COMUNICACIONES -> Gestión de riesgos. Seguridad de pacientes

Plan de mejora en la seguridad de la información del paciente.

- **AUTORES:**
Andrés Muñoz Soto; José Javier Aranda Lorca; José María Olivares Morales.; Pablo Vigueras Paredes; Luis Joaquín González-Moro Prats; Manuel Alcaraz Quiñonero

- **INTRODUCCIÓN:**
El alto grado de informatización de los centros sanitarios hace que cada vez sea más la información del paciente guardada en soportes informáticos (CINTAS, PACK, HD, etc). Esto hace a su vez que la dependencia que la actividad clínica diaria tiene sobre el funcionamiento de los sistemas de información sea mayor.

  Es necesario garantizar al profesional sanitario que la información se encuentre disponible cuando se necesite, y al mismo tiempo proporcionar al paciente la confidencialidad de la información tal y como dice la Ley Orgánica de Protección de Datos. (LOPD).

  Hay que establecer mecanismos encaminados a mejorar la seguridad de los sistemas de información, garantizando la disponibilidad, confidencialidad autenticación e integridad de la información.

  El trabajo realizado está enfocado como un ciclo de mejora apoyado en la metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT), desarrollada por el Consejo Superior de Informática perteneciente al Ministerio de Administraciones Públicas.

- **MATERIAL Y MÉTODOS:**
Ley Orgánica de Protección de Datos. 15/1999
Reglamento de Medidas de Seguridad. Real Decreto 994/1999 de 11 de Junio.
Metodología de Análisis y Gestión de Riesgos en los Sistemas de Información. MAGERIT.
Sistema Informático del Hospital Virgen del Castillo.

  MÉTODO:
Aplicando la metodología de análisis y gestión de riesgos en los sistemas de información (MAGERIT), identificamos activos del sistema de información , amenazas a estos activos, vulnerabilidades y medidas a adoptar encaminadas a la protección de los activos.

  Dividimos el estado de seguridad de los sistemas de información en cuatro subestados:
1) SUBESTADO A DE AUTENTICACION.
2) SUBESTADO C DE CONFIDENCIALIDAD.
3) SUBESTADO I DE INTEGRIDAD.
4) SUBESTADO D DE DISPONIBILIDAD.

  En cada uno de estos subestados decidimos actuar sobre el activo más vulnerable, con mayor amenaza para la organización y menor coste en la implantación de la medida de seguridad a adoptar que nos permita la mejora en la seguridad de un subestado. Posteriormente ponemos en marcha un plan de mejora que se detalla a continuación.

  SUBESTADO A DE AUTENTICACION:
Dentro de este subestado seleccionamos el activo información y decidimos incidir sobre la identificación de los usuarios del sistema de información en el acceso a la información del paciente.

  Tomamos como subcriterio de calidad la IDENTIDAD DE LOS USUARIOS DEL SISTEMA DE INFORMACION.
Medimos los usuarios que acceden al sistema de información con login único, es decir, con identificación personal.
Se cumple este subcriterio de calidad en un 17%. (Medida tomada año 2003).

  Medidas a adpotar encaminadas a mejorar el subestado de autenticación:
1) Se dejan de dar usuarios genéricos para el acceso a los sistemas de información.

  2) Se establece un mecanismo por servicios para la sustitución de login genéricos por personales.
Actualmente el 97 % de los usuarios que acceden al sistema lo hacen con login único. Limitaciónes en las aplicaciones informáticas así como la idiosincrasia de la organización (controles de enfermería), hacen que a fecha de hoy sea imposible llegar al 100%.

  SUBESTADO C DE CONFIDENCIALIDAD:
Dentro de este subestado seleccionamos el activo información y tomamos como medida de mejora de la seguridad en este subestado, la cumplimentación del documento de confidencialidad por parte de los usuarios que acceden al sistema de información del paciente.

  Tomamos como subcriterio de calidad NUMERO DE USUARIOS DEL SISTEMA DE INFORMACION DE PACIENTES QUE HAN FIRMADO EL DOCUMENTO DE CONFIDENCIALIDAD.

  Este subcriterio de calidad se cumple en un 0%. (Año 2003)

Medida a adoptar encaminada a la mejora de este subcriterio de calidad:
1)Se establece como requisito imprescindible y previo al alta de un usuario en los sistemas de información de pacientes la cumplimentación del documento de confidencialidad.

2)Se pone en marcha un plan de formación e información en materia de confidencialidad y protección de datos. Dirigido a todo el personal y con el objetivo de que el profesional disponga de toda la información necesaria para firmar el documento de confidencialidad.
Actualmente el 100% de los usuarios que acceden al sistema con login único tiene firmado el documento de confidencialidad.

SUBESTADO I DE INTEGRIDAD:
Previene contra la modificación o destrucción de activos. La integridad está vinculada a la fiabilidad funcional del sistema de información. Puesto que las aplicaciones informáticas utilizadas son desarrolladas por empresas externas seleccionamos dentro de este subestado el activo copias de seguridad del sistema de información.

Tomamos como subcriterio de calidad el PROCEDIMIENTO DE REALIZACION DE COPIAS DE SEGURIDAD.
En el año 2003 se hacia una copia de seguridad diaria y se utilizaba una cinta para todos los sistemas.

Medidas adoptadas para mejorar este subcriterio de calidad:
1) Ampliar el número de cintas así como el número de copias. Utilizar una cinta por sistema así como una copia por servidor.

2) Guardar las cintas que contienen las copias de seguridad en una caja fuerte inífuga y en ubicación distinta a los servidores.

Actualmente esta medida está totalmente en funcionamiento.

SUBESTADO D DISPONIBILIDAD:
Dentro de este subestado seleccionamos el activo ordenador personal. Identificamos como principal causa que afecta a la disponibilidad de este activo la entrada de virus.

Tomamos como subcriterio de calidad el SISTEMA DE PROTECCION ANTIVIRUS.
En el año 2003 el porcentaje de averias en los ordenadores personales motivado por la entrada de virus era de un 69 %.
En el año 2003 el porcentaje de ordenadores personales con sistema de detección de virus era de un 23 %.
El sistema de instalación del programa antivirus era local al propio ordenador.

Medidas adoptadas para mejorar este subcriterio de calidad:
1) Instalación de un sistema de protección de virus centralizado en un servidor informático. De tal forma que con el menor tiempo posible se instale en todos los ordenadores las actualizaciones del programa de detección de virus, así como las del fichero de firmas.

Actualmente se encuentra en funcionamiento el sistema centralizado de protección antivirus .

El porcentaje de ordenadores personales a los que llega este sistema centralizado es de un 93 %.

El porcentaje de ordenadores que dejan de estar disponibles y cuya causa es la entrada de virus o derivados es de un 6%.

- **CONCLUSIONES:**
Conseguir un sistema de información seguro es una tarea compleja en la que las medidas tecnicas y organizativas han de ir de la mano.

Paralelamente al avance de la informatización de los servicios en las instituciones sanitarias, debe ir la puesta en marcha de las medidas de seguridad encaminadas a garantizar la disponibilidad, confidencialidad e integridad de la información. No basta con informatizar los servicios, hay que garantizar el correcto funcionamiento para que el profesional vea la informatización como una verdadera ayuda y no como un problema.

La aplicación de la metodología MAGERIT puede ser una herramienta útil para dirigir los esfuerzos de la organización a mejoras eficientes en la seguridad de los sistemas de información