LOS DELITOS INFORMATICOS

INTRODUCCION.

I. LEY 19.233 QUE TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA O "LEY DE DELITOS INFORMÁTICOS".

1. ¿Qué es lo que se protege en la Ley de Delitos Informáticos?
2. ¿Qué es un Delito Informático?
3. ¿Cuáles son las conductas sancionadas en la Ley?
4. ¿En qué consiste el Sabotaje Informático?
5. ¿En qué consiste el Espionaje Informático?
6. ¿Cuáles son las penas de estos delitos?
7. ¿Quiénes pueden querellarse contra estas conductas?

II. NORMATIVA UNIVERSITARIA SOBRE EL USO DE CUENTAS ASIGNADAS POR LA DTI.

1. ¿Dónde se encuentran las normas que regulan el uso de cuentas proporcionadas por la DTI?
2. ¿Cuáles son los beneficios de la cuenta a los que tiene derecho un estudiante?
3. ¿Cuáles son los deberes y conductas prohibidas en el uso de cuentas?

3.1 Deberes de los estudiantes

3.2 Faltas a la Normativa de uso de cuentas.

INTRODUCCION.

Con ocasión de conductas que, en general, muestran estudiantes de los distintos niveles educacionales, incluidos los de Educación Superior, esta Unidad de Control ha estimado conveniente referirse a los riesgos a que se pueden exponer quienes incurren en la comisión de conductas denominadas "hacking" y otras, y que tienden a ser percibidas socialmente como inofensivas, pero que pueden encontrarse tipificadas como delito.

En efecto, muchas de estas conductas y otras similares y relacionadas, constituyen actualmente delitos a la luz de lo señalado en la Ley N° 19.223, publicada en el Diario Oficial el 7 de junio de 1993, que tipifica y sanciona los denominados Delitos Informáticos.

En este sentido, se debe recordar que en Chile, en virtud de lo establecido en el artículo 7 del Código Civil, por regla general, toda ley se entenderá conocida y se hace obligatoria desde su publicación en el Diario Oficial, agregando la disposición octava del mismo cuerpo normativo, que la ley se presume conocida por todos, y consiguientemente, el argumento de desconocer el texto legal, no es razón para evitar

los efectos de eventuales querellas y ser sujeto de persecución penal, si en los hechos se ejecuta alguna acción que revista los caracteres tipificados en dicha ley.

Asimismo, la propia normativa universitaria contempla normas obligatorias que establecen los derechos y deberes de los estudiantes respecto del uso de las cuentas proporcionadas por la Dirección de Tecnologías de la Información (DTI).

En este sentido, al asignárseles cuentas a los alumnos regulares de la Universidad de Concepción, la DTI exige que se haya leído, comprendido y aceptado la reglamentación vigente, con el objeto que los estudiantes se familiaricen con los beneficios que la cuenta implica y con los límites a que están sujetos en su uso y goce. La falta de observancia de dichas normas puede acarrear la responsabilidad disciplinaria del estudiante, con la consiguiente aplicación de sanciones y, eventualmente, las responsabilidades penales que se deriven de la infracción.

El presente artículo intentará presentar de la forma más simple y completa posible, las conductas que la ley sanciona como delitos y las normas internas que regulan el uso de los beneficios informáticos que proporciona la Universidad, con el objeto que los estudiantes tomen conocimiento del contenido de la ley y reglamentos y se prevengan y abstengan de incurrir en dichas acciones.

I. Ley 19.233 "LEY DE DELITOS INFORMATICOS". TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA.

1. ¿Qué es lo que se protege en la Ley de Delitos Informáticos?

Toda tipificación de delitos pretende, en último término, proteger bienes jurídicos. Los bienes jurídicos son intereses relevantes de las personas en tanto sujetos sociales, considerados especialmente valiosos y consecuentemente, dignos de protección penal frente a conductas que los dañan o ponen en peligro.

Así, respecto del delito de hurto, por ejemplo, el bien jurídico protegido es la propiedad. En el caso del homicidio, el bien jurídico protegido es la vida.

En el caso de los delitos tipificados en la Ley 19.233, es "un nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales**: la calidad, la pureza e idoneidad de la información en cuanto tal**, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan**"**.

Sin embargo, no sólo se protege ese bien sino que además, concurren otros, tales como**: el patrimonio**, en el caso de los fraudes informáticos**; la privacidad, intimidad y confidencialidad de los datos** como es el caso del espionaje informático**; la seguridad y fiabilidad del tráfico jurídico y probatorio** en el caso de las falsificaciones de datos probatorios vía medios informáticos**;** el **derecho de propiedad sobre la información y sobre los elementos físicos**, materiales de un sistema informático, en el caso de los delitos de daños.

2. ¿Qué es un Delito Informático?

Se ha conceptualizado el delito informático de distinta manera, entre las cuales podemos señalar:

a.- "Aquellos delitos perpetrados por medio del uso de computadores y todos los delitos en que se dañe a los computadores o a sus componentes";

b.- "Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actué con o sin ánimo de lucro" (Marcel Huerta y Claudio Líbano).

Lo esencial radica en que, tanto los medios de comisión como el objeto del delito, dicen relación con dispositivos habitualmente utilizados en actividades informáticas.

3. ¿Cuáles son las conductas sancionadas en la Ley?

La Ley Nº 19.223 contempla cuatro artículos, que si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en dos grandes figuras delictivas:

I) Sabotaje Informático;
II) Espionaje Informático.

Estas dos figuras se subdividen en categorías distintas, atendiendo al objeto contra el cual se atenta y/o al modus operandi.

A continuación se transcriben las disposiciones de la citada ley que tipifican los delitos informáticos:

Artículo 1°. ***"El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.***

Si como consecuencia de estas conductas, se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Artículo 2°. ***"El que con ánimo de apoderarse, usar, o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo***

intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Artículo 3°. ***"El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, será castigado con presidio menor en su grado medio".***

Artículo 4°. ***"El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio.***

Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

4. ¿En que consiste el Sabotaje Informático?

El Sabotaje Informático (artículos 1 y 3 de la Ley Nº 19.223) comprende aquellas conductas tipificadas atendiendo al *objeto que se afecta o atenta* con la acción delictual, y que puede ser un *sistema de tratamiento* de la información o de sus partes componentes, el *funcionamiento* de un sistema de tratamiento de la información, y/o los *datos* contenidos en un sistema automatizado de tratamiento de la información. El atentado a estos objetos puede ser a través de su destrucción, inutilización, obstaculización o modificación.

5. ¿En que consiste el Espionaje Informático?

El Espionaje Informático (artículo 2 y 4 de la Ley Nº 19.223) comprende aquellas figuras delictivas que atienden al *modo operativo que se ejecuta* y que pueden ser, en primer lugar, delitos de **apoderamiento indebido** (apropiarse de la información), **uso indebido** (usar la información para cualquier fin) o **conocimiento indebido** de la información, **cometidos interfiriendo, interceptando** o meramente **accediendo** al sistema de tratamiento de datos. Estas figuras se encuentran descritas en el artículo 2º de la Ley, y comprende lo comúnmente conocido como "hacking".

En segundo lugar, comprende también los **delitos de revelación indebida y difusión de datos contenidos** en un sistema de tratamiento de la información (artículo 4º de la ley).

6. ¿Cuáles son las penas de estos delitos?

Las penas asignadas a los delitos son bastantes altas.

a) **Para el caso de Figuras de Sabotaje Informático:**
   En el caso de las figuras del Artículo 1º, a las conductas de destrucción e inutilización de un sistema de tratamiento de información o de sus partes o

componentes, y a las conductas de impedimento, obstaculización o modificación de su funcionamiento, las penas asignadas van desde **541 días a 5 años**. Para el caso que dichas conductas traigan como consecuencia la destrucción de los datos, la pena asignada va de **3 años y un día a 5 años**.

En el caso del Artículo 3º, las conductas de destrucción, daño o alteración maliciosa de los datos, tienen asignadas penas que van desde los **541 días a los 3 años.**

b) **Para el caso de Figuras de Espionaje Informático:**
En el caso del Artículo 2º, esto es, las conductas de apoderamiento, uso y conocimiento indebido mediante la interceptación, interferencia y acceso al sistema, las penas van desde **61 días a 3 años**.
Finalmente, en lo que respecta al Artículo 4º, las conductas de revelación o difusión maliciosa de los datos, tienen penas que van desde los 541 días hasta 3 años. Si la persona que incurre en estas conductas es el encargado del sistema, la pena sube de **3 años y un día a 5 años.**

7. ¿Quiénes pueden querellarse contra estas conductas?

No hay limitaciones en este aspecto, y puede querellarse cualquier persona víctima de estas conductas. En este punto es importante destacar que los delitos informáticos son delitos de acción pública, lo que significa que no se requiere la existencia de un querellante para que se proceda a iniciar la respectiva investigación y posterior juicio, basta la denuncia y los fiscales están obligados a investigar y perseguir la responsabilidad penal.

II. NORMATIVA UNIVERSITARIA SOBRE EL USO DE CUENTAS ASIGNADAS POR LA DTI.

1. ¿Dónde se encuentran las normas que regulan el uso de cuentas proporcionadas por la DTI?

La normativa interna se encuentra en la página Web de la DTI: **www.udec.cl/dti**

En la columna izquierda, se puede observar el ítem: "Productos y servicios". Al pinchar, se despliega su directorio completo, donde se encuentra la opción "Servicios en línea". Al pinchar, se obtiene un segundo directorio, donde encontramos la opción "Creación de cuentas".

Para acceder al servicio "Creación de cuentas", se debe pinchar la dirección que ahí se proporciona: **www.udec.cl/scu**

En ella se anuncia que "A través de este sistema automático, los alumnos y funcionarios pueden obtener una cuenta electrónica para acceder a distintos servicios en red:

- Obtener una dirección de Correo Electrónico E-mail
- Construir y mantener su propia página Web (30 mb. de espacio en disco)
- Publicar avisos económicos en el sitio de la Universidad
- Accesar la Base de Datos Académica BDA (para funcionarios)
- Accesar a Servicios de información al trabajador
- Accesar al Infodocente
- Enviar Correo al Rector
- Contestar la encuesta docente (para alumnos)
- Accesar el sitio Infoalumno e Infodocente.
- Y muchos servicios más ...

Para crear su cuenta, presione el botón “Continuar"

Al presionar “Continuar”, se despliega la "Normativa de cuentas".

2. ¿Cuáles son los beneficios de la cuenta a los que tiene derecho un estudiante?

Permite disponer de un correo electrónico del tipo nombre@udec.cl para acceder a distintos servicios en línea de la Universidad, almacenar archivos y/o mantener una página Web personal en un espacio virtual de 30MB (art. 4º de la Normativa de cuentas).

3. ¿Cuáles son los deberes y conductas prohibidas en el uso de cuentas?

A continuación se presenta una versión resumida de los deberes y obligaciones a los que están sujetos los estudiantes en el uso de sus cuentas. Para una versión más completa, se recomienda revisar los links directamente.

3.1 Son Deberes de los estudiantes los siguientes:

1) Utilizar la cuenta para fines netamente académicos y/o universitarios, que no contravengan la ética y principios de nuestra casa de estudios ni tampoco la legislación vigente.

2) El titular de la cuenta es el único responsable de la misma y de los contenidos publicados o almacenados en ella.

3) El uso de la cuenta es personal. Por lo tanto, no se deben usar cuentas de terceros ni autorizar su uso por personas distintas al titular.

4) El envío y recepción de mensajes es de carácter privado, por lo tanto, en principio, ningún organismo o persona está facultado para accesar esa información. No obstante, la D.T.I. se reserva el derecho a revisar los materiales enviados, eliminar cualquier material a su entera discreción o revelar en cualquier momento y sin previo aviso cualquier información si lo cree necesario para cumplir con cualquier ley, reglamento, proceso legal o solicitud gubernamental aplicable.

3.2 Son Faltas a la Normativa de uso de cuentas las siguientes conductas, descritas en su Artículo 11:

1) La utilización del espacio otorgado en la cuenta a cada usuario para anunciar u ofrecer la compra o venta de cualquier bien o servicio para cualquier fin comercial, a menos que se haga con la expresa autorización de la D.T.I.

2) La publicación de información que vulnere la legislación nacional, esté reñida con la ética o que contravenga los principios universitarios, tales como imágenes pornográficas, información homofóbica, racista, clasista que pueda dañar la integridad o el honor de las personas, instituciones o creencias. Tampoco se pueden incluir en las páginas personales, hipervínculos hacia sitios con estas características.

3) El almacenamiento de música, software, películas, imágenes, código malicioso, claves de acceso o cualquier archivo cuyo contenido sea ajeno a los fines para los que se otorgó la cuenta.

4) La carga de archivos que contengan virus, "Troyanos", "gusanos", bombas de tiempo, archivos dañados o cualquier otro programa o software similar, el envío de mail masivos (spam), sistemas de cancelación de exposiciones (cancelbots) u otras acciones que puedan perjudicar el funcionamiento de los equipos de la Universidad o de propiedad de terceros.

5) Cualquier intento de apropiación de información de las bases de datos corporativas o de privados, el molestar a otros usuarios y la generación de sobrecarga, por ejemplo, a través de la creación de foros en las páginas personales, ya sea en equipos de la Universidad o de conexiones fuera de la ella.

Contraloría Universitaria
Universidad de Concepción
Julio 2007.