, modifica la Ley de Propiedad Intelectual (Ley 11.723) para extender la protección del derecho de autor a los programas de computación. Esta ley establece que los programas de software están protegidos como obras literarias, otorgando derechos exclusivos a los autores para reproducir, distribuir, y modificar el software.

**Piratería del Software**

La piratería de software es la copia, distribución y uso no autorizado de software protegido por derechos de autor. Las formas comunes de piratería incluyen:

- **Copia ilegal:** Reproducción de software sin autorización.

- **Distribución a través de internet:** Compartir software ilegalmente a través de redes de intercambio de archivos o sitios web.

- **Uso sin licencia:** Instalación y uso de software sin adquirir una licencia legítima.

La lucha contra la piratería del software incluye medidas legales, como la aplicación de leyes de propiedad intelectual, y medidas tecnológicas, como el uso de mecanismos de protección y licenciamiento.

**Protección y Regulación**

Además de las leyes nacionales, existen regulaciones internacionales que combaten los delitos informáticos y protegen el software:

1. **Convenio de Budapest sobre Ciberdelincuencia:** Un tratado internacional que busca armonizar las leyes nacionales sobre delitos informáticos y fomentar la cooperación internacional en la lucha contra el cibercrimen.

2. **Acuerdos de la OMPI (Organización Mundial de la Propiedad Intelectual):** Proveen un marco para la protección de los derechos de autor a nivel internacional, incluyendo el software.

Estos marcos legales y normativos buscan asegurar que los delitos informáticos sean prevenidos, detectados y sancionados adecuadamente, protegiendo así a los individuos y a las organizaciones de las amenazas cibernéticas