médicos. Describir cómo se identifican los usuarios (p. ej.: tiene que introducir nombre de usuario) y de autenticación (p. ej.: con contraseña). Describir a qué datos accede cada usuario (perfiles de usuarios). Especificar qué personas pueden conceder, alterar o anular el acceso autorizado sobre los datos y recursos (ficheros, ordenadores, etc.). Indicar qué personas tiene acceso a las copias de seguridad o a copias parciales de los datos (p. ej. para trabajos científicos). Indicar qué personas tiene acceso a los lugares donde están los ordenadores o las copias de los ficheros con datos protegidos.

- Contraseñas: Si se usan contraseñas, describir cómo se asignan (las elige el propio usuario o las asigna el responsable del centro), cómo se hacen llegar al usuario y cómo se garantiza su confidencialidad. Describir con qué periodicidad se cambian las contraseñas.

- Descripción de los ficheros a los que afectan las medidas de seguridad. Es decir, una descripción de la base de datos (nombre del fichero o ficheros, tamaño aproximado, localización en el disco duro, tipo de base de datos, estructura de tablas y campos que contienen.

- Incidencias: Debe aparecer por escrito una relación de medidas a tomar en caso de: averías del ordenador (empresas con las que podemos contactar), borrados accidentales (cómo recuperar ficheros de la papelera de reciclaje), sospecha de accesos no autorizados (registrar fecha y hora de estos sucesos).

- Copias de seguridad: describir cómo se realizan las copias de seguridad, en qué soporte (disquetes, CD. DVD, cintas,...), con qué frecuencia, cuántas copias hay disponibles y dónde están localizadas. Qué pasos hay que seguir cuando sea necesario recuperar los datos almacenados en una copia de seguridad. Realizar un inventario de copias disponibles y de soportes que puedan almacenar, aunque sea temporalmente, datos de salud.

- Fecha de creación y última actualización del documento.

2) Usuarios

Hay que dar a conocer las medidas de seguridad y el mencionado documento a todas las personas que trabajen en el centro médico, según las funciones de cada uno, sin olvidar las consecuencias en que pudiera incurrir en caso de incumplimiento. Las contraseñas deben cambiarse periódicamente, según indique el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Los usuarios sólo deben poder acceder a los datos que precisen para sus funciones. Los médicos pueden acceder a toda la historia clínica, pero si el personal de enfermería o el personal administrativo no precisan acceder a los informes de alta, deben establecerse mecanismos para limitar ese acceso.

Cada vez que un usuario accede o intenta acceder a la base de datos de pacientes, debe quedar un registro de ese acceso o intento de acceso, que debe incluir como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. El período mínimo de conservación de los datos registrados será de dos años.

Tras un determinado número de intentos fallidos de acceso, el sistema debe impedir intentarlo de nuevo.

El responsable de seguridad debe revisar periódicamente la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes. En realidad basta comprobar que sólo han accedido las personas autorizadas a anotar las posibles incidencias.

3) Registro de incidencias

Portada de la página web de la Agencia de Protección de datos
https://www.agpd.es/index.php

Llevar un registro de todas las incidencias relativas a la seguridad del fichero. Podemos escribirlas en un documento Word o una tabla en Excel o una base de datos Access. Debe apuntarse siete aspectos:

a) la persona que hace la anotación,

b) la fecha y hora en que se produce la anomalía,

c) el tipo de incidencia (por ejemplo, se borra accidentalmente una de las copias de seguridad),

d) si hemos contactado con alguna empresa u otra persona paras que nos ayude a solucionar el problema

e) cómo se han recuperado los datos,

f) qué datos se han visto afectados y

g) qué consecuencias ha tenido el episodio.

Es necesaria la autorización por escrito del responsable del fichero para realizar procedimientos de recuperación de los datos.

4) Ficheros temporales

Todo fichero temporal o de pruebas será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación. Por lo tanto si creamos una copia del fichero para hacer pruebas con la base de datos de pacientes, estos ficheros deben ser borrados una vez que terminemos de realizar esas pruebas.

5) Disquetes, discos y otros medios de almacenamiento

Si se guardan datos de pacientes (con identificación de los mismos) en disquetes, CD-ROM, llaveros USB o cualquier otro medio, aunque sea temporalmente, para su transporte, ese soporte de almacenamiento debe cumplir los siguientes requisitos:

- Identificar el tipo de información que contiene (tarea difícil en un llavero USB pues no es fácil que puedan llevar etiquetas adheridas, pero basta con crear una carpeta en su interior con un nombre explícito, por ejemplo: "pacientes con cirrosis").

- Almacenar esos soportes en lugares de acceso restringido.

- Sólo el responsable del fichero puede autorizar la salida de soportes informáticos que contengan datos de carácter personal del local donde está ubicado la base de datos de pacientes.

Debe existir una relación de soportes (disquetes, CD-ROM, etc.) que entran y salen de la consulta. Para ello, se contempla la creación de un registro de los mismos que guarde los siguientes datos: el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción o el destinatario.

Si se desechan esos soportes (disquetes que se tiran a la basura, o llaveros USB que se entregan a otras personas para otros usos), se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él.

Si los discos o unidades que salen de la consulta médica, si contienen datos de salud, deben ir cifrados o tratador por algún mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte