**Deontología Informática**

La deontología según el diccionario del a real academia de la lengua, es, un sentido más amplio, la ciencia o tratado de los deberes y normas morales. En un sentido más concreto, tiene que ver con el comportamiento moral o ético, es decir con los principios y normas morales que regulan las actividades humanas. La deontología informática, por extensión, trata, por tanto, de la moral o ética profesional en el manejo del activo más importante que tienen las empresas, un bien cada vez más apreciado, que es la información.

Históricamente, los profesionales de la informática, como grupo, no han sido involucrados en cuestiones de ética. A menudo, se ve, a las computadoras simplemente como maquinas y algoritmos y no se perciben las serias cuestiones de éticas inherentes a su utilización.

De cualquier modo, cuando se considera que esas maquinas influyen, directa e indirectamente, en la calidad de vida de millones de individuos se comprende que es un tema de gran importancia. Las computadoras se utilizan para diseñar, analizar, soportar y controlar las aplicaciones que protegen y guían las vidas de las personas. El uso de los sistemas informáticos puede tener efectos más allá de lo que alcanza la imaginación.

Esa actitud estará dirigida en el futuro hacia problemas de seguridad. En particular, se debe considerar, publicar ampliamente el código fuente de virus y otras amenazas para la seguridad.

Un tipo de conducta poco ética es la instrucción por medios informáticos, aunque de esta no resulte ningún daño obvio. La actividad por si misma es inmoral e incluso si el resultado es una mejora de seguridad, aunque existen multitud de posibles razones para justificarla.

**Seguridad Informática**

La seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños

incluyen el mal funcionamiento del *hardware*, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.

En un sistema de los denominados 'tolerante a fallos' dos o más ordenadores funcionan a la vez de manera redundante, por lo que si una parte del sistema falla el resto asume el control.

Los virus informáticos son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de 'inmunizar' o eliminar el virus del ordenador. Para evitar problemas en caso de apagón eléctrico existen las denominadas UPS (acrónimo de *Uninterrupted Power Supply*), baterías que permiten mantener el sistema informático en

funcionamiento, por lo menos el tiempo necesario para apagarlo sin pérdida de datos. Sin embargo, la única forma de garantizar la integridad física de los datos es mediante copias de seguridad.

El mayor problema que tienen que resolver las técnicas de seguridad informática es el acceso no autorizado a datos. En un sistema seguro el usuario, antes de realizar cualquier operación, se tiene que identificar mediante una clave de acceso. Las claves de acceso son secuencias confidenciales de caracteres que permiten que los usuarios autorizados puedan acceder a un ordenador. Para ser eficaces, las claves de acceso deben resultar