RECOMENDACIÓN SOBRE MEDIDAS DE SEGURIDAD A APLICAR A LOS DATOS DE CARÁCTER PERSONAL RECOGIDOS POR LOS PSICÓLOGOS

Para poder tratar datos de carácter personal en una base de datos adecuándose a la Ley 15/1999, de Protección de Datos de Carácter Personal deberá notificarse el fichero a la Agencia de Protección de Datos y aplicarse las medidas de seguridad que garanticen el nivel de seguridad que les corresponda, así como cumplir con todos los principios de protección de datos. En el caso que nos ocupa al recogerse datos considerados datos especialmente sensibles se deberán aplicar medidas de seguridad de un nivel alto. A continuación se detallan algunas de las medidas de seguridad a aplicar:

Medidas de seguridad ficheros automatizados

Elaborar un Documento de Seguridad

En el que se especificará:

- ✓ Ámbito de aplicación.
- ✓ Medidas, normas, procedimientos reglas y estándares de seguridad.
- ✓ Funciones y obligaciones del personal.
- ✓ Estructura y descripción de ficheros y sistemas de información.
- ✓ Procedimiento de notificación, gestión y respuesta ante incidencias.
- ✓ Procedimiento de realización copias de respaldo y recuperación de datos.
- ✓ Identificación del responsable de seguridad.
- ✓ Control periódico del cumplimiento del documento.
- ✓ Medidas a adoptar en caso de reutilización o desecho de soportes.

Personal contratado

- ✓ Funciones y obligaciones claramente definidas y documentadas.
- ✓ Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.

Incidencias

- ✓ Registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados.
- ✓ Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente.
- ✓ Autorización por escrito del responsable del fichero para su recuperación.

Identificación y autenticación

- ✓ Relación actualizada de usuarios y accesos autorizados.
- ✓ Procedimientos de identificación y autenticación.
- ✓ Criterios de accesos.
- ✓ Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian.
- ✓ Almacenamiento ininteligible de contraseñas activas.
- ✓ Se establecerá los mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado.
- ✓ Límite de intentos reiterados de acceso no autorizado.

Control de acceso

- ✓ Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones.
- ✓ Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.
- ✓ Concesión de permisos de acceso sólo por personal autorizado.
- ✓ Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.

Gestión de soportes (CD, *pen drive*, disquete, programas, etc.)

- ✓ Identificar el tipo de información que contienen.
- ✓ Inventario.
- ✓ Almacenamiento con acceso restringido.
- ✓ Salida de soportes autorizada por el responsable del fichero.
- ✓ Registro de entrada y salida de soportes.
- ✓ Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado.
- ✓ Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento.
- ✓ Cifrado de datos en la distribución de soportes. El cifrado consiste en transformar un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que desconocen la clave.

Copias de respaldo

- ✓ Verificar la definición y aplicación de los procedimientos de copias y recuperación.
- ✓ Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción.
- ✓ Copia de respaldo al menos y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.

Establecer un responsable de seguridad

- ✓ Uno o varios nombrados por el responsable del fichero.
- ✓ Encargado de coordinar y controlar las medidas del documento.
- ✓ No supone delegación de responsabilidad del responsable del fichero.

Pruebas con datos reales

- ✓ Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado.

Auditoría

- ✓ Cada dos año, interna o externa.
- ✓ Adecuación de las medidas y controles.
- ✓ Deficiencias y propuestas correctoras.
- ✓ Análisis del responsable de seguridad y conclusiones al responsable del fichero.
- ✓ Adopción de las medidas correctoras adecuadas.

Registro de accesos

- ✓ Registrar usuario, hora, fichero, tipo acceso y registro accedido.
- ✓ Control del responsable de seguridad. Informe mensual.
- ✓ Conservación 2 años.

Telecomunicaciones

- ✓ Transmisión de datos cifrada.

Medidas técnicas a aplicar en ordenadores

- ✓ Las medidas a aplicar a los ordenadores que se utilicen deberán ser las siguientes:
- ✓ Procedimientos de identificación y autenticación.
- ✓ Mecanismos que eviten el acceso a datos o recursos con derechos distintos a los autorizados.
- ✓ Procedimientos para realizar copias de seguridad.

- ✓ Establecer limites de intentos reiterados de acceso no autorizados.
- ✓ Cifrado de datos en la distribución de soportes o transmisión de datos.
- ✓ Registrar usuario, hora, fichero, tipo de acceso y registro accedido en ficheros de nivel alto.

Otras medidas de seguridad

Cualquier persona que intervenga en el tratamiento de los datos de carácter personal está obligada al secreto profesional respecto de los mismos, incluso aun después de finalizar sus relaciones con el titular del fichero.

Los criterios de archivo deben garantizar la seguridad y correcta conservación, la recuperación de la información y posibilitar el ejercicio de los derechos de los usuarios (derecho a acceder a la información que se tiene sobre él, modificarla si es incorrecta, cancelarla cuando sea posible, etc.)Se recomienda archivar separadamente toda la documentación clínica que forma parte del contenido de la historia clínica, de toda la documentación administrativa.

- ✓ Historia clínica.
- ✓ Documentación administrativa: Hojas de cita previa, hojas admisión, etc.

Anotar las anotaciones subjetivas separadas de la historia clínica,

Control de Acceso físico al archivo Únicamente el personal responsable de la atención psicológica debe tener acceso al archivo. La información estará bajo llave y se deberá indicar en una relación detallada todo el personal con posibilidad de acceso a las historias clínicas.

Romper cualquier papel que contenga datos personales, antes de tirarlo a la papelera

Establecer procedimientos para desechar papel. Cuando se tiene que desechar bastante documentación utilizar máquinas destructoras de papel o empresas que garanticen la seguridad de los datos.

No dejar expedientes en la mesa. Cuando se va a producir una ausencia del puesto de trabajo, guardar el expediente en un cajón o armario bajo llave.

Salir de los ordenadores cuando se produzca una ausencia de tal forma que el sistema nos pida identificarnos cuando se regrese, por ejemplo (establecer en propiedades del fondo de pantalla "proteger con contraseña al reanudar")

No intentar saltar los mecanismos y dispositivos de seguridad que determine la consejería, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos.

No sacar de las instalaciones ninguna documentación, ni soporte (CD, pen drive, disquete, etc.) con datos de carácter personal sin autorización del responsable del fichero o sin anonimizar.

Dirigir a impresoras protegidas los listados que contengan datos de carácter personal que requieran protección y controlar su salida, para evitar su difusión, copia o sustracción.

Cifrado de telecomunicaciones En caso de tener que comunicar algún dato por correo electrónico utilizar algún programa para cifrar los datos, para que sólo las personas con acceso a la clave puedan descifrarlo.

Registrar cualquier incidencia que se pueda producir respecto a los datos de carácter personal.

Cada usuario será responsable de la confidencialidad de su contraseña. Si la contraseña es conocida por otros de manera fortuita o fraudulenta, deberá ser registrado como una incidencia y proceder a cambiarla.

Cumplir la normativa que se determine de cambio de contraseñas, Y a la hora de elegir contraseñas, no utilizar nombre ni apellidos, fechas de nacimiento, número de DNI, etc.

No se deben escribir las contraseñas, a no ser que se haga de tal forma que no exista riesgo de revelación no autorizada.