PREPARACIÓN PARA EL DIRECTIVO

# Problemas éticos y de seguridad asociado al uso de las tecnologías de gestión de información en salud.

**AUTORES:** Dra. Lidia Ortiz Céspedes
Lic. Nadia Rodríguez Cárdenas
Lic. Ana Elizabeth Hernández Suárez
Lic. Teresa Luisa Benavides Gamiotea
Lic. Guisver Gil Green
Lic. Judith Prieto Sedano

**PROFESORES FACILITADORES:**

MsC. María Niurka Vialart Vidal
MsC. María Vidal Ledo

**Escuela nacional de salud pública (ENSAP)**
**Maestría de psicología de la salud.**
**Módulo 1: Tecnologías y gestión de información en salud**

**INTRODUCCIÓN:**

Desde el surgimiento del ser humano como ser racional se apropió, como no logró hacerlo ninguna otra especie, de un medio de comunicación especial: el lenguaje, con sus diferentes manifestaciones (oral, escrito, gestual). Iniciando un largo camino de enriquecimiento de este proceso tanto desde el punto de vista fonético, léxico como gramatical. Comenzamos a darle una especial significación a cada vocablo articulado, de ahí que hoy ante el análisis de un fenómeno social como el que nos ocupa, para comprenderlo en su esencia debamos previamente definir algunos conceptos:

¿Qué entendemos por ética?

Según la Real Academia de la Lengua Española _la "ética es la parte de la filosofía que trata de la moral y de las obligaciones del hombre" y el "conjunto de normas morales que rigen la conducta humana".(1) Luego puede aceptarse que la ética es la ciencia que trata sobre la moral, investiga aquello que es específico al comportamiento humano y enuncia principios generales y universales inspiradores de toda conducta regulado mediante normas o códigos que prescriben el buen comportamiento, las mejores prácticas y prohibiciones que definen su actuación.(2)

Y…… ¿gestión de información?

Gestión de información es el proceso mediante el cual se obtienen, despliegan o utilizan recursos básicos (económicos, físicos, humanos, materiales) para manejar información dentro y para la sociedad a la que sirve. (3)

Entendiendo la información como antesala del conocimiento, no en un campo particular, sino en todos. Sea cual sea la definición que se adopte, la información es el recurso por medio del cual el saber individual se socializa, hereda y trasciende. Proteger la información es una actitud legítima; monopolizarla, impedir que otros accedan a ella, puede ser arbitrario. Por supuesto, hay tipos de información que por su sensibilidad, por su carácter, deben protegerse. Es inaceptable, tanto un criterio absolutamente liberal en materia de acceso a la información, como una posición absolutamente restrictiva. (3)

Entonces nos preguntamos ¿Qué entendemos por seguridad informática?

Conjunto de medidas ( administrativas, organizativas, físicas, técnicas legales y educativas)dirigidas a prevenir, detectar y responder a las acciones que pongan en riesgo la integridad, confidencialidad y disponibilidad, de la informatización que se procesa, intercambie, reproduzca o conserve a través de las tecnologías de la información. (4)

Las ciencias médicas incluyen diversas disciplinas científicas que tienen como objeto de estudio al ser humano y su estado de salud. Se produce un acopio de información que requiere almacenarse y gestionarse, empleándose para la toma de decisiones en diferentes instancias a nivel individual y profesional. Esta realidad nos permite plantearnos nuevas metas que prolonguen la esperanza de vida de la población cubana

con mayor salud y calidad de vida. Por este motivo debemos ser estrictamente rigurosos en el cumplimiento de las normas éticas y de seguridad para la custodia de esta información.

A partir de la década de los 90, con el proyecto de informatización del Sector en que se definen sus principios de desarrollo, se contempla la incorporación de las Tecnologías de la Información y las Comunicaciones en los procesos de la salud. Comienza a incorporarse en proyectos particulares el código de ética y el plan de seguridad y contingencia informática.

Con este trabajo pretendemos acercarnos a elementos generales sobre estos temas.

**DESARROLLO:**

Teniendo en cuenta que en el sistema de salud el centro de acción y de atención es el paciente, entendido como una entidad biopsicosocial, la concepción de los sistemas de seguridad informáticos que se conciban han de tener presente que no se protegen datos fríos, aislados, sino información personal sobre la situación de salud de millones de pacientes.

Por las características especiales del sistema de salud cubano (gratuito, masivo, etc.) un mismo individuo es atendido multifactorialmente por varias entidades de salud (policlínicos, hospitales, clínicas estomatológicas, farmacias) etc. lo que genera gran número de información que se entremezcla en los sistemas de información de salud, para la toma de decisión clínica o para el proceso de dirección en salud en los diferentes niveles, por esto todo el personal profesional o técnico vinculado al manejo de esta información ha de ser sumamente cuidadoso con su custodia.

Por lo que es de vital importancia al crear un modelo ético y de acceso a la información, tener en cuenta: respetar el derecho de acceso a la información y el derecho a la privacidad, desarrollando estrategias para proteger la intimidad de los individuos y organizaciones; respetar los derechos de autor, sin distinción de tipo de soporte o medio de transmisión de la información; establecer los límites de acceso a la información según la jerarquía e interés institucional y personal; promover la creación de entidades que regulen y controlen la transmisión y el uso de los datos en las redes informáticas; formar y capacitar, en los diferentes niveles educativos, sobre conceptos básicos del proceso de la gestión informática.

Es oportuno mencionar un documento que no es un código de ética, pero que constituye una propuesta, que pudiera adquirir ese estatus. Se trata del reglamento que controla el acceso, uso y transmisión de la información que circula en la red de Infomed que pertenece al Centro Nacional de Información de Ciencias Médicas.

Establece, entre otros elementos, aspectos que deben cumplir los usuarios y la administración del sistema.

**Los usuarios:**

1. Son responsables de garantizar que la información a la que accedan cumpla con los objetivos científico-técnicos para los que se creó la red.
2. Las cuentas no deben utilizarse con fines lucrativos o de índole personal, deben garantizar que estas no se utilicen por terceras personas.

3. Queda prohibida la distribución de información mediante la red no acorde con los principios revolucionarios, deberán informar inmediatamente a la administración de la red cualquier tipo de ataque proveniente de organizaciones contrarrevolucionarias.
4. La administración central de la red se reserva la facultad de sancionar a los usuarios finales que incumplan el código de ética vigente.

**La administración del sistema:**

1. Están en la obligación de garantizar la calidad de la información que se genere en sus distintos segmentos.
2. Es responsable de suministrar y administrar las direcciones y dominios que forman la red.
3. Las instituciones que forman parte de la red deberán presentar una carta firmada por el director de la institución, donde se especifiquen los datos de la persona responsable de administrar esa entidad.
4. Queda prohibido terminantemente la distribución por ella de información no autorizada por los niveles correspondientes o que no se ajuste a sus propósitos fundamentales.
5. Las administraciones de la red, deberán garantizar la integridad y calidad de la información científica que proviene de ellos.(5)

El acceso público en Internet a estudios médicos provisionales puede llevar a consumir los medicamentos inadecuados, o a dejar de tomarlos en virtud de una información inadecuada. Además, los sitios médicos y de salud en el web tienen la obligación particular de proteger la privacidad y la confidencialidad de los individuos. Los pacientes y los individuos con interés en patologías particulares deben sentirse seguros al obtener información y utilizar los recursos en el sitio, sin inquietud de que tal uso se identificará con ellos sin su permiso, por ejemplo: imágenes fotográficas de los pacientes que deben ser autorizadas en caso de que se vayan a transferir a la Web.

Deben cumplirse con los principios de la privacidad y la confidencialidad para compartir legal y éticamente información importante acerca de las patologías de los pacientes. (Registro médico electrónico) (6) Mediante el intercambio de esta información puede mejorarse la atención clínica al individuo mediante la investigación médica.

Las publicaciones médicas, impresas o en línea, no deben revelar información que identifique al individuo sin su consentimiento informado y manifiesto. Estos principios se aplican a la información en las publicaciones médicas, y a puntos de reunión menos formales, como los grupos de discusión en línea, los espacios de conversación interactiva y las listas electrónicas.

La publicación electrónica crea una polémica en torno a las ventajas y desventajas de éstas con respecto a las publicaciones en papel: la posible ausencia de arbitraje de los trabajos científicos, la autoría cuestionada de algunos de ellos, los posibles cambios de la información electrónica, la facilidad de los lectores para consultar la información, entre muchos otros; se contraponen a ventajas como las potencialidades de las publicaciones electrónicas, para expandir rápidamente información actualizada a amplios mercados. Estas cuestiones también se analizan brevemente desde la óptica de la Unidad de Análisis y Tendencias en Salud, entidad del Ministerio de Salud Pública de Cuba, que ha comenzado ha insertarse en el entorno de la publicación electrónica.

Los manejos adecuados de esta plataforma tecnológica, puede propiciar el contacto entre todos los hombres o posibilitar conflictos; por lo que la función del profesional

de la información, ante el acceso a la información que circula debe estar respaldado por respeto a los demás y a su desempeño.

Las normas, reglas y principios del uso, acceso y transmisión de la información se rigen por determinados valores éticos que se corresponden con la misión de nuestra organización, los principios y valores de esta.

Entre estos principios se encuentran:

**1. 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.

**2. 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.

**3. 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.

**4. Principio de Acceso**

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.

**5. Principio de Resguardo Legítimo** (*Legitimate Infringement en inglés)*

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.

**6. 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, según lo establecido en el Principio Nº 1; deberá sólo ser efectuada de la forma menos invasora posible, tal que garantice el mínimo de interferencia a los derechos de las personas afectadas.

**7. 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.

Así mismo, basado en ellos plantean las "Reglas de conducta ética para profesionales de la Información en Salud, definiendo:

- **Deberes centrados en los sujetos.**
- **Deberes hacia los profesionales de la Salud.**
- **Deberes hacia las instituciones y empleadores.**
- **Deberes hacia la sociedad.**
- **Deberes sobre ellos mismos.** (Profesionales de la Información en Salud).
- **Deberes hacia la profesión.**

Dada la significación de los datos que se procesan en el sector, se hace necesario elaborar un plan de seguridad informático.

Hay tres aspectos fundamentales que definen la seguridad informática:

- Confidencialidad.
- Integridad.
- Disponibilidad.

**Confidencialidad**

Condición que asegura que la información no pueda estar disponible para personas, entidades o procesos no autorizados. En la salud, las normas éticas, técnicas y de procesos aseguran que los usuarios pueden acceder sólo a la información asistencial, que les está permitida en base a su nivel de autoridad o jerarquía, normalmente impuestas por disposiciones legales, administrativas o del servicio que brinda. En entornos de administrativos o dirección, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, situaciones inusuales en el estado de salud de la población, que son requeridos en la toma de decisiones.

**Integridad**

Es el servicio de seguridad que garantiza que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado, permite asegurar que no se ha falseado ni alterado la información, ni intencional, ni accidentalmente.

En el ámbito de las comunicaciones, un aspecto de la integridad es la autenticidad, proporciona los medios para verificar que el origen de los datos es el correcto. En los procesos de salud normalmente es muy importante mantener la integridad y precisión de los datos ya que de acuerdo a ellos se actúa, ya sea en la toma de decisión médico - paciente, como en la de dirección del Sistema, en cuanto a los procesos involucrados

en la salud y calidad de vida de la población. Se usan para ello códigos, firmas añadidos a los mensajes en origen y recalculadas, comprobadas en el destino.

**Disponibilidad**

Es el grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Significa que el sistema informático, se mantiene funcionando eficientemente y que puede recuperarse rápidamente en caso de fallo, lo contrario significa denegación del servicio de hecho muchos ataques de virus existentes consiste no en el borrado de la información sino en el bloqueo de esta.

Estos principios deben formar parte de la política de seguridad de la institución: **Política de Seguridad Institucional**. La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.(7)

**REGLAS BÁSICAS PARA ESTABLECER UNA POLÍTICA DE SEGURIDAD INFORMÁTICA ADECUADA**

- La política de seguridad debe adecuarse a nuestras necesidades y recursos.
- Debe tener en cuenta el valor que se le da a los recursos y a la información.
- El uso que se hace del sistema en todos los departamentos.
- Deben evaluarse los riesgos, el valor del sistema protegido y el coste de atacarlo.
- El conocimiento del sistema a proteger y de su entorno.
- El conocimiento y experiencia en la evaluación de riesgos y el establecimiento de medidas de seguridad.
- El conocimiento de la naturaleza humana, de los usuarios y de sus posibles motivaciones.

En base a lo anterior se elabora el Plan de Seguridad y Contingencias Informáticas, basado en la identificación y análisis de riesgos, detectando los aspectos que hacen al Sistema Informático susceptible de ser atacado, que no son mas que las debilidades en el sistema informático. Las amenazas posibles como: ataques de personas, programas malignos, sucesos naturales o de otra índole y las medidas técnicas de protección frente a ellas

Dada la importancia del tema de seguridad en la información, aún cuando no esté informatizado el proceso, se recomienda realizar el análisis de riesgos en aquellos lugares como Archivos de Historias Clínicas, Imagenología, Biblioteca y otros, donde se archiva y custodia información sensible y que paulatinamente se incorpora en el proceso de Informatización del Sector.

Se recomiendan una serie de medidas generales a tener en cuenta por el personal que tenga un equipo a su custodia:

1-Mantener el equipo con password en el Setup, Red, y Refrescante de pantalla, como medida preventiva estas claves deben estar en sobre sellado en la dirección pues ante situaciones especiales, se pueda mantener la actividad de Salud.

2- Mantener instalado un Antivirus con actualización constante, para evitar ataques que persiguen afectar la salud de las personas, la economía, las investigaciones, la toma de decisión o los servicios en general, y robar la información que puede ser sensible o clasificada.

3- Controlar o supervisar las comunicaciones a través de las trazas, explicando la necesidad de mantener este recurso lo más óptimo y no congestionado para que su acceso sea lo más rápido posible.

4- Mantener actualizados los estudios de vulnerabilidad, que permite tener un control de los medios y la técnica de la cual se dispone en el centro, e informar a los niveles superiores y efectuar las mejoras en los equipos y los softwares, así como conocer los puntos críticos y estar preparados para cualquier situación emergente.

5- Detectar donde los recursos deben estar por su importancia y tomar las medidas de protección física y lógica, sobre los equipos y la información contenida en ellos.

6- Conservación y custodia, mediante métodos de almacenamiento y compactación que permitan clasificar y guardar la información en el más mínimo espacio, para su más rápido acceso de forma compactada y protegida de acuerdo a su nivel de confiabilidad. Realizar las salvas físicas periódicas y ubicarlas en lugares apropiados fuera del área donde se originan. (7)

Un elemento vital es la preparación del proceso de recuperación tras un ataque, y la posibilidad de volver a la situación anterior al mismo habiendo reemplazado o recuperado el máximo de los recursos en equipos e información.

La recuperación de la información se basa en el uso de una política de copias de seguridad adecuada, mientras la recuperación del funcionamiento del sistema se basa en la preparación de recursos alternativos.

Los procesos de la salud en general y aquellos dirigidos a la atención directa a pacientes, como son los de apoyo al diagnóstico, atención y tratamiento, son altamente sensibles y es por ello que su seguridad es una constante preocupación en el proceso de informatización del Sector y sus objetivos se encaminen a lograr una cultura de seguridad en los trabajadores de la salud que integre a su conducta cotidiana, el cumplimiento de política institucional y las medidas del Plan de Seguridad de manera útil y funcional.

El Estado cubano consciente de la necesidad de la existencia de una base legal ha legislado decretos y leyes para el respaldo del cumplimiento de las medidas establecidas en el plan de seguridad informática entre ellas podemos citar:

- Resolución 6/96 del MININT.
- Decreto Ley 199/99 del Consejo de Estado.
- Resolución 188/2001 del MIC.
- Resolución 269/2002 del SIME.
- Instrucción 1/2004 del VM de desarrollo del SIME (Requisitos y Procedimiento a tener en cuenta para el acceso a Internet en las Entidades del SIME).
- Resolución 12/2007 del MIC.(4)

**CONCLUSIONES:**

- Los avances tecnológicos en la Salud Pública cubana representan un nivel cualitativo superior de desarrollo científico técnico en el sector, pero a la vez traen consigo problemas éticos y de seguridad
- Se impone la necesidad de crear y supervisar el cumplimiento de los mecanismos, para minimizar los problemas éticos y de seguridad asociados al uso de las tecnologías de gestión de información, por las características especiales de nuestro sector
- Urge fomentar en los profesionales, técnicos y trabajadores de la salud en general la responsabilidad individual y colectiva en la aplicación de las medidas del Plan de Seguridad Informática en cada centro asistencial o institución.

**REFERENCIAS BIBLIOGRÁFICAS:**


1-Diccionario de la Real Academia de la Lengua Española. Sitio consultado: 12/02/2008 URL: http://www.rae.es

2-Rojas M., Y, Cabrales H., G., Chaviano, O.G., Santos JM., Molina G.,A. La ética: un nuevo reto para el profesional de la información en el siglo XXI. Revista Electrónica ACIMED, Vol. 12. No. 2. Marzo - Abril 2004. Versión electrónica, última actualización 2005. Sitio consultado: 12/02/08. URL:http://bvs.sld.cu/revistas/aci/vol12_2_04/aci10204.htm

3- Ponjuan DG., Gestión documental, de información y del conocimiento…..punto de contactos y diferencias. [CD-ROM]. Maestría de Psicología de la Salud. ENSAP-CEDISAP. 1987-2006.

4- Vialart VN., Seguridad informática. Módulo de Gestión de Información en Salud. Aula Virtual. [Disponible en **http://www.aulauvs.sld.cu**.] Maestría de Psicología de la Salud.

5- Infomed. Reglamento de Infomed [en línea]. Disponible en:

http://www.sld.cu/servicios/Pg56m.htm[Consultado: 10 de octubre del 2002].

6- Código de ética de IMIA para los profesionales de la información en salud. Sitio en Internet consultado 13/2/08.

URL: www.gibba.org.ar/docencia/codigo%20imia.doc

7- Vidal L M. Información, Tecnologías y Ética en salud. CECAM-ENSAP.Sitio consultado 12/2/08.

URL:www.cecam.sld.cu/pages/rcim/revista_9/articulos_pdf/eticaensalud.pdf