Programa de seguridad de la información (Propuesta para los Hospitales Militares)

*Ricardo Linares Alvarez de Sotomayor**
*José Mª Gervas Camacho***
*Carmelo Perea Perea****
*Juan Alfonso de la Torre*****
*Manuel Marcos de Cabo******

RESUMEN

La información debe llegar a los diferentes niveles asistenciales sanitarios asegurando los contenidos que les corresponda. En este estudio se pretende establecer una sistematica sobre la seguridad de la información sanitaria.

SUMMARY

Information should reach the different levels of medical assistance with the assurance that the contents is the appropriate one for each. In this study an attempt is made to establish a system for the security of medical information.

1. INTRODUCCION

1.1. FUNDAMENTOS

Los efectos positivos de la aplicación informática son innumerables y obvios, pero entre sus puntos débiles se encuentra el riesgo que significa depender de ellos en tan alto grado.

A medida que el número de terminales va aumentando y dispersándose por todo el hospital, el concepto de seguridad va tomando un significado coda vez más preocupante.

Los últimos datos fiables sobre este tema, indican que la inversión media de las empresas españolas en materia de seguridad representa el 4 por ciento del total del gasto informático.

* *COL.SAN.(MED.)*
** *TCOL.SAN.(MED.)*
*** *CTE.SAN. (MED.)*
**** *CTE. INF.*
***** *TTE. ART.*
(Hospital Militar Central "Goméz Ulla").

1.2. RIESGOS

Todo sistema informático soporta varios tipos de riesgo claramente diferenciados y que se puedan agrupar en:

* RIESGOS EXTERNOS
- Naturales.
- Humanos.
- Accidentales.

* RIESGOS INTERNOS.
- De tipo técnico.
- Humanos.

Voluntarios e involuntarios.

Dado el motivo de estas reuniones, nos centraremos exclusivamente en los riesgos externos humanos y en los internos, pues la seguridad contra el resto de los tipos de riesgos se encuentra a un nivel más que aceptable.

1.3. PROBLEMAS

Los puntos que propician la inseguridad informática desde el punto de vista del personal del propio sistema son:

* El confusionismo operativo.
- Desconocimiento del Sistema (normas de acceso y uso)
- Alto número de usuarios.
- Criterios de contratación.

* Los intereses particulares o de grupo.
* El descontento laboral.
- Alta movilidad de los usuarios.
- Personal no fijo en los puestos de acceso a los nudos de información.

* Los controles inadecuados.
* El desinterés ante las amenazas.
* Las investigaciones deficientes.
- Terminales compartidos.
- Software de control deficiente o escaso.

2. CONCEPTO DE SEGURIDAD DE LA INFORMACION

Seguridad Informática o Seguridad Lógica, se puede definir como el conjunto de medidas de protección económicamente rentables, que abarcan a todo el Sistema Informático del Hospital, enumerando como partes principales:

* El Sistema físico-lógico. (informático).
* La información.

3. PROGRAMA DE SEGURIDAD

3.1. ESTABLECIMIENTOS DE PROCEDIMIENTOS

La protección, fundamentalmente, hace referencia a:

* La intimidad de la información individual.
* La confidencialidad de los datos sobre una colectivo de individuos.
* La integridad de la información sobre estos datos.
* La disponibilidad de toda la información del hospital.
* El entorno de los edificios y maquinaria.

El método empleado para la obtención de la seguridad, debe ser global y contemplar todos los aspectos referentes a la información tanto mecanizada como la manual. De nada serviría tener un sistema informático inviolable si el archivo físico de historias clínicas es de libre disposición para todo el personal de hospital.

La INTIMIDAD se consigue mediante la concienciación del personal que manipula la información.

La CONFIDENCIALIDAD se consigue mediante la clasificación de la información, estableciendo normas sobre ella, creando controles para velar por ella y detectando las transgresiones que se pudieran producir.

La INTEGRIDAD supone conseguir que la información esté actualizada y sea exacta y completa; cosa que se logra con una detallada organización, en la que se deberan incluir procedimientos puntuales de control y desarrollo, así como una estructuración de las tareas para prevenir errores.

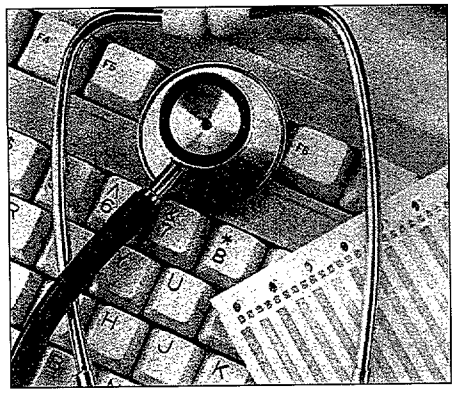
La DISPONIBILIDAD implica la posibilidad real de acceso a la información en cualquier momento. Esto se consigue con un adecuado Plan de Backups, (Información duplicada para seguridad).

La SEGURIDAD FISICA de la información implica un acceso restringido del personal al C.P.D.(Centro de Proceso de Datos).

3.2. DEFINICION DE LOS NIVELES DE SEGURIDAD Y EL NIVEL DE RIESGO

El principio básico de todas las normas empleadas por el Departamento de Defensa de los Estados Unidos, es la prohibición expresa de rebajar la clasificación de la seguridad, con controles obligatorios y discreccionales de acceso, la identificación y la autentificación.

Conviene identificar el nivel de seguridad que se pretende conseguir y por lo tanto el nivel de riesgo que se puede asumir, habida cuenta que la seguridad total es imposible y que el nivel de seguridad y el costo necesario para alcanzarla están relacionados por la función $COSTO=2x^2$ (siendo x el nivel de seguridad).



3.3. EL AUDITOR INFORMATICO, FUNCIONES GENERALES

Es importante para el mantenimiento del nivel adoptado, la existencia de un responsable de seguridad informática, que no debe depender de ninguno de los departamentos en los que vaya a realizar su trabajo y elevará sus informes directamente al director del hospital.

Este deberá aconsejar en todas o alguna de las siguientes áreas:

* Los criterios de seguridad corporativa.
* La protección del C.P.D., las comunicaciones y los terminales.
* La definición y ejecución de los estándares y procedimientos de seguridad.
* El cumplimiento de la legislación vigente en materia de seguridad.
* La evaluación de riesgos y su seguimiento.
* Implementación y administración de los equipos de seguridad.

3.4. PLAN DE EMERGENCIA Y SEGURIDAD

3.4.1. CONOCIMIENTO DE LOS RIESGOS

Se pretende con el presente plan de obtener un buen servicio de la informática, que la información con la que se trabaja sea íntegra y que los datos y el material estén seguros. Para ello se tendrán en cuenta tres tipos de riesgos:

RIESGOS FISICOS,(Técnicos): Son aquellos que afectan a los soportes e información pero sin intencionalidad.

RIESGOS DOLOSOS, (Intencionales): Son aquellos que se producen de forma intencionada, como por ejmplo:

* Acceso indebido a ficheros.
* Robos de soportes (cintas, listados, etc).
* Sabotaje de ficheros y programas.
* Falsificaciónes.
* Manipulación.
* Utilización indebida de la información.

RIESGOS POR MAL FUNCIONAMIENTO,(Involuntarios): Son aquellos que se derivan de una mala utilización no voluntaria, como por ejemplo:

* Mala transmisión de los datos.
* Pérdida de soportes (discos, cintas, etc.).
* Mal funcionamiento del ordenador.
* Funcionamiento defectuoso de los programas.
* Mala utilización de los usuarios.

3.4.2. CLASIFICACION Y CONTROL DE LA INFORMACION

Para establecer el nivel que deseamos para cada caso, conviene establecer las categorías de la información que se posee.

Se establecen las siguientes categorías:

PERSONAL: Información sobre el personal, salarios, exámenes médicos, pensiones, aspectos laborales, etc.

RESTRINGIDA: Es la información que si se hiciera pública causaría transtornos al individuo.

RESERVADA: Información que de ser conocida por determinadas personas o grupos, perjudicarían gravemente al colectivo militar.

CONFIDENCIAL: Información que si fuera conocida por personal no autorizado causaría daños y perjudicaría al hospital.

SECRETA: Asuntos que una vez filtrados llevarían al hospital a la no operación.

3.4.2.1. AREAS

Desde el punto de vista hospitalario, se ponen en correlación las siguientes grandes áreas de trabajo con influencia en las distintas aplicaciones:

*AREA ASISTENCIAL GENERAL: Gestión fundamentalmente clínica, realizada por personal clínico, con aplicaciones como por ejemplo enfermería, urgencias, etc.

*AREA ADMINISTRATIVA: Gestión realizada por personal administrativo con aplicaciones como por ejemplo facturación, secretaría de planta, admisión, etc.

*AREAS ESPECIFICAS: Basadas en una gestión puramente departamental, caracterizadas por un número reducido de usuarios.

Aqui se pueden separar las aplicaciones según su grado de conexión con el Area Asistencial en:

- INDEPENDIENTES:
* Nómina.
* Personal.
- GENERALES:
* Dirección.
* Información al público.
* Informática.
* Mantenimiento.
- PETICIONARIAS
* Almacén.
* Archivo.
* Cocina.
* Consulta externas.
* Exploraciones funcionales.
* Farmacia.
* Laboratorio.
* Radiología.

AREA PERICIAL: Basada en una gestión puramente aplicada a los tribunales médicos militares y confección de informes periciales.

Este área debe ser totalmente estanca de manera que la información que en ella se obtenga no sea explotable por el resto de las áreas del hospital.

3.4.2.2. NIVELES DE INFORMACION:

En la actualidad están definidos los siguientes niveles de información en razón de su empleo, responsabilidad, ubicación y función.

NIVEL	NUDO MILIT.	NUDO CLIN.	AREA ASISTENCIAL	A. ADMINISTRATIVA.	AREA ESPECIF.	AREA PERICIAL
0	S	S	Jefe Area	Jefe Area	Jefe Area	Presidente
1	S	S	Jefe Servicio		Jefe Servicio	Jefe Servicio
2	S	S	Med. Servicio	Jefe Negociado	Med./ Mando intermedio.	Jefe Negociado
3	N	S	Supervisora		Supervisora	
4	N	S	ATS, corretu.		ATS.	
5	S	S		UF1 (Secretaria)	UF1 (Secreatria)	Administrativo.
6	N	N	UF2		UF2 (M.Consultas Ext)	
7	S	S	C.P.D.	C.P.D.	C.P.D.	C.P.D.
APLICA. Ejemplos			HOSPITAL. URGENCIA	ADMISION FACTURAC.	COCINA ARCHIVO	TRIBUNAL REGIONAL

Tabla 1

> 0 — Jefe de Area, Subdirección o Departamento.
> 1 — Jefe de Servicio o Negociado.
> 2 — Médicos de un Servicio (básicamente pueden acceder a visualizaciones de su responsabilidad)
> 3 — Supervisoras.
> 4 — ATS (Enfermeras fijas de planta o correturnos).
> 5 — Usuario final 1. (UF1) (Ejemplo Secretaría).
> 6 — Usuario final 2. (UF2) (Ejemplo soldado de consultas externas).
> 7 — Explotación. Personal del Servicio de Informática.
> 7.1 — Explotación sistemas.
> 7.2 — Explotación desarrollo.

3.4.2.3. NUDOS DE PELIGROSIDAD DE LA INFORMACION

Se establecen básicamente dos puntos neurálgicos:

CLINICO: Correlación Nombre de Paciente /Diagnóstico OMS/ Procedimiento quirúrgico.

MILITAR: Correlación Nombre de Paciente /Domicilio/Destino/ Dirección y Teléfono.

Consecuentemente con ésto y, puesto que el nombre del paciente debe estar permanentemente presente, hay que separar en determinadas visualizaciones, por niveles y usuarios el DIAGNOSTICO y DOMICILIO. Y marcar como nivel de riesgo aceptable el no permitir el listado de la totalidad de la información en todos los puntos del sistema (ver Tabla I).

NUDO CLINICO (Visualizar DIAGNOSTICOS del paciente).

NUDO MILITAR (Visualizar DESTINO, DIRECCION y TELEFONO del paciente).

3.4.3. RESPONSABILIDAD Y CONTROL DE ARCHIVOS

Refiriéndonos a las responsabilidades con respecto a la información podemos diferenciar entre:

* El propietario de la información.
* El Usuario.
* El Depositario.

EL PROPIETARIO (Auditor informático):

Define la problemática a resolver por la plicación. Establece los requisitos de seguridad y fija los niveles de confidencialidad. También es el encargado de autorizar al personal para acceder a la información, según unos criterios y límites:

1. Solo lectura.
2. Acceso parcial a los datos.
3. Lectura y modificación de la información.
4. Acceso total a la información (Añadir, modificar, borrar, leer).

EL USUARIO:

Es la persona o personas autorizadas a acceder a la información en

alguno de sus niveles. Deberán responder del modo y límites autorizados.

EL DEPOSITARIO (Servicio de Informática):
Es el responsable de la custodia, conservación y actualización de los datos.

3.4.4. CONOCIMIENTO DE LAS SALIDAS

Por otra parte es importante para el establecimiento de un sistema informático seguro, la identificación de todas las puertas (salidas permanentes) del sistema, y controlar su utilización.

En la actualidad se dispone de:

- Una conexión a la RED IBERPACK, que permitirá en un futuro próximo la conexión a otros hospitales en el trabajo diario.
- Una conexión "punto a punto" con el Hospital del Aire que permite disponer de dos bases de datos gemelas, para asegurar la disponibilidad de la información.
- Un módem que permite a la empresa instaladora conectarse con cada hospital para averiguar posibles averías y mantenimiento del sistema.

4.UTILIZACION DE LA INFORMACION

Según el nivel en el que nos encontramos, identificamos la relación que se tiene con el Sistema, de esta manera en el siguiente cuadro vemos los cuatro niveles fundamentales y su función correspondiente. (Ver Tabla II).

5. FUNCIONES ESPECIFICAS DEL RESPONSABLE

Cada responsable, a su nivel, será el encargado de ejecutar con exactitud el plan de seguridad establecido.
El Auditor Informático para temas de seguridad será el encargado de:

* Marcar los criterios de seguridad.
* Dictar las normas de ejecución.
* Definir procedimientos.
* Vigilar el cumplimiento de la legislación, general y particular.

FUNCION	ESTADO
Utiliza la información.	Dirección.
Asesora en las medidas de control.	Auditor.
Responsable de la integridad.	Servicio de Informática.
Alimentan el sistema.	Usuarios finales.

Tabla 2

CONTROL DE ACCESO AL C.P.D.

Es el factor más importante en el conjunto de cualquier seguridad.
El personal que está relacionado directa o indirectamente con el sistema informático puede de forma accidental o descuidada así como deliberada constituir una amenaza para la seguridad, por lo tanto no debería permitirse la entrada a toda persona ajena al C.P.D.La puerta permanecerá cerrada permanentemente.
Cualquier persona ajena al Servicio de Informática será tratada como visita registrándosela en el correspondiente libro de visitas, la hora de entrada, la hora de salida y el motivo de la misma.
Solo con el hecho de estar autorizado a entrar al C.P.D. ya se está en posesión de dos de los tres requisitos básicos para cometer un acto delictivo: oportunidad y capacidad; todo el sistema quedaría por lo tanto pendiente de que esa persona tuviera también el tercer requisito, el motivo.
Disponer de una ventanilla o similar para la relación con el personal que trate de recoger los listados diarios distintos a los que el propio personal del centro reparta diariamente; y contar con una salida de emergencia en el lado opuesto a la entrada principal, son dos ejemplos más de las medidas que son necesarias en cualquier C.P.D:

6. CONCLUSIONES

Para terminar, podríamos relacionar unos cuantos ejemplos de acciones a tener en cuenta en el establecimiento de cualquier sistema de seguridad.
No utilizar personal temporal al preparar material muy delicado.
Dar a los borradores la misma categoría que al documento terminado.
Sólo deben enviarse los documentos a las personas que necesitan su contenido para realizar su trabajo diario.
Las personas que reciben los documentos, deberán disponer de los medios necesarios para tenerlos bien guardados.
Revisar periódicamente los procedimientos de despacho y recepción con el fin de mejorarlos.
Establecer como norma el recoger las mesas de trabajo antes de ausentarse de ella por un período prolongado. Es necesario que la información quede siempre guardada para evitar que sea leida o robada.
Implementar en la medida de lo posible, procedimientos criptográficos para el almacenamiento de la información.
Asegurarse de que los visitantes vayan siempre acompañados por el personal del C.P.D.
Los teléfonos no son seguros.
La fotocopiadora debe estar estrictamente controlada y se utilizará por la persona que trabaja con esa información.
Todas las salidas impresas deberían hacerse en papel color naranja, de esta manera se evita que se realicen fotocopias de esta información.
La destrucción del material confidencial podrá efectuarse mediante fuego controlado o fragmentándolo.
Ejecutar con exactitud el Plan de Backups, y guardar estos bajo un control riguroso y en armarios ignífugos.

NO HAY POR QUE CENTRALIZAR LO QUE NO ES IMPRESCINDIBLE, NI MALGASTAR RECURSOS DE SEGURIDAD EN EL MATERIAL QUE NO ESTE CLASIFICADO; SIN EMBARGO ES NECESARIO CONCIENCIAR A TODO EL PERSONAL, DESDE EL DIRECTOR HASTA EL USUARIO FINAL, DE LA IMPORTANCIA PARA TODOS DE EJECUTAR CON ESCRUPULOSIDAD EL PLAN DE SEGURIDAD.