ARTÍCULO CIENTÍFICO

Problemas éticos y de la seguridad informática asociados al uso de esta tecnología

Isabel Benítez Hernández

La Informática es una rama del saber característica de nuestros días, las computadoras y todo lo que las rodea se han convertido en algo consustancial al nuevo paradigma de la sociedad post-industrial. En breve tiempo, las nuevas tecnologías de la información han llegado a ser el centro y la base de importantes operaciones de gestión. Hoy en día no es posible entender la vida social sin el servicio de estos equipos y sus redes. La mayoría de las actividades industriales, comerciales, militares, investigativas y de servicios tales como transporte, salud y la educación, entre otras, dejarían de funcionar sin el apoyo que ya hoy en día reciben de los medios informáticos.1

Consideramos que las nuevas tecnologías informáticas han cambiado nuestro modo de vivir, este desarrollo ha conllevado a cambios en la forma de actuar y de pensar de los hombres y ha traído consigo nuevas pautas de comportamiento inherentes a la dignidad humana. En los últimos años se están planteando a nivel internacional la necesidad de desarrollar e implantar el código ético y de seguridad informática que regule el saber informático.

PROBLEMAS ÉTICOS

El Código de Ética para todos los usuarios de la Informática se basa en principios éticos fundamentales y es aplicable a situaciones que caracterizan las actividades de esta tecnología. El código se centra en la esencia misma de lo que es ser un usuario de Informática.

Dicho código en la rama de la salud tiene dos componentes esenciales: uno, los principios que son relevantes para todo el personal que de una forma u otra tenga acceso a la información electrónica vinculada con la salud y el otro, reglas de conducta que describen las normas de comportamiento que se espera sean asumidas por todo el personal que se relaciona con la informática de la salud. Estas reglas son una ayuda para interpretar los principios en aplicaciones prácticas. Su propósito es guiar la conducta ética de todos los que de una forma u otra se involucre con la utilización de la tecnología informática al servicio de la salud.

Son muchos los principios que se vinculan con la ética informática dentro de los cuales y como pilar fundamental están los principios de la ética médica sin embargo los principios en que se basa el código de ética para la informática médica son los siguientes:

· **Principio de Accesibilidad**. El sujeto de un registro electrónico tiene el derecho de acceder al registro y a exigir la exactitud del mismo con relación a su precisión, integridad y relevancia.

· **Principio de Privacidad y Disposición de la Información**. Todas las personas poseen el derecho fundamental a la privacidad y,

en consecuencia, a ser informadas y ejercer el derecho de autorizar la recolección, almacenamiento, acceso, uso, comunicación, manipulación y disposición de la información sobre sí mismas.

· **Principio de Transparencia**. La recolección, almacenamiento, acceso, uso, comunicación, manipulación y disposición de información personal debe ser revelado en tiempo y forma apropiados al sujeto de esos datos.

· **Principio de Seguridad**. Todas las personas tienen el derecho a que la información que ha sido legítimamente recolectada sobre sí, sea debidamente protegida, mediante todas las medidas disponibles, razonables y apropiadas tendientes a evitar pérdidas, degradación, así como la destrucción, el acceso, uso, manipulación, modificación o difusión no autorizada.

· **Principio de Garantía**. El derecho fundamental sobre el control de la recolección, el almacenamiento, acceso, uso, manipulación, comunicación y disposición de la información personal, está condicionado sólo por las necesidades legítimas, apropiadas y relevantes de información en una sociedad libre, responsable y democrática, así como por los correspondientes derechos iguales y competentes de otras personas.

· **Principio de la alternativa menos invasora**. Cualquier acción legítima que deba interferir con los derechos del individuo a su privacidad o al control sobre la información relativa a ésta, deberá sólo ser efectuada de la forma menos invasora posible, tal que garantice el mínimo de interferencia a los derechos de las personas afectadas.

· **Principio de Responsabilidad**. Cualquier interferencia con los derechos de privacidad de un individuo o del derecho de tener control sobre la información relativa a su persona, debe ser justificada a tiempo y de manera apropiada ante la persona afectada.

Basado en estos principios la IMIA ha planteado un conjunto de reglas de conducta moral para el personal con acceso a los registros sanitarios individuales e institucionales de las unidades de salud,[2] éstos deberes morales deben comprender a todos aquellos que tienen acceso a las Nuevas Tecnologías de la Información y la Comunicación, sean éstos profesionales de la informática o solo usuarios de los mismos. Por esa razón el Código de IMIA resulta un referente obligado. Estas normas de conducta pueden ser expresadas a través de deberes morales, a continuación ejemplificaremos algunas:

- Actuar con honestidad e integridad, en caso de tomar información de diferentes fuentes para realizar una investigación, una publicación o cualquier tipo de trabajo, es indispensable poner las referencias bibliográficas que se utilizaron para el mismo, pudiendo ser penado judicialmente por una reclamación de derecho de autor de no cumplirse.

- Es importante cuando uno realiza una publicación o tiene el resultado final de un trabajo de investigación realizar el registro de la propiedad intelectual.

- Después de haber realizado el registro de la propiedad intelectual enviar las conclusiones de un trabajo realizado a los autores de fuentes importantes que se utilizaron para dicho trabajo.

- Usar correctamente las tecnologías de información médica.

- Promover y asistir a los colegas en el uso correcto de las tecnologías de información médica.

- Cerciorarse de que todas las informaciones electrónicas sean tratadas correctamente y se cumplan las medidas de seguridad que se exigen.

- Que la información electrónica se almacene, use, manipule y comunique solo con los propósitos legítimos y autorizados cumpliendo con los protocolos y mecanismos que deben estar establecidos para ello.

- Cumplir con las regulaciones establecidas para el uso de los registros de pacientes con base electrónica con el consentimiento previo.

- Todo usuario de la información electrónica debe conocer los derechos que tiene en cuanto a su acceso, uso, almacenamiento, manipulación y todo lo establecido para con la misma.

- El personal de salud que utiliza la información electrónica tiene el deber de tratar a los especialistas de informática con ética y respeto.

- Sin impugnar la reputación de los colegas debe informarse a las autoridades correspondientes sobre cualquier conducta impropia de uno de ellos, o aquello que pudiera conllevar riesgo a un profesional de la salud o un paciente.

A continuación se relacionan algunos conflictos éticos más frecuentes: uso indebido del correo electrónico, uso de programas comerciales y recursos computacionales sin la debida licencia de su autor, acceso no autorizado a redes y base de datos, pornografía en Internet, creación y uso de virus informáticos. Toda esta serie de situaciones tiene su origen en la pérdida de valores por parte de los individuos que conformamos la sociedad.

Ejemplos de estos conflictos son: La Inseguridad en Internet, todos sabemos que el correo electrónico es totalmente inseguro, en cualquier punto del camino, el correo electrónico puede ser leído por alguien sin escrúpulos; también el administrador de la máquina puede leer el correo electrónico de un usuario sin dejar señales de haberlo hecho, en las condiciones actuales no se logra prevenir la acción fraudulenta de individuos y grupos organizados que burlan la seguridad de los sistemas y llegan a producir cuantiosos daños a individuos e instituciones.

El Abuso del Correo Electrónico es muy frecuente en la actualidad, han sido tipificados un grupo de abusos entre los que figuran la divulgación de contenido inadecuado, la emisión a través de canales no autorizados, la difusión masiva no

autorizada y ataques con objeto de imposibilitar o dificultar el servicio de correo electrónico.[3]

La industria del software se ha convertido en uno de los negocios más lucrativos de los últimos tiempos, sin embargo, su futuro económico se ve ensombrecido por un fenómeno llamado piratería de software (copia ilegal de programas para computadoras).[4] Las copias de software deben ser hechas sólo con la debida autorización. Los profesionales de la Informática están obligados a proteger la integridad de la propiedad intelectual.

Recientemente, incidentes de accesos no autorizados a sistemas computacionales han ampliado la discusión de la ética en computación.[5] Las opiniones sobre el tema son divergentes, lo que sí está claro es que la intromisión no autorizada no se justifica de ninguna manera.

Un hecho que últimamente ha motivado mucha polémica en diferentes sectores de la sociedad es la pornografía en Internet. La pornografía por medio electrónicos es toda una industria que vela sus intereses económicos sin importarle las implicaciones morales y éticas en la sociedad.[4]

El uso de Internet por la industria pornográfica está creciendo rápidamente, hace 12 años pocas personas tenían acceso a tecnologías de almacenar, transmitir o recibir imágenes pornográficas por computadora, sin embargo, esta industria, en la última década, ha comenzado a utilizar las redes de computadoras para penetrar a mercados en todo el mundo, incluso en países donde está prohibido este tipo de material.

No cabe duda que la creación y propagación de virus informáticos constituye un problema ético de actualidad. Su creación tiene como único objetivo hacer daño; "Daño" significa heridas o consecuencias negativas, tales como pérdidas indeseables de información, pérdidas de propiedad, daños a la propiedad o impactos ambientales no deseados".

SEGURIDAD INFORMÁTICA

Debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información o de sus sistemas de tratamiento. Apuntaremos sólo dos ejemplos de esta vulnerabilidad creciente. Primero, con la gran expansión del uso de ordenadores personales se ha magnificado el problema de la SSI, debido sobre todo a la carencia de controles de seguridad básicos en este tipo de sistemas. En segundo lugar, la evolución hacia entornos con acceso global y múltiple, con un aumento de la conectividad entre organizaciones distintas, plantea retos importantes a la gestión de la seguridad.

Estos aspectos se relacionan con las tres características que debe cubrir la seguridad informática. Preservar estas 3 características de la información constituye el objetivo de la seguridad.

1. *Confidencialidad*: Secreto y privacidad, que la información sea revelada solo a los usuarios autorizados, en la forma y tiempo determinado.

2. *Integridad*: Precisión y autenticidad, que la información sea modificada solo por personal autorizado (incluyendo su creación y borrado)

3. *Disponibilidad*: Ataques y eficiencia, que la información sea utilizable cuando y como lo requieran los usuarios autorizados.

La Seguridad Informática se orienta hacia las actividades intencionales o premeditadas y pérdidas ocasionados por causas accidentales, tanto naturales, como las que son producto de actividades laborales o sociales. Un ejemplo de ello es cuando hay fase de alerta ciclónica como se toman todas las medidas para proteger las máquinas como desconectarlas, subirlas para pisos más elevados por si hay inundaciones, guardarlas en closet seguros o ponerlas alejadas de las ventanas y puertas con la pantalla hacia la pared, y tener pararrayos en los edificios altos.

Cada centro laboral debe tener un Plan de Seguridad Informática que es un documento básico que establece los principios organizativos y funcionales de la Seguridad Informática en un organismo, órgano o entidad, a partir de un sistema de medidas que garantice la confidencialidad, integridad y disponibilidad de la información en las tecnologías informáticas, aprobado en base al análisis de riesgo e identificación de las amenazas. El responsable máximo es el director de la entidad.

Entre los mecanismos más importantes podemos citar: Identificación y autenticación de usuarios, monitoreo y control de acceso a los recursos, trazas o registros de auditoria, protección contra virus informáticos, utilización de firewalls o cortafuegos

Podemos nombrar ejemplos de medidas de Seguridad Informática: Cuando hay la amenaza de un virus, se toman medidas con los antivirus, cuando hay la amenaza de la pérdida de la información, se toma medida con la copia de seguridad, cuando hay amenaza con accesos no autorizados, se toman medidas con los *password*, cuando hay amenaza con los intrusos externos, se toman medidas con los cortafuegos, entre otras.

Errores más frecuentes con los usuarios: Manipulación incorrecta de los documentos adjuntos en mensajes de correo, no implementar las actualizaciones de seguridad de las aplicaciones que usan, instalación de juegos, protectores de pantallas y otras aplicaciones de procedencia desconocida, no realizar respaldos de información, incorrecta utilización de los recursos compartidos, conectar módems a la computadora de manera arbitraria.

Errores técnicos más frecuentes: Conectar los sistemas a Internet sin haberlos asegurado correctamente, conectar sistemas a Internet con servicios innecesarios y con la configuración intacta de los usuarios predefinidos, no actualizar inmediatamente los sistemas cuando se detecta alguna vulnerabilidad, no realización de diagnósticos internos y externos a la red, no establecimiento de procedimientos de análisis de las trazas de los servicios que brinda la red y de la conservación de las mismas.

Errores más frecuentes en los directivos: Designación de personal sin capacitación, al área de seguridad y no garantizar su superación, aplicación incorrecta y/o parcial de actualizaciones técnicas, confiar ciegamente en un

cortafuegos, creer que la seguridad es solamente un problema técnico, minimizar el grado de sensibilidad de la información, delegar y olvidar la Seguridad Informática, poco dominio de la Base Legal de la Seguridad Informática.

Se puede concluir que en nuestro país se trabaja intensamente con el objetivo de utilizar cada día más las tecnologías de la información y la comunicación para apoyar la salud pública del país, de esta manera el MINSAP asume su proceso de informatización en el marco del proceso de informatización de la sociedad cubana para expresar con eficiencia y calidad la atención médica al pueblo, por lo que es de suma importancia el desarrollo e implementación del Código Ético y de Seguridad Informática en todas las entidades.

REFERENCIAS BIBLIOGRÁFICAS

1. Litewka, Sergio. Telemedicina: Un Desafío Para América Latina. Acta bioeth., 2005, vol. 11, No. 2, p. 127-132. ISSN 1726-569X.

2. Código de Ética de IMIA para Profesionales de la Información de la Salud. Disponible en: http://www.imia.org/pubdocs/Spanish_Translation.pdf Consultado: Enero 18, 2008.

3. Sanz de las Heras, Jesús. Abusos en el correo electrónico. Seminario Complutense de Telecomunicaciones e Información. Madrid. http://www.ucm.es/info/dinforma/activi/libro/indce/htm Diciembre 1998 . Consultado: Enero 24, 2008.

4. Silvestre Reyna Caamaño, Gerardo. Informática: Ética vs Competitividad. http://www.stats4all.com/asp/login.asp? Consultado: Enero 12, 2008.

5. Peña, Rosalía. El derecho a la propiedad sobre las bases o bancos de datos. Seminario Complutense de Telecomunicaciones e Información Madrid, Diciembre 1998.

6. Saatchy & Saatchy. Worldwide is a unit of Cordiant. Plc. November 20, 1997.

7. Ucín Guibert, José M. SJ. ¿Qué es la ética de la informática? Bilbao, julio de 1997.

8. Conger, Sue, Karen Loch, D. "Ethics and Computer Use", Communications of the ACM, Vol. 38, No. 12, p. 31-32 December 1995.

9. González García, Nerys, Torres Delgado J. Antonio, Febles Rodríguez, J. Pozo Lauzán, Pedro Rafael, et al. Informática Médica I: p. 108-110. 1998.

10. Yánez Fernández, José, García Fumero, Alberto. Redes, comunicaciones y el laboratorio de informática: p. 1-3. 2001.

11. Gallecos, Frederick. Software Piracy, some facts, figures and issues. Information System Security. 2000.

12. Siegel, Carol A., Sagalow Ty, R. Sarritella, Poul. Cyber Risks Management Technical and insurance controls for enterprises-level security. Securty Managent Practice. Sept.-Oct. 2002.

13. A.C.M. Código ético para los profesionales de la Informática propuesto por la.. en 1992. IEEE Technology and Society Magazine, No. 3, p. 18, Fall 1994.

14. Peña, Rosalía. El derecho a la propiedad sobre las bases o bancos de datos. Seminario Complutense de Telecomunicaciones e Información Madrid, Diciembre 1998.

15. Taladriz, Margarita. Libertad de expresión y redes de información. Seminario Complutense de Telecomunicaciones e Información. Madrid, Diciembre 1998.

16. Arregoitia López, Siura R. Protección contra los delitos informáticos en Cuba. GIGA Revista Cubana de Computación. No. 4, 2002.