Guía de buenas prácticas en Protección de Datos Personales en Psicología Clínica y de la Salud

DOCUMENTO PRELIMINAR

Madrid, junio 2011

Colegio Oficial de Psicólogos de Madrid

ÍNDICE:


Colegio Oficial
de Psicólogos
de Madrid

1. INTRODUCCIÓN

El documento presente tiene la finalidad de identificar las buenas prácticas en materia de protección de datos de carácter personal en el ámbito de la intervención profesional en el ámbito de la Psicología Clínica y de la Salud. Pretende ser una guía práctica, y a tal efecto, se presentan las cuestiones específicas a resolver en materia de protección de datos en cada una de las etapas que se contemplan en la intervención psicológica.

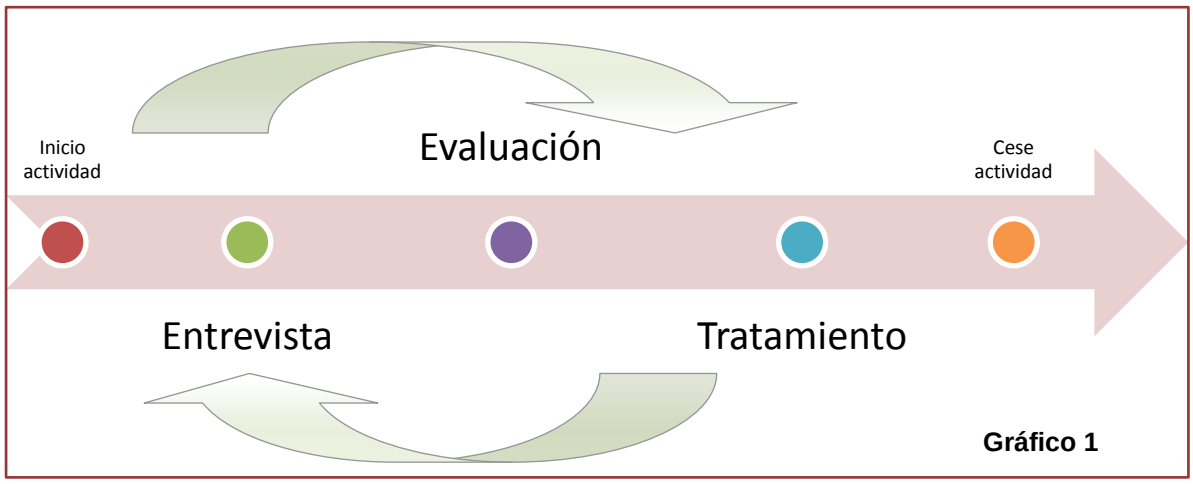


Gráfico 1

El marco normativo específico y los modelos facilitados figuran en los anexos correspondientes con la finalidad de facilitar la comprensión de las cuestiones clave en cada etapa de la intervención.

No obstante será cada profesional el responsable de valorar si lo indicado en la presente guía es adecuado a su caso particular y el responsable de ajustar su tratamiento a la legislación vigente.

1. •**Declarar** el alta del fichero en la Agencia Española de Protección de Datos.
2. •**Recoger, tratar e informar** a los usuarios conforme a la LOPD.
3. •**Elaborar** el documento de seguridad y actualizarlo.
4. •**Auditar** la protección de datos cada dos años.
5. •**Facilitar** el ejercicio de los derechos sobre sus datos.*
6. •**Garantizar** la seguridad del tratamiento.
7. •**Garantizar** estos aspectos ante **terceros.**

(*): Derechos fundamentales (derechos ARCO):

Derecho de acceso: derecho a conocer los datos personales que figuran en el fichero, la finalidad de la recogida, el origen y las cesiones realizadas o previstas. **Derecho de rectificación**: derecho a solicitar modificaciones en los datos personales inexactos o incompletos que figuran en el fichero. **Derecho de cancelación**: es el derecho a solicitar la eliminación de los datos personales que figuran en el fichero. **Derecho de oposición**: es el derecho a oponerse a un tratamiento de los datos personales.

Gráfico 2: Buenas Prácticas

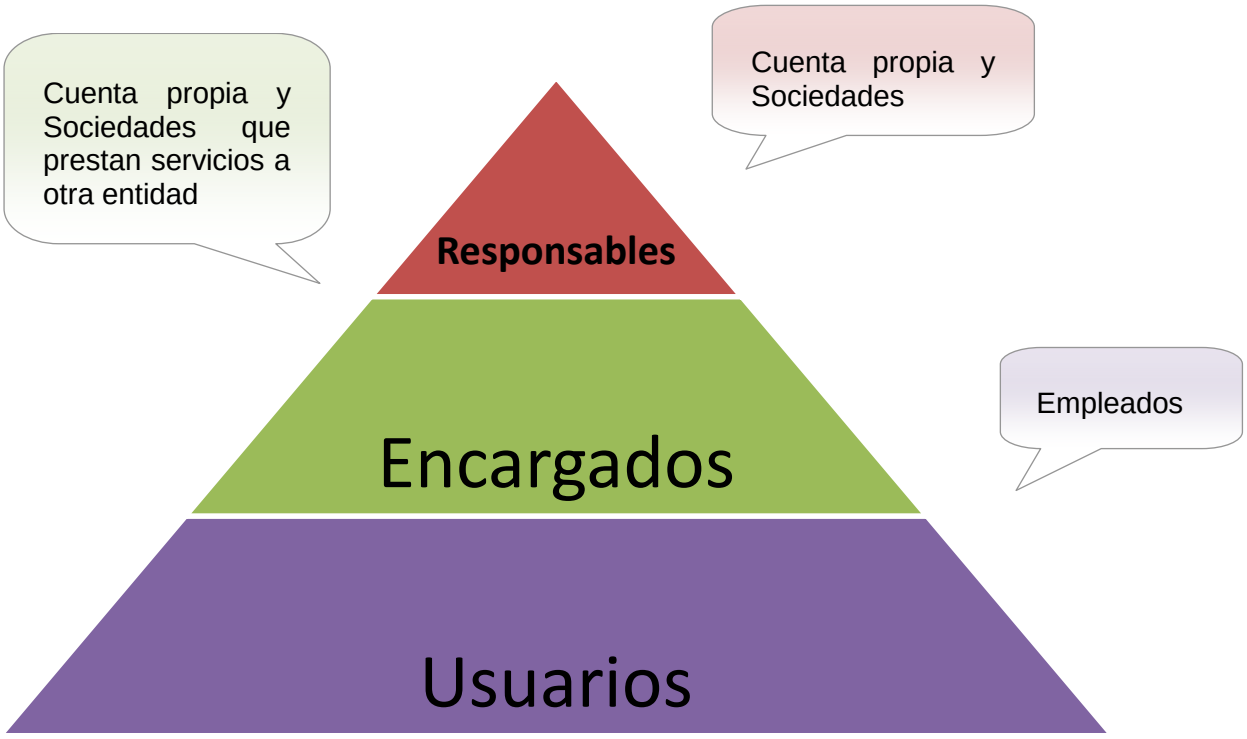
2. FORMAS DE EJERCICIO PROFESIONAL Y RESPONSABILIDAD EN EL TRATAMIENTO DE LOS DATOS

A lo largo del desarrollo de la actividad profesional, las diferentes vías de ejercicio profesional (por cuenta propia, por cuenta ajena, etc.) implican obligaciones diferentes, especialmente en el momento del inicio y del cese de la misma. Por ello, la presente guía se ha estructurado en dos apartados principales, un apartado con las peculiaridades de cada forma de ejercicio y otro con los aspectos comunes (entrevista inicial, evaluación, tratamiento, informes). Se espera así facilitar la lectura y uso de la guía, para que cada profesional pueda obtener la información que necesita conforme a su situación.

Una de las cuestiones fundamentales en materia de protección de datos es delimitar las responsabilidades que se adquieren en el momento que se recogen y utilizan datos de carácter personal, y en el ámbito de las responsabilidades, hay que distinguir la responsabilidad principal, que es la persona, física o jurídica, *responsable del fichero*.

La figura *responsable del fichero* es aquella que decide sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal. Veamos aplicado en nuestro ámbito profesional y según el tipo de ejercicio profesional quién es la persona responsable de los ficheros:

Gráfico 3 Responsabilidad del tratamiento



2.1 Profesionales por cuenta propia

Los profesionales autónomos - despacho propio o alquilado- son las figuras responsables de sus propios ficheros ya que son quienes deciden sobre la finalidad, contenido y el tratamiento de los datos de carácter personal de sus clientes y pacientes. En la misma situación se consideran a los profesionales que comparten la misma ubicación profesional, si bien cada profesional constituye una sociedad económica independiente.

Además, son responsables de los ficheros aquellos profesionales por cuenta propia que atienden a clientes de una compañía determinada sin mantener una relación de dependencia con la misma, como es el caso de ciertos profesionales que atienden a asegurados de una compañía aseguradora sanitaria. Por tanto, son los responsables de las historias clínicas de sus pacientes, y cuando cese su actividad en la compañía deberán llevarse las historias clínicas o formalizar los pasos necesarios para la cesión de los datos a la compañía.

2.2 Sociedad profesional

Cuando varios profesionales forman una sociedad profesional y el cliente/paciente con quién contrata los servicios es con la sociedad en sí, no con uno de los profesionales en concreto. En este caso los ficheros serían responsabilidad de la sociedad.

2.3 Profesional por cuenta ajena y autónomos con contrato de prestación de servicios

En este caso los profesionales tienen un contrato laboral con una empresa/sociedad, tienen por tanto una relación de dependencia, existe una relación laboral con la empresa, que será quién tiene la responsabilidad de los ficheros. Estos profesionales tienen la obligación de realizar un tratamiento de datos según las instrucciones del responsable, y en caso de abandonar la empresa no podrían llevarse las historias clínicas de los pacientes. Debería ser el paciente quién solicitará su historia clínica y la facilitará al profesional en caso de desear seguir el tratamiento con el profesional que abandona la empresa.

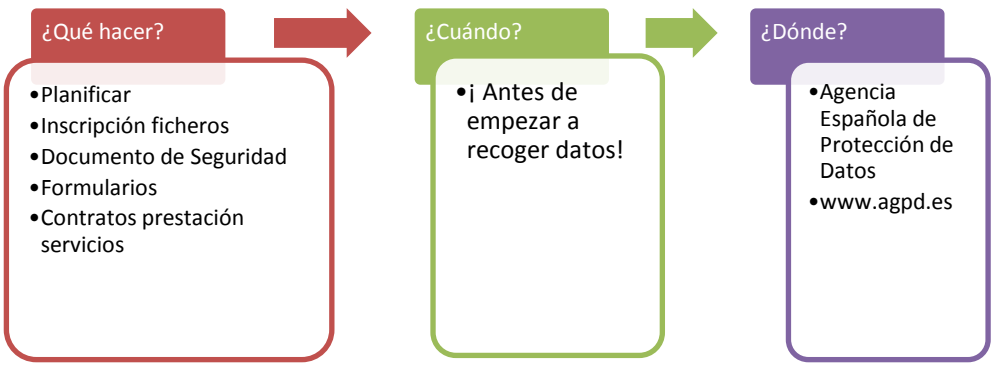
Los profesionales que son autónomos pero trabajan para una empresa con un contrato de prestación de servicios y el responsable del fichero es la empresa que contrata, deben realizar un tratamiento de los datos según las instrucciones del responsable, pero no son los responsables del fichero, son *encargados de tratamiento*.

Este aspecto debe quedar claramente especificado en el contrato de prestación de servicios, junto con un clausulado sobre aspectos a tener en cuenta en el tratamiento de los datos.

3. INICIO Y CESE ACTIVIDAD EN PROFESIONALES AUTÓNOMOS

Gráfico 4 Inicio de actividad

Al iniciarse la actividad como psicólogo, hay algunas cuestiones importantes a tener en



cuenta en materia de protección de datos. Es fundamental conocer las principales obligaciones en relación a la legislación de protección de datos, para ello además de este documento, se puede

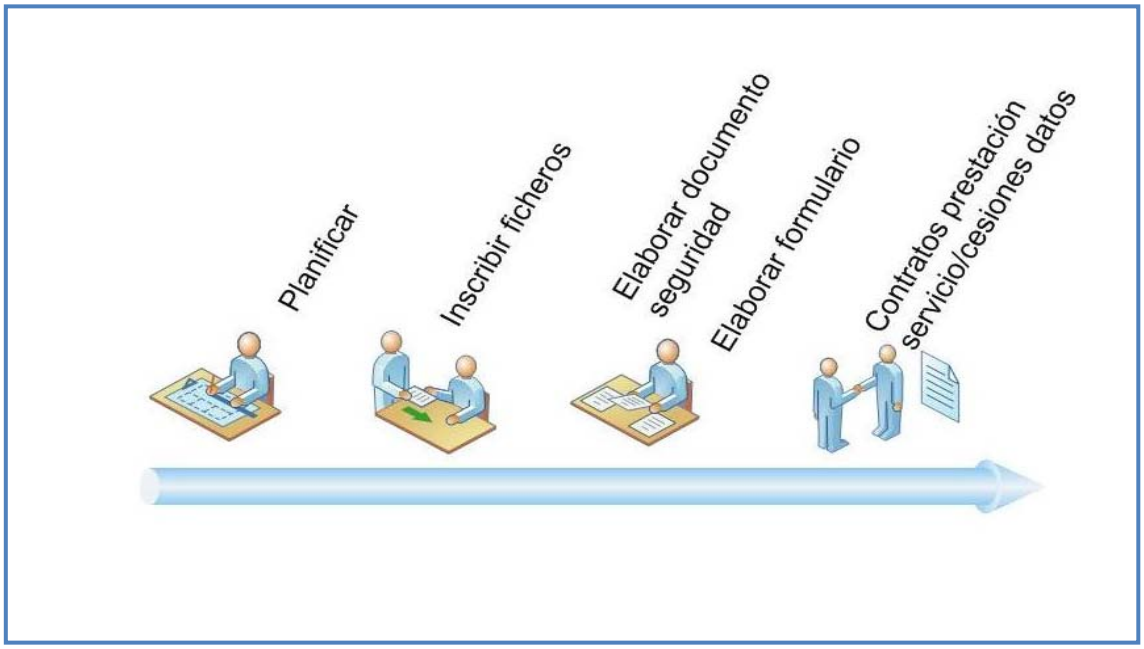
consultar en la página *web* del Colegio http://www.copmadrid.org, más documentación sobre este tema, ya que en la presente guía no se pueden desarrollar todos los aspectos con la amplitud que merecen, también puede consultarse la página de la Agencia Española de Protección de Datos http://www.agpd.es/.

Durante esta fase es necesario planificar como será el tratamiento de datos, determinar si habrá cesiones de datos a terceros, o se contratará alguna empresa para gestionar algún servicio o gestión, para poder declararlas en el momento de la inscripción de ficheros.

Al iniciar la actividad como psicólogo, si es como *profesional autónomo* al igual que se realizan otros trámites de inicio de actividad, como puede ser la inscripción en el Colegio de Psicólogos o la afiliación y/o alta en el Régimen Especial de Trabajadores Autónomos de la Seguridad Social, se debe notificar a la AEPD que se van a recoger datos de carácter personal.

Las cuestiones a resolver en esta etapa para los profesionales autónomos y responsables en las sociedades profesionales son las siguientes:

Gráfico 5 Cuestiones a resolver al iniciar actividad



3.1 Planificación del tratamiento

3.1.1 ¿Qué datos será necesario recoger y que nivel de seguridad tienen?

Sólo se recogerán los datos realmente necesarios. Desde un primer momento se determinará qué información es pertinente, adecuada y no excesiva con respecto a la finalidad con que se efectúa y se elaborará el formulario de recogida de datos teniendo en cuenta los principios de protección de datos. En el anexo 1 se puede consultar los principios de calidad a cumplir de acuerdo a la Ley de Protección de datos.

En el caso de la intervención psicológica se pueden recoger datos como los siguientes:

Gráfico 6 Posibles datos a recoger

La normativa vigente establece tres niveles de seguridad, básico, medio y alto dependiendo de los datos recogidos en cada caso. Los niveles de seguridad se corresponden con las medidas de seguridad a aplicar sobre los datos.

Los datos de carácter personal relativos a la salud, las creencias, la ideología, religión, origen racial, afiliación sindical o vida sexual son datos especialmente protegidos a los que hay que aplicar el conjunto de medidas incluidas en un nivel de seguridad alto, al igual que los datos recabados para fines policiales o relativos a violencia de género.

Los datos de nivel básico, pero que permiten obtener un perfil de las personal son considerados dentro de un nivel de seguridad medio, también lo son los datos sobre infracciones penales o administrativas, de solvencia patrimonial o de crédito, o si son de entidades de la administraciones tributarias, financieras, de la seguridad social, de mutuas de accidentes de trabajo, u operadores de servicio de comunicaciones respecto a datos de tráfico y localización.

En cambio los datos identificativos, (como nombre y apellidos, dirección, DNI, teléfono, correo electrónico, etc.), de características personales (como estado civil, fecha nacimiento, lugar nacimiento, datos de la familia, nacionalidad, sexo, edad, etc.), de circunstancias sociales (como alojamiento/vivienda, aficiones/estilo de vida, etc.) académicos y profesionales (formación/titulaciones) de empleo (categoría/grado, puestos de trabajo) o económicos financieros (nivel socioeconómico) se consideran en un nivel de seguridad básico.

Para cada nivel de seguridad habrá que implantar medidas de seguridad tanto técnicas como organizativas referidas a los siguientes aspectos.

Gráfico 7 Niveles de seguridad

IMPORTANTE:

Es conveniente saber que la acumulación de datos de nivel básico que permitan obtener el perfil de una persona o evaluar aspectos de su personalidad o comportamiento son datos de un NIVEL MEDIO.

De los datos anteriormente mencionados como posibles en una historia clínica[1], sólo deberán incluirse los datos que se consideren **relevantes** y **realmente necesarios** para la finalidad de la historia clínica.

Además de la historia clínica pueden existir los siguientes ficheros: "Nóminas" (Sí se tiene personal contratado), "Contabilidad" (con los datos de proveedores y facturación) o "Agenda". Aquí se han mencionado tan sólo algunos ejemplos, en cada caso se deberá estudiar qué ficheros será preciso crear y que datos deberá contener según los principios de protección de datos.

3.1.2 ¿Quién facilitará los datos?

En esta fase, es necesario determinar cuál será el origen de los datos, se verá si los datos serán facilitados directamente por la persona interesada, entidades privadas, administraciones públicas, fuentes accesibles al público, padres o tutores en el caso de un menor, etc., para indicarlo en el momento de la inscripción del fichero y para solicitar los correspondientes autorizaciones para el tratamiento de los datos. También se deberá indicar la categoría a la que pertenecen las personas que facilitarán los datos, (pacientes, empleados, clientes, representante legal, etc.) y

[1] *En la publicación de la Agencia de Protección de Datos de la Comunidad de Madrid "Protección de datos personales para Servicios Sanitarios Públicos" se trata de manera extensa la problemática de la Historia clínica, analizando los datos a incluir y el nivel de seguridad a aplicar.*

ayudará a determinar las cláusulas de protección de datos que habrá que incluir en convenios y contratos de prestación de servicios o cesiones de datos.

3.1.3 ¿Hay alguna contratación de prestación de servicios que comporte un tratamiento de datos?

Si se prevé que se contratará alguna empresa o profesional para gestionar alguna tarea que implique el tratamiento de datos de carácter personal, habrá que formalizarlo por escrito, incluyendo cláusulas de protección de datos en la que se aclarará el papel de cada parte en el tratamiento de los datos. En el momento de la inscripción del fichero habrá que comunicar las contrataciones de prestación de servicios que se van a realizar.

3.1.4 ¿Alguna empresa nos ha contratado para prestar algún servicio que implique tratamiento de datos?

Si es el profesional el contratado, se deberá incluir de igual manera cláusulas de protección de datos en las que se indique el papel de cada parte en el tratamiento de los datos, si se prestaran los servicios fuera de los locales de la empresa que contrata, el profesional será responsable a su vez de mantener un documento de seguridad.

3.1.5 ¿En qué contratos se deben incluir cláusulas de protección de datos?

Por ejemplo, cuando se contrata una empresa para gestionar la facturación o la tramitación de las nóminas hay que incluir cláusulas de protección de datos, ya que obligatoriamente deberán tratar con datos de carácter personal, (en el apartado siguiente se comentará las cláusulas de protección a incluir), pero también hay casos en los que hay que incluir cláusulas de protección aún no habiendo un tratamiento de los datos, es el caso por ejemplo de las empresas de limpieza, se trata de una prestación de servicios sin acceso a datos personales, pero aún así se deberá recoger en el contrato de prestación de servicios expresamente, la prohibición de acceder a los datos personales y la obligación de secreto de los datos que hubiera podido conocer con motivo de la prestación del servicio.

3.1.6 ¿Qué debe incluir un contrato de prestación de servicios?

En este documento se anexan las cláusulas a incluir en cualquier contrato de prestación de servicios. Deberá hacerse referencia a lo siguiente:

- ✓ Que se tratarán los datos personales únicamente conforme las instrucciones del responsable.
- ✓ Cumplir las normas de seguridad, que de acuerdo a la normativa vigente, el responsable del fichero y el encargado del tratamiento están obligados a implantar.
- ✓ Destruir los datos personales una vez cumplido el objeto del contrato o en su caso devolverlos al responsable, así como cualquier soporte o documento en que conste algún dato de carácter personal.
- ✓ Prohibición de utilizar los datos para una finalidad diferente a la del contrato.
- ✓ Prohibición de comunicar estos datos a terceros, ni siquiera para su conservación.

3.1.7 ¿Se realizarán cesiones de datos a terceros?

También habrá que estudiar si se tienen que ceder datos a terceras personas, y si dicha cesión requiere el consentimiento de dicha persona o no. Como regla general, los datos sólo pueden ser cedidos a terceros con el consentimiento del cedente, no obstante existen algunas excepciones como cuando la recogida de datos está determinada por una ley o está incluida dentro de las excepciones indicadas en la LOPD, para más información sobre este aspecto se puede consultar el art. 11 e la LOPD. (Es importante recordar que aún no necesitándose consentimiento si deberá informarse de la cesión).

Deberá indicarse en el momento de la inscripción las cesiones de datos que se prevea se van a producir. En el formulario de recogida de los datos deberá incluirse información sobre la cesión de datos y solicitar el consentimiento en los casos que corresponda.

3.2 Inscripción del fichero

Un fichero es un conjunto organizado de datos de carácter personal que hay que declarar oficialmente ante la administración pública competente (AEPD).

Pueden crearse ficheros que contengan datos de carácter personal cuando resulte necesario para el logro de una actividad legítima de la empresa y se respeten las garantías que establece la Ley. Se debe notificar el fichero a la AEPD antes de la recogida de los datos. Se refiere tanto a ficheros integrados en sistemas informáticos, como a ficheros manuales que puedan estar archivados en armarios, cajones o estanterías, siempre que los datos se encuentren estructurados (organizados), por algún criterio que permita acceder con facilidad a los datos de una persona. No se trata de comunicar a la AEPD los datos, sino de informar del tipo de datos que se manejan, por ejemplo “nombre”, “dirección postal”, “dirección correo electrónico” de los pacientes atendidos en consulta. La declaración de un fichero incluye los siguientes aspectos:

- ✓ La forma de recogida de la información.
- ✓ La fuente de los datos.
- ✓ El tipo de datos (nombre y apellidos, domicilio, datos profesionales, académicos, etc.)
- ✓ El nivel de las medidas de seguridad a aplicar.
- ✓ Las posibles cesiones para su tratamiento.
- ✓ Sistema de tratamiento de los datos (automatizado, no automatizado, mixto).

Se trata de detallar las características del fichero y del tratamiento de los datos **antes** de la recogida de datos.

3.2.1 ¿Cómo se realiza la notificación de los ficheros?

El trámite se realiza a través de la página *web* de la AEPD www.agpd.es y es completamente gratuito.

Hay que rellenar un formulario desde la web de la AEPD. Para ello basta con seguir los pasos indicados en el manual de la Agencia o bien acceder al asistente –una aplicación que guía la introducción de datos- en el apartado *RESPONSABLE DEL FICHERO*, en la opción *Obtención del formulario NOTA.*

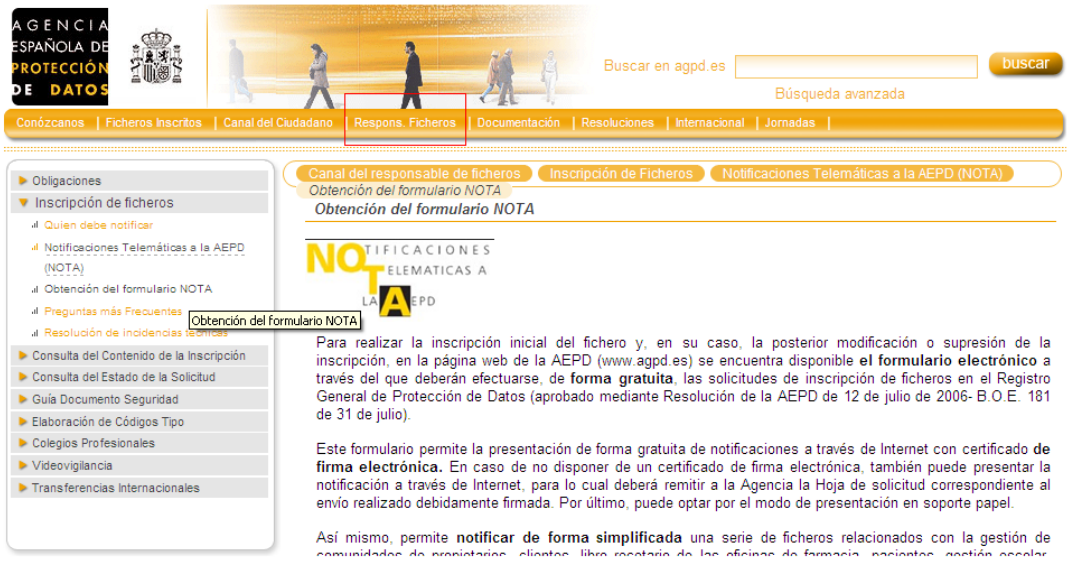
Gráfico 8

Manual del formulario electrónico de notificación de ficheros de titularidad privada

Pasos para la cumplimentación del formulario

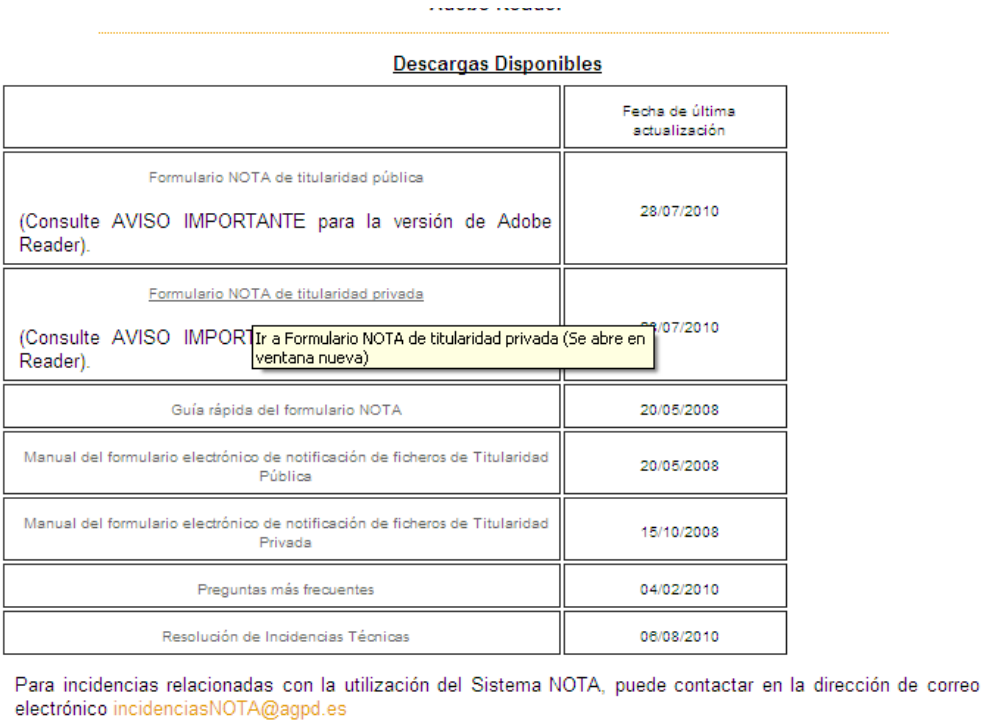
1. Responder a las preguntas iniciales del asistente dependiendo del tipo de solicitud y forma de presentación elegido.
2. Cumplimentar los apartados de la notificación. Se recomienda guardar la notificación antes de pasar a la siguiente fase de cumplimentación, ya que una vez que se haya optado por cumplimentar la Hoja de solicitud no se podrán realizar nuevos cambios en la notificación.
3. Cumplimentar la Hoja de solicitud.
4. Generar/Enviar la notificación: En el caso de presentación a través de Internet con certificado de firma electrónica, deberá antes **Finalizar** y **Firmar** la notificación con su certificado de firma electrónica reconocido. En el caso de presentación en formulario en papel, deberá pulsar el botón «*Finalizar formulario*» que se encuentra al final de la *Hoja de solicitud* generándose el código de barras bidimensional PDF 417 (nube de puntos), así como el correspondiente código de envío que establece la correspondencia entre el contenido que figura en cada una de las páginas que componen el modelo de notificación y la nube de puntos generada.
5. En las presentaciones a través de Internet, deberá recibir el acuse de recibo de la AEPD del envío realizado. La no recepción del mensaje de confirmación, o en su caso, la recepción de un mensaje de indicación de error implica que no se ha producido la recepción del mismo, debiendo realizarse la presentación en otro momento o utilizando otros medios.
6. Enviar la *Hoja de solicitud* firmada a la AEPD. En el caso de presentación a través de Internet con certificado de firma electrónica no será necesario remitir la Hoja de solicitud. En el caso de presentación en formulario en papel, se presentará la *Hoja de solicitud* con el código bidimensional correctamente impreso, así como las dos páginas con el contenido de la notificación en las que deberá figurar el código de envío generado por el formulario electrónico.

Gráfico 9



En la parte inferior de la hoja se puede acceder al *FORMULARIO NOTA DE TITULARIDAD PRIVADA,* y al seleccionarlo se mostrará un formulario en formato Adobe Reader, que habrá que ir cumplimentando.

Gráfico 10



Descargas Disponibles

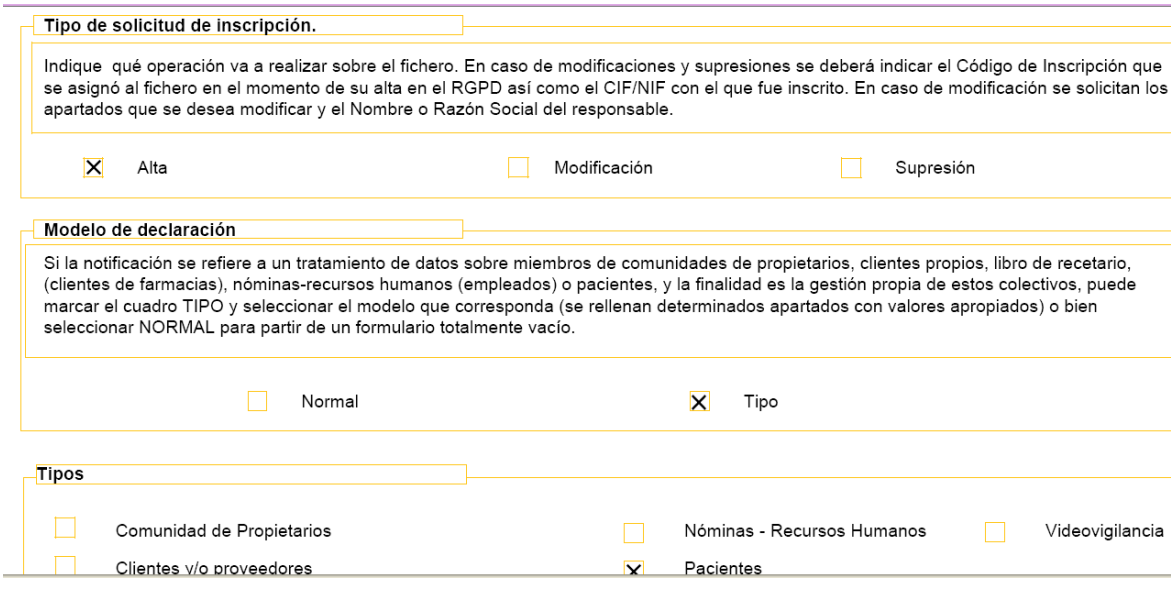
	Fecha de última actualización
Formulario NOTA de titularidad pública (Consulte AVISO IMPORTANTE para la versión de Adobe Reader).	28/07/2010
Formulario NOTA de titularidad privada (Consulte AVISO IMPORT… Reader).	…/07/2010
Guía rápida del formulario NOTA	20/05/2008
Manual del formulario electrónico de notificación de ficheros de Titularidad Pública	20/05/2008
Manual del formulario electrónico de notificación de ficheros de Titularidad Privada	15/10/2008
Preguntas más frecuentes	04/02/2010
Resolución de Incidencias Técnicas	06/08/2010

Ir a Formulario NOTA de titularidad privada (Se abre en ventana nueva)

Para incidencias relacionadas con la utilización del Sistema NOTA, puede contactar en la dirección de correo electrónico incidenciasNOTA@agpd.es

Según se vayan rellenando casillas se irán desplegando más aparatados con casillas a cumplimentar. Para el caso de la historia clínica, se puede escoger el modelo de declaración TIPO, y seleccionar el formulario pre-cumplimentado PACIENTES, que adaptándolo a la actividad propia de un psicólogo y el caso particular de cada profesional puede facilitar el proceso de notificación del fichero.

Gráfico 11



Tipo de solicitud de inscripción.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de Inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

☒ Alta ☐ Modificación ☐ Supresión

Modelo de declaración

Si la notificación se refiere a un tratamiento de datos sobre miembros de comunidades de propietarios, clientes propios, libro de recetario, (clientes de farmacias), nóminas-recursos humanos (empleados) o pacientes, y la finalidad es la gestión propia de estos colectivos, puede marcar el cuadro TIPO y seleccionar el modelo que corresponda (se rellenan determinados apartados con valores apropiados) o bien seleccionar NORMAL para partir de un formulario totalmente vacío.

☐ Normal ☒ Tipo

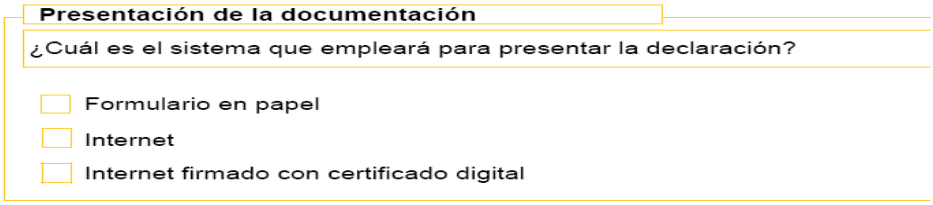
Tipos

☐ Comunidad de Propietarios ☐ Nóminas - Recursos Humanos ☐ Videovigilancia

☐ Clientes y/o proveedores ☒ Pacientes

La aplicación ofrece tres formas de enviar la notificación:

Gráfico 12



Al finalizar de cumplimentar el formulario según la opción que hayamos escogido en el inicio, habrá que enviar la declaración a la AEPD en una de estas tres vías:

- ✓ Formulario papel.-
  Si se ha escogido está opción, una vez se termine de cumplimentar el formulario se deberá imprimir la notificación (en la que aparecerá un código de barras, firmar la hoja de solicitud y enviar a la AEPD C/Jorge Juan, 6 28001-Madrid.
- ✓ Internet.-
  Si se ha escogido está opción, una vez cumplimentada la notificación, se enviará la notificación pulsando el botón Generar/enviar en la hoja de solicitud. En ese momento el sistema le enviará la hoja de solicitud que confirma que la notificación ha sido enviada correctamente. El siguiente paso es firmar la hoja de solicitud y enviarla a la AEPD, bien por correo postal o por fax.
- ✓ Internet con certificado digital.-
  Si se dispone de certificado digital, una vez cumplimentada la notificación y la hoja de solicitud, se finalizará formulario y se firmará electrónicamente siguiendo las instrucciones de la aplicación.

3.3 Otros aspectos a Planificar del tratamiento de los datos

3.3.1 ¿Qué se debe incluir en el formulario de solicitud de datos?

Como responsable de fichero se debe informar sobre los siguientes aspectos:

- ✓ Nombre del fichero.
- ✓ Responsable del fichero.
- ✓ Finalidad de la recogida de los datos.
- ✓ Posibles cesiones.
- ✓ Información relativa a la forma de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- ✓ Se debe aclarar qué información será imprescindible ofrecer para continuar el proceso y cuál será opcional. La persona debe conocer en todo momento qué consecuencias tendrá la información que facilita.

Al ser el responsable del fichero el que debe probar que ha cumplido con el deber información, es necesario conservar el soporte que acredite su cumplimiento durante el tiempo que persista el tratamiento de los datos. En el anexo se puede encontrar un texto modelo a incluir en el formulario de recogida de los datos.

3.3.2 ¿Se pueden solicitar datos de carácter personal por correo electrónico o internet?

Cuando se solicitan datos por internet o correo electrónico hay que respetar los mismos principios de protección de datos que en formato papel, teniendo en cuenta que al implicar datos de un nivel de seguridad alto (datos de salud), la información deberá transmitirse encriptada. Se deberán informar de los mismos aspectos que cuando se recogen en papel, una buena práctica es diseñar el formulario de recogida de datos de tal forma que aparezca un mensaje con la información sobre protección de datos al entrar en la aplicación, para propiciar la lectura de la información de forma ineludible, dentro del flujo de acciones que debe ejecutar el usuario para expresar la aceptación definitiva de la transmisión. Deberá quedar huella del consentimiento, así como de las modificaciones realizadas por el usuario.

3.3.3 ¿Qué personas accederán a los datos y que nivel de acceso tendrán?

Esta fase es el momento adecuado para decidir qué personas necesitarán acceder a los datos y el nivel de acceso que tendrá. Por ejemplo el profesional que realiza la intervención psicológica necesitará acceder a la historia clínica entera, pero el personal administrativo sólo necesitará acceder a los datos administrativos. Es el momento de determinar los permisos de cada persona para posteriormente incluirlos en el documento de seguridad, manteniéndolo en todo momento actualizado. Como regla general cada persona deberá acceder tan sólo a los datos que necesite para la finalidad del tratamiento de los datos, siempre teniendo en cuenta los principios de protección de datos.

3.3.4 ¿Qué otros aspectos se deben planificar?

Cualquier aspecto del tratamiento de los datos hay que planificarlo en este momento, para tenerlo en cuenta desde el principio y elaborar el documento de seguridad teniendo en cuenta los aspectos planteados.

Por razones de claridad de exposición muchos de estos aspectos se desarrollan en otros apartados pero se deberán tener en cuenta desde el principio.

3.4 Implantación de medidas de seguridad y elaboración del documento de seguridad

El Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999, regula, el conjunto de medidas de índole técnica y organizativa que se deben cumplir en un tratamiento de datos para garantizar la seguridad y confidencialidad de los datos. Al iniciar la actividad, se deberán determinar las medidas de seguridad que habrá que implantar según el nivel de seguridad del fichero, tanto manual como automatizado. En el caso de la historia clínica se trata con datos de un nivel de seguridad alto, y por tanto habrá que aplicar las medidas de dicho nivel.

3.4.1 ¿Qué es el documento de seguridad?

Se debe elaborar un documento de seguridad en el que se recopilan las normas de seguridad que se van a implantar, es un documento interno, (no hay que presentarlo en la AEPD), que se debe mantener permanentemente actualizado y ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, o en el contenido de la información y adecuarse a las normativas vigentes en materia de seguridad de los datos de carácter personal. El documento de seguridad estará a disposición de la Agencia de Protección de Datos.

Las normativas indicadas en el documento serán de obligado cumplimiento para el personal con acceso a los sistemas de información.

3.4.2 ¿Cómo se elabora y qué incluye un documento de seguridad?

El documento de seguridad puede ser único y comprensivo de todos los ficheros o tratamientos o individualizado para cada fichero o tratamiento.

La AEPD pone a disposición de los responsables de ficheros una *Guía modelo de documento de seguridad* muy útil para elaborar el documento de seguridad propio, bastará con adaptar a las circunstancias particulares de cada uno, lo indicado en el modelo que ofrece la Agencia.

El Documento de Seguridad tendrá los siguientes contenidos:

1. Ámbito de aplicación, detallando los recursos protegidos.
2. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el Reglamento.
3. Funciones y obligaciones del personal en relación al tratamiento de los datos de carácter personal incluidos en los ficheros.
4. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que lo tratan.
5. Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
6. Las medidas que sean necesario adoptar para el transporte de soportes y documentos, así como para su destrucción.
7. En el caso de niveles medio y alto también se incluirá:
    a. La identificación del responsable/es de seguridad.
    b. Los controles periódicos que se realizarán para verificar el cumplimiento de lo dispuesto en el documento.

3.4.3 ¿Cómo se conservarán los datos y qué medias de seguridad se necesitarán?

Se deben conservar los datos de tal forma que los pacientes/clientes puedan ejercer su derecho de acceso, rectificación y cancelación de datos personales propios. Para ello la información tiene que estar almacenada de tal forma que se pueda facilitar el ejercicio de dichos derechos, es decir de forma organizada, estructurada por algún criterio específico (alfabético, por número expediente, etc.).

Dependiendo del nivel de seguridad del fichero se deben aplicar diferentes medidas de seguridad, a continuación se exponen las diferentes medidas de seguridad a aplicar, diferenciando por el sistema de tratamiento utilizado para almacenar los datos.

Si se almacenan los datos tanto en un formato no automatizado como automatizado, a la hora de notificar el fichero se hará como MIXTO y se deberán cumplir ambos tipos de medidas de seguridad.

Se deberán aplicar medidas de seguridad en función del tipo de fichero – no automatizado y automatizado - y del nivel de seguridad que requieran los datos. A continuación resumimos las medidas a aplicar: Tabla 1.

MEDIDAS	FICHERO NO AUT.	FICHERO AUT.
1. Documento de seguridad (cualquier nivel de seguridad)	Si	Si
2. Responsable de seguridad	Si (medio y alto)	Si (medio y alto)
3. Funciones y obligaciones del personal (cualquier nivel de seguridad)	Si	Si
4. Registro de incidencias (cualquier nivel de seguridad)	Si	Si
5. Control de acceso	Si	Si
6. Registro de acceso lógico/registro acceso documentación	Sí (alto)	Si (alto)
7. Identificación y autenticación (cualquier nivel de seguridad)	No	Si
8. Criterios de archivo (cualquier nivel de seguridad)	Si	No
9. Control acceso físico/almacenamiento información	Si (alto)	Sí (medio y alto)
10. Copias de respaldo y recuperación (cualquier nivel de seguridad)	No	Si
11. Dispositivos de almacenamiento (cualquier nivel de seguridad)	Si	No
12. Custodia de soportes (cualquier nivel de seguridad)	Si	No
13. Gestión de soportes y documentación (cualquier nivel de seguridad)	Si	Si
14. Auditoría periódica (nivel medio y alto)	Si	Si
15. Copia o reproducción (nivel alto)	Si (nivel alto)	No
16. Distribución de soportes/traslado documentación (nivel alto)	Sí (nivel alto)	Si (nivel alto)
17. Telecomunicación (nivel alto)	No	Si (alto)

A continuación definimos muy brevemente cada medida:

Documento de Seguridad.- Son contenidos obligatorios para cada tipo de fichero (automatizado o manual) y nivel de seguridad del fichero. En los niveles medio y alto se deberá identificar también el responsable de seguridad y controlar periódicamente el cumplimiento del documento.

Funciones y obligaciones del personal.- Deben estar claramente definidas y documentadas. Se incluye La formación al personal sobre normas, procedimientos y consecuencias de no cumplirlas.

Responsable seguridad.-En el caso de ficheros de nivel medio o alto se designará uno o varios responsables de seguridad. Es el encargado de coordinar y contralar las medidas de seguridad del documento. No supone delegación de responsabilidad.

Incidencias.- Deberá existir:

- ✓ Un procedimiento de notificación y gestión de incidencias que afecten a datos personales.
- ✓ Un registro en el que se haga constar: tipo incidencia, momento incidencia, personal que lo detecta, persona que lo comunica. Además, en los ficheros con niveles medio o alto deberá consignarse:
  - o procedimientos realizados de recuperación de los datos
  - o personas que ejecutaron el proceso
  - o los datos restaurados
  - o y si ha sido un grabado manual.

Gestión y distribución de soportes y documentos.- Deberán permitir identificar el tipo de información que contienen, ser inventariados y ser accesibles por el personal autorizado en el documento de seguridad. Los soportes con datos de carácter personal considerados sensibles (nivel alto) se identificarán de forma comprensible sólo para los usuarios con acceso autorizado. Además,

- ✓ La salida de soportes y documentos (incluidos los adjuntos de los correos electrónicos), deberá ser autorizados por el responsable del fichero, o encontrarse la persona que lo realiza debidamente autorizado en el documento de seguridad.
- ✓ En el caso de ficheros de nivel medio y alto se establecerá un registro de entrada y salida de soportes que permita conocer:
  - o el tipo de documento o soporte.
  - o la fecha y hora.
  - o el emisor.
  - o el tipo de información que contienen.
  - o la forma de envío.
  - o y la persona responsable de la recepción.
- ✓ La distribución de soportes de datos de un nivel alto, se realizará cifrando los datos, utilizando otro mecanismo que garantice que la información no será accesible ni manipulada durante el transporte, también se cifrarán los datos que contengan dispositivos portátiles cuando estén fuera de las instalaciones del responsable del fichero.
- ✓ En los traslados de la documentación se adoptaran las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido.
- ✓ En la eliminación de cualquier documento o soporte, deberá realizarse evitando el acceso a la misma o su recuperación posterior.

Copias respaldo.- Se establecerán procedimientos de:

- ✓ copias de seguridad (mínimo semanal, excepto que no se hubieran producido cambios). La generación de copias o la reproducción de los documentos sólo podrá ser realizada por personal autorizado en el documento de seguridad, si son de nivel alto. En el caso de de ficheros de un nivel alto, la copia, junto con los procedimientos de recuperación se guardarán en un lugar diferente al que se encuentren los sistemas informáticos. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
- ✓ recuperación de los datos, que garanticen en todo momento su reconstrucción en el estado que se encontraban antes de la pérdida o destrucción.
- ✓ Se verificará al menos cada 6 meses la correcta definición, funcionamiento y aplicación de los procedimientos. Las pruebas anteriores a la implantación o modificación de los sistemas no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Auditoría.- A partir del nivel medio, se someterá a los datos, sistemas e instalaciones implicados a una auditoría interna o externa para verificar todas las medidas de seguridad. La auditoría deberá realizarse cada vez que se produzcan modificaciones sustanciales del sistema de información y como mínimo cada dos años. El informe quedará a disposición de la Agencia de Protección de Datos.

- ✓ El informe deberá dictaminar sobre las medidas de seguridad y controles, identificando deficiencias y proponer medidas correctoras o complementarias necesarias. Se puede encontrar información sobre cómo realizar una auditoría en el modelo de documento de seguridad que la AEPD pone a disposición de los interesados (www.aepd.es).

A continuación presentamos brevemente las definiciones de las medidas de seguridad específicas de los **ficheros automatizados** (ficheros informáticos):

Control acceso lógico.- El personal accederá exclusivamente a los recursos necesarios para el desarrollo de sus funciones. Se mantendrá una relación actualizada de usuarios, permisos y accesos autorizados. Asimismo, se indicarán y desarrollarán los mecanismos que impidan el acceso a personas no autorizadas.

Registro de accesos.- En el caso de ficheros de nivel alto – como ocurre con la historia clínica- se registrará:

- o Usuario.
- o fecha y hora.
- o fichero accedido.
- o tipo de acceso.
- o y si ha sido autorizado o denegado.

El responsable de seguridad deberá controlar el registro de accesos y revisarlo mensualmente.

Es interesante saber que si el responsable del fichero es una persona física y puede garantizar que será la única persona que accederá y tratará los datos, (documentándolo en el documento de seguridad), en ese caso no será necesario el registro de accesos.

Identificación y autenticación.- Las medidas deben garantizar la correcta identificación y inequívoca y personalizada –*autenticación*- de los usuarios. El documento de seguridad se establecerá una periodicidad para cambiar las contraseñas, no superior a un año. Además, en ficheros con nivel alto se debe limitar el número de intentos reiterados de acceso no autorizado.

Control acceso físico.- Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a las instalaciones con los equipos de los sistemas de información.

Telecomunicaciones.- El acceso a través de redes deberá garantizar un nivel de seguridad equivalente al acceso en modo local, en el caso de transmisión de datos de carácter personal de un nivel alto a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Por último, presentamos brevemente las definiciones de las medidas de seguridad específicas de los **ficheros no automatizados,** (ficheros NO informáticos, por ejemplo en formato papel, organizados en carpetas:

Criterios de archivo.- Las medidas deben garantizar la correcta conservación, localización de los documentos y el ejercicio de los derechos ARCO). Como pauta debe aplicarse el criterio previsto en su legislación correspondiente – por ejemplo, en la historia clínica, la Ley 41/2002. En ausencia de una legislación específica, debe aplicarse el criterio establecido en el Documento de seguridad.

Acceso a la documentación.- El acceso a la documentación de los ficheros de un nivel de seguridad alto deberá ser registrada y se deberán establecer procedimientos a tal efecto, incluso para identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios - por ejemplo, mediante plantillas básicas incorporadas al inicio del expediente.

Dispositivos de almacenamiento y custodia de soportes.- Los dispositivos deberán disponer de mecanismo que obstaculicen su apertura. Cuando la información no se encuentra en los dispositivos correspondientes (por estar en revisión o tramitación), la persona al cargo deberá custodiarla e impedir en todo momento que pueda ser accedida por personas no autorizadas.

Almacenamiento de la información.- En caso de ficheros de un nivel alto, los armarios, archivadores u otros elementos en los que se almacenan los ficheros no automatizados con datos de carácter personal, deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Estás áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos. De no poder cumplirse deberán implantarse medidas alternativas, motivándolo en el documento de seguridad.

3.4.4 ¿Qué medidas técnicas se han de aplicar a los ordenadores?

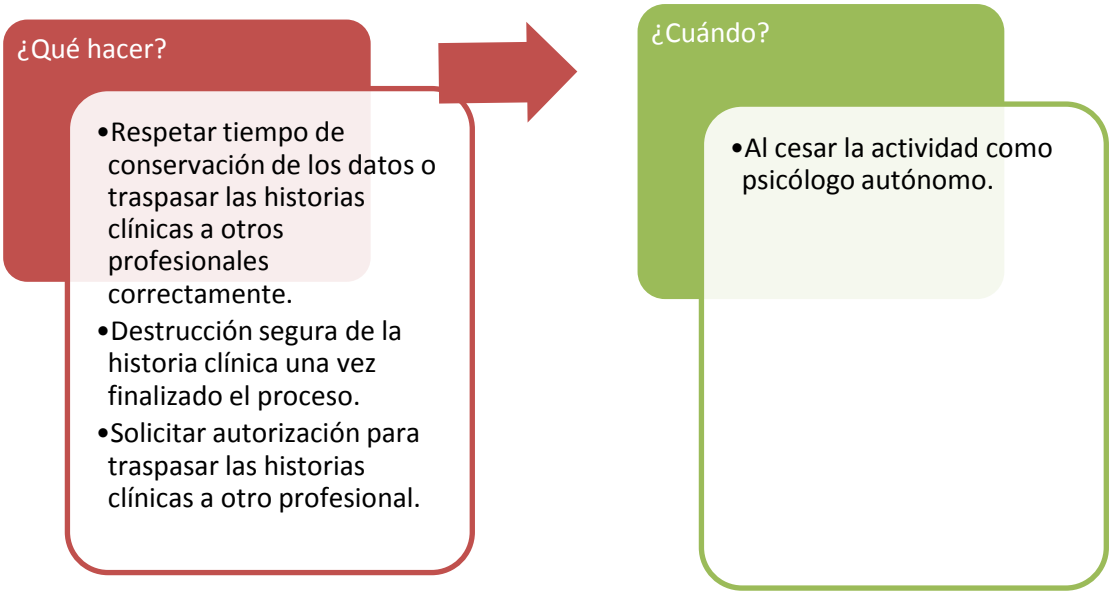
Las medidas a aplicar a los ordenadores que se utilicen deberán ser las siguientes:

- ✓ 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 límites de intentos reiterados de acceso no autorizados.
- ✓ Cifrado de datos en la distribución de soportes o transmisión de datos de nivel alto.

- ✓ Registrar usuario, hora, fichero, tipo de acceso y registro accedido en ficheros de nivel alto.
- ✓ Asegurarse que el software destinado a tratar con los datos de carácter personal describan en su descripción técnica el nivel de seguridad que permitan alcanzar (básico, medio o alto) Para la historia clínica se requiere que pueda alcanzar un nivel alto.

Recordamos que la Agencia Española de protección de datos facilita un modelo de documento de seguridad editable, que facilita en gran medida, la implantación de parte de las medidas de seguridad mencionadas.

Gráfico 13 Cese de actividad



3.4.5 ¿Cuándo tiempo hay que conservar los datos si se cesa en el ejercicio profesional?

La ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica es la regulación específica sobre la historia clínica.

Gráfico 14

Dicha ley determina que se deberá conservar la historia clínica por un periodo de al menos 5 años contados a partir de la fecha de alta del último proceso asistencial, también hay que recordar que podrá conservarse la documentación durante más tiempo a efectos judiciales, si el profesional valora que puede ser conveniente, por las características de un caso en concreto, por preverse una reclamación civil como consecuencia de una acción profesional o porque lo pudiera solicitar un juez, el plazo general de prescripción de las acciones que se pudieran entablar por el usuario contra el profesional es de 15 años. En todo caso, si el historial hubiera sido destruido por haber transcurrido más de cinco años, no se incumplirá la Ley.

Es recomendable facilitar al paciente una copia de su historia clínica al finalizar el tratamiento.

3.4.6 ¿Se deben conservar los datos tras el fallecimiento del profesional?

Los sucesores tienen la obligación de conservar los datos en condiciones que garanticen el nivel de seguridad del fichero, al menos durante el tiempo que establece la ley. Otra opción puede ser que otro profesional se hiciera cargo, siempre informando y solicitando permiso a los usuarios.

3.4.7 ¿Cómo se pueden destruir los datos, una vez finalizado el periodo de custodia?

Hay que destruir los documentos o soportes que contengan datos de carácter personal de tal forma que se impida el acceso a la información contenida en el mismo o su recuperación posterior. Se pueden emplear máquinas destructoras de documentos o encargar la gestión a empresas especializadas que certifiquen que la destrucción será realizada mediante procedimientos que garanticen el cumplimiento de la LOPD.

4. INICIO Y CESE DE ACTIVIDAD DE PROFESIONALES POR CUENTA AJENA Y AUTÓNOMOS CON CONTRATO DE PRESTACIÓN DE SERVICIOS

En ambos casos el responsable del fichero es la persona que contrata, pero si existe para el profesional, la obligación de realizar un tratamiento de los datos según los principios de protección de datos y cumplir con las normativas y procedimientos que indique el responsable del fichero.

4.1 Profesional por cuenta ajena

La firma del contrato es el momento de solicitar información sobre todos los aspectos en materia de protección de datos, se deberá solicitar al responsable del fichero, para tener claro la actuación en cada momento, evitando dudas e improvisaciones, puede ser que el responsable solicite que se firme un compromiso de confidencialidad sobre los datos.

Gráfico 15: inicio de la actividad por cuenta ajena.

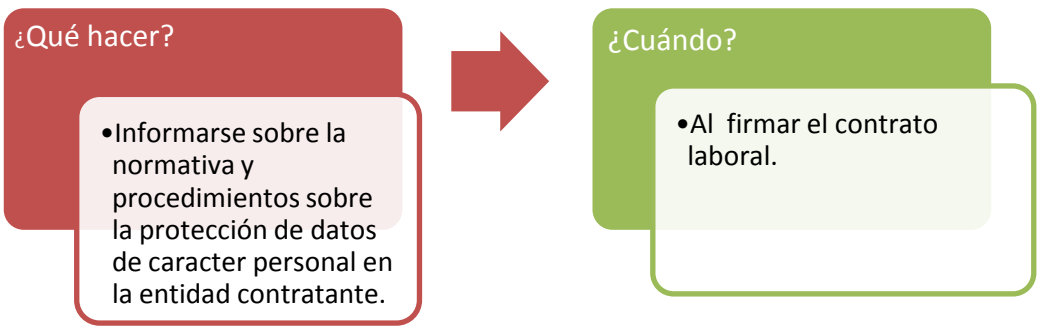
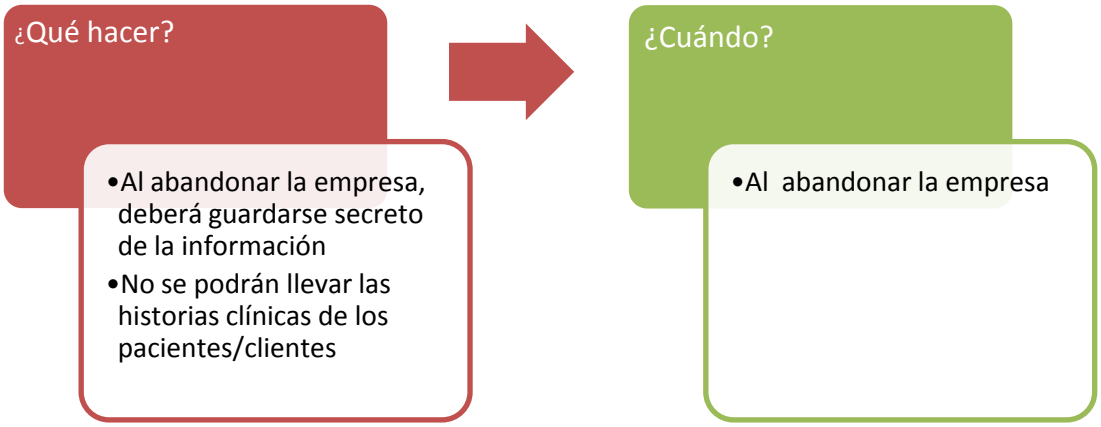


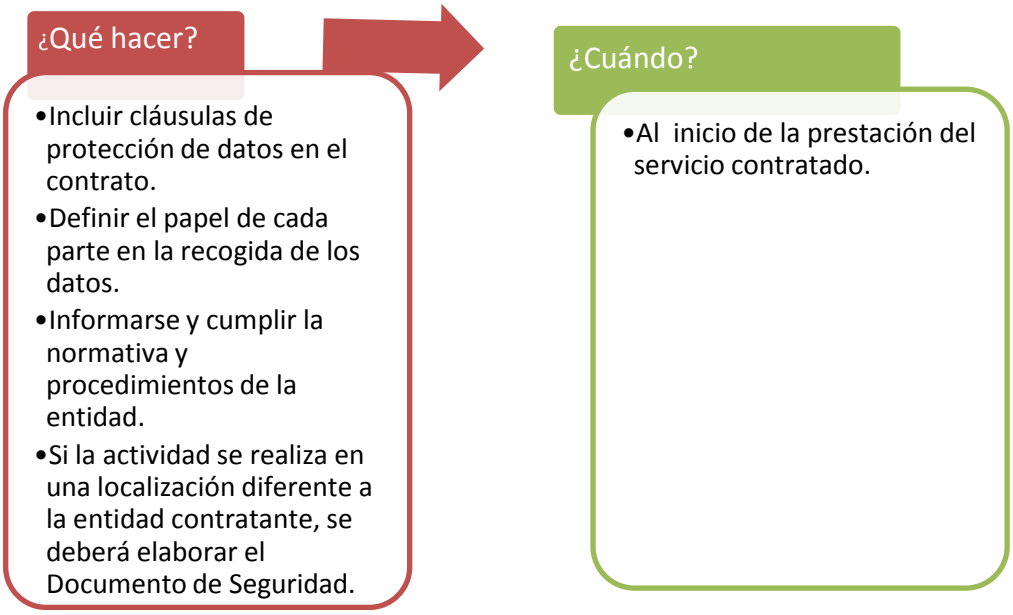
Gráfico 16: cese de la actividad por cuenta ajena.



4.2 Autónomo con contrato de prestación de servicios

El profesional contratado con contrato de prestación de servicios debe aclarar en el contrato de quién es la responsabilidad de los datos, (en este documento anexamos las cláusulas que hay que incluir). Es el momento de dejar claro todos los aspectos en materia de protección de datos.

Gráfico 17: inicio de actividad con contrato de prestación de servicios



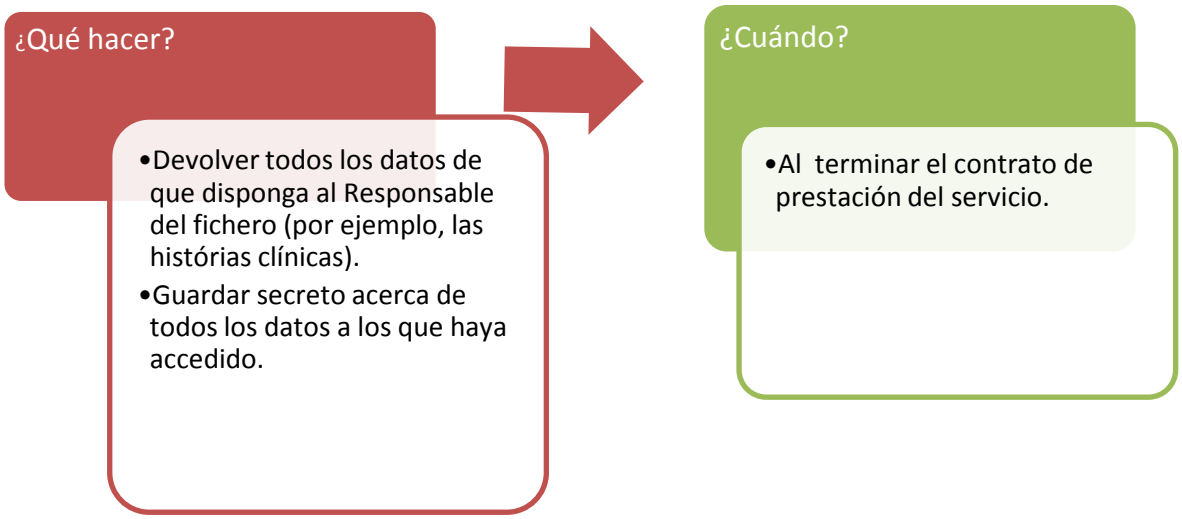
En este caso se actúa como *encargado del tratamiento,* se podrá acceder a los datos que resulten necesarios para la prestación del servicio al responsable del fichero, según las instrucciones de éste. Si los servicios se prestan en los locales del responsable del fichero en el documento de seguridad de éste deberá hacerse constar esta circunstancia.

Si los servicios no se prestaran en los locales del responsable del fichero sino en los del propio profesional contratado, deberá elaborarse un documento de seguridad, identificando el

fichero y el responsable del mismo e incorporando las medidas de seguridad a implantar según el nivel de seguridad del fichero.

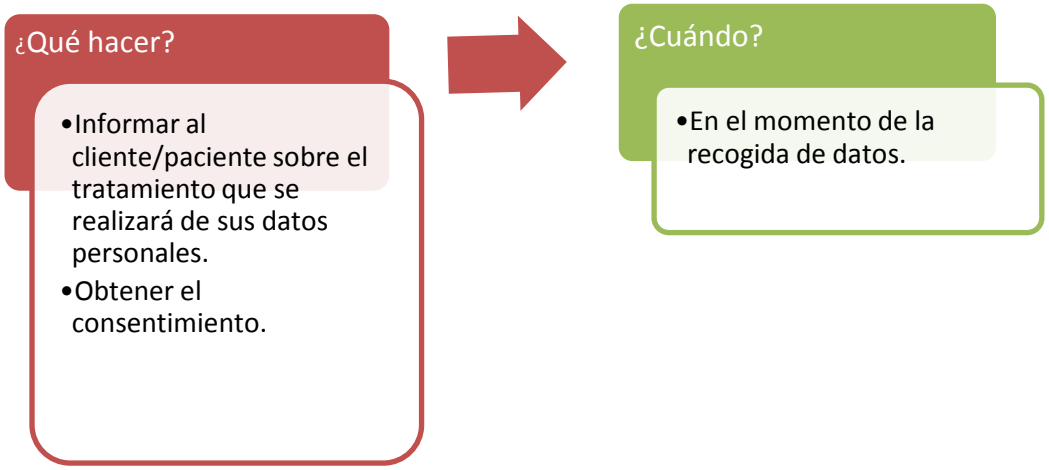
Si algún paciente quisiera seguir el tratamiento con el profesional, deberá ser el propio paciente/cliente quién solicite al responsable del fichero una copia de su historia clínica y se la facilitará con posterioridad al profesional, en ningún caso podría disponer de otra manera de la historia clínica ya que es responsabilidad del responsable del fichero.

Gráfico 18: Cese de prestación del servicio contratado.



5. ENTREVISTA INICIAL

Gráfico 19: entrevista inicial



En la entrevista inicial se comienza a recoger los primeros datos de carácter personal, y por tanto se inicia el tratamiento de los datos en sí, es el momento de llevar a la práctica los aspectos que se planificaron en el apartado anterior.

5.1. Información sobre el tratamiento de los datos y obtención del consentimiento

Es el momento de cumplir con el principio de información de recogida de los datos, al igual que se informa al paciente/cliente en esta primera entrevista sobre aspectos de la intervención psicológica, se debe informar y presentar para su firma un impreso de recogida de datos en el que se habrá incluido una leyenda informativa informando sobre el tratamiento de los datos (ver punto 3.3.1), es conveniente también tener algún cartel informativo sobre protección de datos en la sala de espera.

No es necesario informar y solicitar el consentimiento en cada recogida de datos, sólo habrá que volver a informar si se van a utilizar los datos para una finalidad diferente, ya que la solicitud del consentimiento se refiere a cada tratamiento concreto, si por ejemplo, una persona ha concedido consentimiento para utilizar su dirección para contactar con ella para gestionar las citas, no podemos utilizar ese dato para enviar publicidad, deberá pedirse permiso de forma concreta para ese tratamiento.

El impreso deberá conservarse para poder acreditar que se ha informado sobre protección de datos, puesto que corresponde al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho. Se puede conservar utilizando métodos informáticos, por ejemplo escaneando la documentación, siempre y cuando se garantice que en el escaneado no ha mediado alteración del soporte original.

Gráfico 20: entrevista inicial.

.

5.2. Consentimiento de menores de edad

El Real Decreto 1720/2007 de desarrollo de la LOPD, indica que el caso de menores de edad, se podrá proceder al tratamiento de datos con su consentimiento cuando sean mayores de 14 años, salvo en los casos que la Ley exija para su prestación la asistencia de los titulares de la patria potestad. En el caso de menores de 14 años, se requiere el consentimiento de padres o tutores.

La información recabada del menor debe ser sobre el propio menor, no se puede recabar datos que permita obtener información sobre los demás miembros del grupo familiar, sin el consentimiento de los titulares de los datos, aunque si se podrán solicitar los datos de identidad y dirección de los padres o tutores para recabar la autorización.

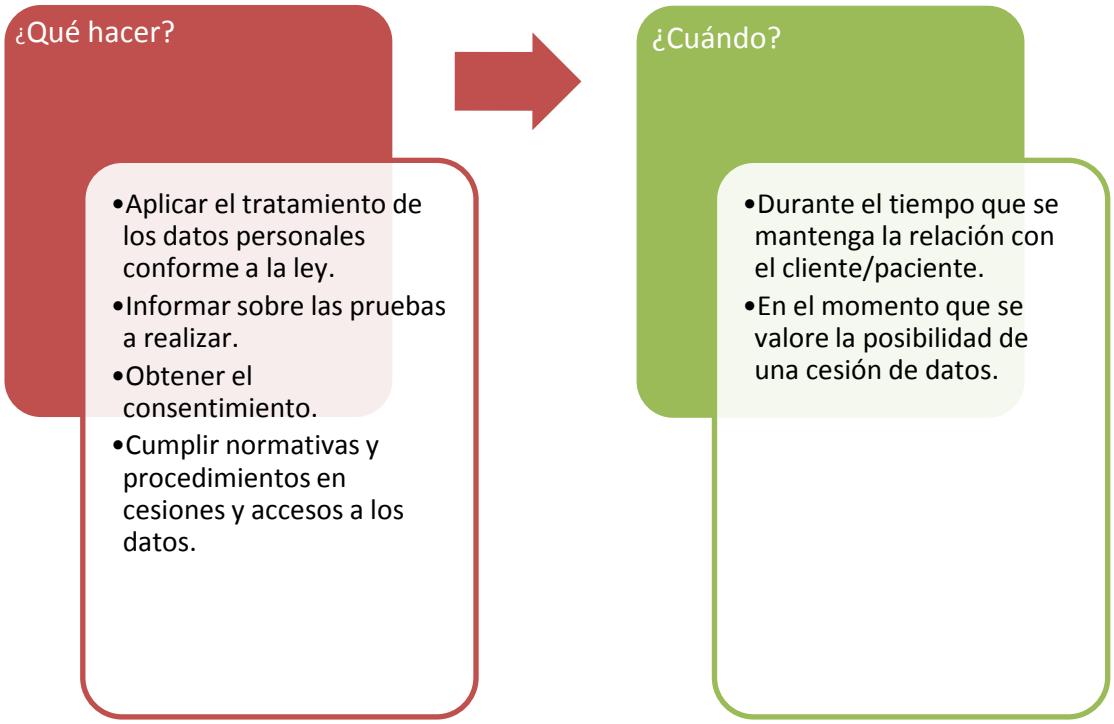
La información sobre el tratamiento de los datos deberá expresarse en un lenguaje que sea comprensible para el menor y hay que recordar que corresponderá al responsable del fichero articular procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representante legal.

No obstante, hay que tener en cuenta que la regla de los catorce años no se aplica en los casos “en los que la Ley exija para su prestación [del consentimiento] la asistencia de los titulares de la patria potestad o tutela”.

6. EVALUACIÓN PSICOLÓGICA Y DERIVACIÓN DE PACIENTES

Durante la evaluación psicológica como en todo el proceso de intervención psicológica hay que realizar un tratamiento adecuado según la normativa de protección de datos, además hay que prestar particular atención a los siguientes aspectos:

Gráfico 21. Evaluación psicológica



6.1. Es necesario que se informe sobre las pruebas que se realicen?

Las pruebas se realizarán siempre con el consentimiento informado del paciente/cliente. Los datos obtenidos de las pruebas que se realicen son considerados también datos de carácter personal, y el paciente/cliente debe saber que serán incorporados y tratados en un fichero de igual manera que el resto de datos facilitados.

En el caso de menores, tal y como se indica en la *Guía de buenas prácticas para la elaboración de informes psicológicos periciales sobre custodia y régimen de visitas de menores*

(Colegio Oficial de Psicólogos de Madrid, 2009), los miembros del núcleo familiar deben conocer previamente la finalidad de la evaluación y los procedimientos que se van a emplear, así como prestar su consentimiento para ello con las limitaciones legamente establecidas en función de la edad.

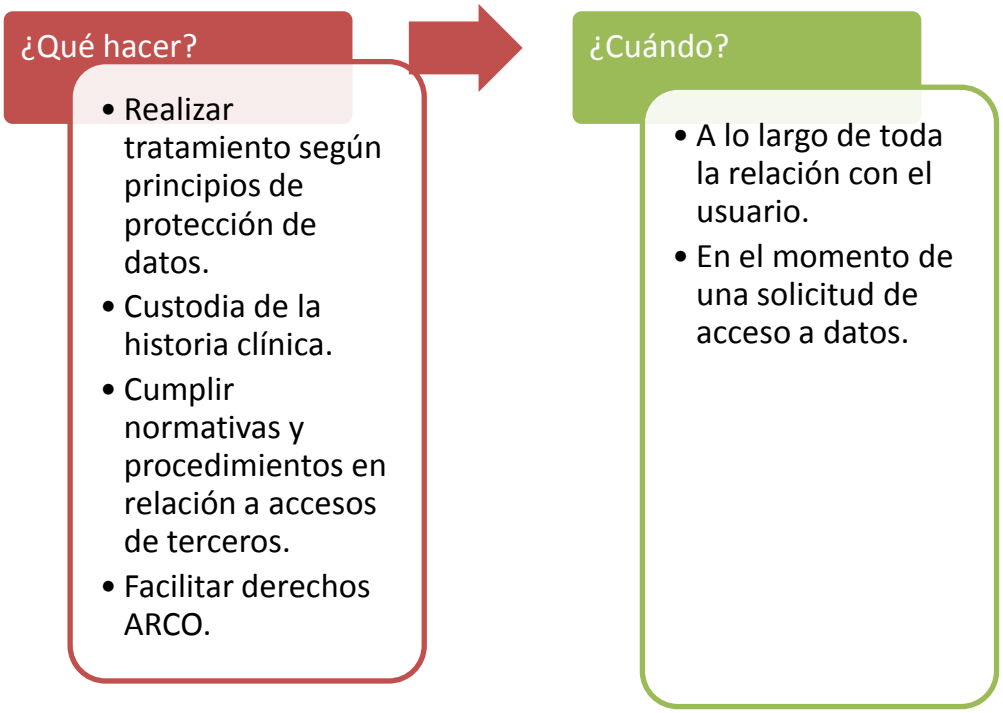
En el caso de evaluación de un menor, se debe informar a todas las partes con patria potestad. Si una de las partes se opone al tratamiento, no se debe realizar la intervención con el menor, sólo se continuaría con autorización judicial.

6.2. ¿Cómo se realiza la cesión de datos a otros profesionales?

En la evaluación psicológica se puede concluir que es más conveniente que la intervención la realice otro profesional, si es necesario facilitar datos sobre el paciente, se deberá informar al paciente y solicitar su consentimiento para facilitar dichos datos, o que sea el propio paciente quién los facilite al profesional al que se deriva el caso.

7. TRATAMIENTO

Gráfico 22: tratamiento psicológico.



7.1. Historia clínica

Al no existir una legislación específica reguladora de la historia clínica psicológica, hemos tomado como referente la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica junto con la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, al elaborar la presente guía.

7.1.1. Archivo por separado de la documentación clínica de la administrativa

Se recomienda archivar por separado la documentación clínica que forma parte del contenido de la historia clínica, de la documentación administrativa que no forma parte de la historia clínica, pero es necesaria para gestionar la historia como pueden ser las hojas de cita previa, documentos contables, facturación, costes económicos de las pruebas, etc. Así facilitaremos el acceso al nivel que es realmente necesario ya que el personal administrativo no necesita acceder a la historia clínica, tal como indicábamos en el punto 3.3.3.

Por otro lado también en conveniente anotar de forma separada las anotaciones personales del psicólogo.

7.2. Secreto profesional y deber de secreto

En cualquier fase del tratamiento de los datos, se tiene obligación de guardar el deber de secreto, que subsiste incluso una vez finalizada la relación laboral de cualquier tipo. Es un deber diferente al que se tiene como profesional psicólogo, (secreto profesional) pero que concurre con el mismo. El deber de secreto, es un deber que afecta a todas las personas que tratan con datos de carácter personal.

Se debe informar sobre él a todos los trabajadores del centro/consulta y resulta además conveniente, incluir cláusulas de confidencialidad en los contratos de trabajo o prestación de servicios. En el anexo se puede encontrar un modelo de cláusula de confidencialidad.

La historia clínica, al contener datos especialmente delicados necesita un especial cuidado en garantizar su confidencialidad, hay que asegurar que sólo podrán acceder a los datos que incluye personas autorizadas, para ello además de implantar las debidas medidas de seguridad pertinentes, hay que concienciar a todas las personas que tengan acceso a la información de la necesidad de guardar el deber de secreto, y ser especialmente cuidadoso en entornos informales (tomando un café, por ejemplo, en no comentar los casos, o de hacerse siempre anonimizando la información, ya que puede ser una potencial fuente de filtraciones de información confidencial.

7.3. Derechos de acceso, rectificación y cancelación de los datos

El derecho de acceso, es el derecho del ciudadano a obtener información sobre sus propios datos de carácter personal que estén siendo objeto de tratamiento, la finalidad del tratamiento, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas, por lo tanto se debe facilitar siempre el acceso a los propios datos, tanto los datos que ha facilitado directamente el paciente/cliente, como el resultado de las pruebas y de las observaciones objetivas. Si se hacen comentarios subjetivos es recomendable anotarlos a parte si no se desea que formen parte de la historia clínica, ya que luego puede resultar más complejo tratar de separar esos datos si el paciente solicita el acceso a sus datos. No tendrían por tanto derecho a acceder a las anotaciones subjetivas del psicólogo, ni a los datos facilitados por terceras personas.

En caso de duda acerca de las anotaciones o si existen datos facilitados por terceros, se puede realizar un informe que resuma los datos objetivos recogidos. (Tiempo para resolver 30 días desde la recepción).

En caso de no disponer de datos también habrá que contestar en dicho sentido en el mismo plazo de tiempo.

El artículo 28 del Reglamento de Desarrollo de la LOPD indica que el afectado puede optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta:

- ✓ Visualización en pantalla.
- ✓ Escrito, copia o fotocopia remitida por correo, certificado o no.
- ✓ Telecopia.

- ✓ Correo electrónico u otros sistemas de comunicación electrónica.
- ✓ Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

Se puede denegar el acceso, si no han pasado 12 meses desde la última petición.

Derecho de rectificación y cancelación

Es el derecho del afectado de modificar o suprimir los datos que resulten ser inexactos o incompletos. En la solicitud deberá indicar a qué datos se refiere y la corrección que hay de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado. La solicitud debe resolverse en el plazo de 10 días a contar desde la recepción de la solicitud.

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que en el mismo plazo, pueda rectificarlo a su vez.

Se recomienda dejar constancia por escrito de haber cumplido con la facilitación de dichos derechos. Hay que recordar también que son derechos independientes unos de otros y por tanto no puede entenderse que el ejercicio de ninguno de ellos sea requisito para el otro.

Estos derechos son personalísimos, por lo que serán ejercidos tan sólo por el afectado, pero el afectado puede ejercerlos a través de un representante voluntario, expresamente designado para el ejercicio del derecho. En este caso deberá constar claramente acreditada la identidad del representado mediante presentación del DNI y la representación conferida por aquél.

7.3.1. ¿Cómo se tiene que solicitar el acceso a los datos personales?

La solicitud debe hacerse por escrito, indicando nombre y apellidos, y adjuntando fotocopia del documento nacional de identidad o documento que lo identifique. Es conveniente tener formularios para facilitar el ejercicio de los derechos de acceso, rectificación y cancelación. En este documento adjuntamos un modelo.

7.3.2. Derechos de acceso, a la historia clínica del menor

Aunque la ley reconoce al menor, pero mayor de 14 años la posibilidad de ejercer sus derechos de acceso a sus datos personales, hay que tener en cuenta si dicho acceso puede causarle un daño psicológico, por lo que la regla de los catorce años no se aplica “en aquellos casos en los que la Ley exija para su prestación [del consentimiento] la asistencia de los titulares de la patria potestad o tutela”.

Habrá que estudiar cada caso, según su capacidad de juicio y discernimiento, no obstante puede considerarse distintos tramos de edad:

Pacientes con dieciséis años cumplidos o emancipados

Tienen derecho a la información y al acceso a la historia clínica propia, sus padres serán informados, aún sin su autorización en casos de una enfermedad grave.

Pacientes con doce años cumplidos

El derecho a la información y el acceso a la historia clínica lo tienen los representantes legales, teniendo el menor un acceso a su información adecuado a la facultad legal de dar opinión. Aunque se le deberá informar sobre el tratamiento y escucharle el consentimiento será responsabilidad de los padres.

Pacientes que no han cumplido los doce años

Todos los derechos los ejercitarán los representantes legales, aunque se deberá dar al menor una información asistencial adecuada a las posibilidades de comprensión del menor.

7.3.3. Derechos de acceso de familiares y terceras personas

Los familiares pueden acceder a la historia clínica si el paciente lo autoriza de forma expresa o tácita, por tanto ningún familiar puede acceder a la información del paciente salvo que exista dicho consentimiento o una habilitación legal, si según el criterio del profesional, el individuo carece de capacidad para entender la información, a causa de su estado físico o psíquico, entonces si se podrá poner en conocimiento de personas vinculadas por razones familiares o de hecho.

7.3.4. Derechos acceso a historia clínica de una persona fallecida

En este caso se podrán facilitar los datos a personas vinculadas al paciente por razones familiares o de hecho, salvo que el fallecido lo hubiera prohibido expresamente y así se acredite.

No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni las facilitadas por terceros.

La consideración de familiar alcanza a la mujer, hijos, padres y hermanos, y la relación de hecho deber estar acreditada en el correspondiente registro o con la inscripción en el padrón.

7.3.5. Casos especiales, derechos en conflicto

Aunque lo normal es que si ambos padres mantienen la patria potestad, aunque no tengan la custodia, ambos tengan acceso a la historia clínica, en el supuesto de padres separados y enfrentados respecto a los intereses del niño o de padres con problemas personales y sociales complejos que hagan dudar de su gestión en beneficio del hijo, en la publicación de la Agencia de Protección de Datos de la Comunidad de Madrid *"Protección de Datos personales para servicios sanitarios Públicos"*, recomiendan consultar con instituciones específicas, en el caso de malos tratos o posibles abusos sexuales indican que habría que denunciar y no dar a los padres acceso a la historia clínica.

7.3.6. Derecho de acceso a órganos judiciales, defensor del pueblo, defensor del menor

Deberá facilitarse tan sólo los datos estrictamente solicitados. Los jueces deberán limitar su petición a acceso a los datos imprescindibles, si esta petición fuera ambigua se deberán pedir aclaraciones.

La comunicación de datos a los órganos indicados no requiere la autorización del paciente, ya que es una de las excepciones indicadas en la LOPD a dicha exigencia. En el artículo 11.2 d) de la LOPD, indica lo siguiente "*Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.*

7.3.7. Derecho de acceso a fuerzas y cuerpos de seguridad

Hay que facilitar los datos que nos soliciten cuando sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales y tan sólo se deberá dar acceso a los que resulten necesarios, y sólo para los fines de una investigación concreta.

7.4. Elaboración de informes

En el informe se incluirán los datos que se han recogido a lo largo de la intervención, es válido aquí por tanto todo lo mencionado sobre incluir tan sólo la información que sea relevante y

pertinente para la finalidad del informe. Los informes no deben ser utilizados para ninguna finalidad diferente a la finalidad para la que se recogieron los datos.

7.4.1. ¿Qué datos es adecuado incluir en un informe?

Los datos que se incluyen en un informe psicológico con relación a los comportamientos o las actitudes de las personas evaluadas tienen que estar suficientemente fundamentadas y contrastadas, así mismo no deben incluirse datos excesivos o no pertinentes a la finalidad del informe, (por ejemplo en un informe pericial sería dar respuesta al objeto de la pericia).

7.4.2. ¿Quién puede tener acceso a los informes?

Sólo debe tener acceso a un informe, la persona que ha solicitado dicho informe, en el caso de menores, dependerá de la edad del menor, este aspecto se ha desarrollado con mayor amplitud en el apartado de derechos de acceso a la historia clínica.

En el caso concreto del informe pericial de custodia, la *Guía de buenas prácticas para la elaboración de informes psicológicos periciales sobre custodia y régimen de visitas de menores (Colegio Oficial de Psicólogos de Madrid, 2009),* indica que tiene derecho al acceso y a la recepción del informe pericial las partes que autorizaron la realización del informe de custodia y sus respectivos abogados y el Juez.

En el caso de un informe solicitado por un Juez, se entregará a éste el informe, sin perjuicio del derecho a conocer el contenido del mismo por parte del sujeto evaluado o sus padres o tutores, que pueden conocerlo a través del Juzgado y, en caso de que ello no sea posible, a través del profesional que lo emite, siempre que de ello no se derive perjuicio grave para el sujeto o para el Psicólogo, conforme al artículo 42 del Código Deontológico del Psicólogo.

A las personas que han colaborado en la investigación del entorno del menor, en un informe de custodia, si lo solicitan, se les puede leer la parte correspondientes a sus declaraciones o sus aportaciones en pruebas psicológicas.

7.4.3. ¿Qué procedimientos garantizan la protección de datos al entregar un informe a un usuario?

Se deberá entregar el informe directamente a la persona interesada, en caso de entregárselo a un representante voluntario, deberá ser expresamente designado por la persona interesada. En este caso deberá constar claramente acreditada la identidad de ambos mediante presentación del DNI y la representación conferida por aquél.

En caso de realizarse la entrega del informe a través de telecomunicación, deberá garantizarse las medidas de seguridad correspondientes al nivel de seguridad del fichero, en el caso de un nivel de seguridad alto, el Real Decreto 1720/2007 determina que la información debe enviarse encriptada, no obstante, aún no siendo los datos de dicho nivel, debido a la naturaleza de los datos de dichos informes es conveniente que sea encriptada siempre que se transmitan datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas, o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

7.4.4. Confidencialidad en un informe pericial

En el caso de informe pericial, obviamente se inicio la evaluación para informar en un proceso judicial, por lo que se está excluido del deber de confidencialidad, no obstante hay que recordar que esa exclusión sólo atañe al objeto específico del informe pericial, evitando incluir información no relacionada con dicho objeto. Así mismo, como bien se indica en la *Guía de buenas prácticas para la elaboración de informes psicológicos periciales sobre custodia y régimen de visitas*

de menores (Colegio Oficial de Psicólogos de Madrid, 2009), el perito debe informar de esta limitación de la confidencialidad en este tipo de evaluación a la persona a la que se está evaluando y que la información será utilizada para una evaluación forense.

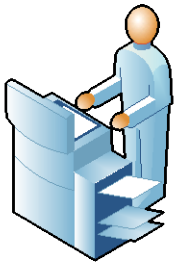
Seis buenas prácticas

1

Carteles en salas de reunión, fax, impresoras y fotocopiadoras:

Retirar los documentos que contienen datos de carácter personal al abandonar la sala o el equipo usado.

2



Impresoras compartidas:

Situadas en zonas de acceso exclusivo por personal autorizado.

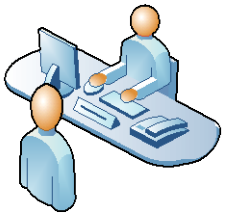
Antes de enviar por fax:

¡ Avisar al destinatario !

¡ Comprobar que el número es correcto ¡

¡ No dejar el fax transmitiendo sin nadie al cargo!

3

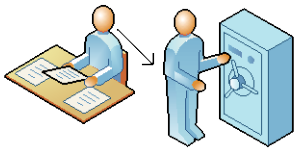


Pantallas y ordenadores:

Las pantallas situadas para no permitir la visualización de datos por personal no autorizado.

Con contraseña para reanudar sesión después de un intervalo determinado de inactividad

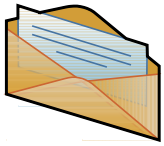
4



Al retirarse del puesto de trabajo:

Guardar el expediente en un cajón o armario bajo llave.

¡No dejar expedientes sobre la mesa!

5		**Al enviar e-mail:** Incluir los destinatarios en copia oculta. Cifrar los archivos adjuntos.
6		**Al destruir documentación:** Romper en trozos que hagan irreconocibles los datos Utilizar máquinas destructoras ó contratar empresas con garantías.

Fuentes de información recomendadas

Web Agencia Española de Protección de datos.

https://www.agpd.es/portalwebAGPD/canalresponsable/index-ides-idphp.php

Se puede acceder a abundante información sobre protección de datos. Ofrece acceso a guías de protección de datos, entre ellas un modelo guía de documento de seguridad que facilita en gran medida la elaboración de un documento de seguridad.

Web del Colegio Oficial de Psicólogos de Madrid. Área Protección de Datos.

http://www.copmadrid.org/webcopm/section.do?area=19000101010101020150

En la página web del Colegio Oficial de Psicólogos de Madrid, se puede encontrar abundante documentación sobre protección de datos, manuales, guías, apartados de preguntas frecuentes, así como acceso a normativas y modelos de textos y documentos tipo para facilitar la adecuación a la legislación de protección de datos.

Así mismo tienen a disposición de las personas interesadas un foro para plantear dudas e inquietudes sobre protección de datos. Foro de Protección de Datos del Colegio oficial de Psicólogos de Madrid. http://www.copmadrid.org/foros/

Además, los colegiados cuentan con un servicio de asesoramiento sobre protección de datos, tanto telefónico como por correo electrónico – Lola Manzano, protecciondatos@cop.es, teléfono 91 541 99 99.

Agencia de Protección de Datos de la Comunidad de Madrid. (2009). Seguridad y Protección de datos personales. Madrid: Thomson.

Un manual muy completo, en el que se desarrolla todas las medidas de seguridad a implantar en los ficheros, (tanto técnicas como organizativas, también facilitan modelos y documentos tipo).

Agencia de Protección de Datos de la Comunidad de Madrid. (2008). Protección de datos personales para Servicios Sanitarios Públicos Madrid: Thomson.

Dirigido a servicios sanitarios públicos contiene información de interés para cualquier profesional del área clínica y a su vez se pueden encontrar numerosos modelos que facilitan en gran medida la adecuación a la LOPD.

Referencias bibliográficas

Boletín Oficial del Estado. *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* BOE núm., 298, 14/12/1999.

Boletín Oficial del Estado. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE núm., 17, 19/01/2008.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DO L 281 de 23.11.95, p. 3

Boletín Oficial de la Comunidad de Madrid. Recomendación 2/2004, de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas. Aprobada por Resolución del Director de la Agencia de Protección de Datos de la Comunidad de Madrid con fecha 30-7-2004) BO. Comunidad de Madrid 12 agosto 2004, núm. 191, pág. 7)

Boletín Oficial de la Comunidad de Madrid. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. BOE núm., 274 15/11/ 2002

Colegio Oficial de Psicólogos de Madrid (2009), Guía de buenas prácticas para la elaboración de informes psicológicos periciales sobre custodia y régimen de visitas de menores

Agencia de Protección de Datos de la Comunidad de Madrid. (2008) Protección de datos personales para Servicios Sanitarios Públicos, Thomson, Madrid

Agencia de Protección de Datos de la Comunidad de Madrid (2009) Seguridad y Protección de datos personales, Thomson, Madrid.

ANEXO I. Extractos de la LOPD-Principios de protección de datos

La protección de datos es el derecho fundamental a controlar los propios datos de carácter personal, para articularlo hay unos límites y pautas que determina la ley de protección de datos. Por ello cualquier tratamiento de datos de carácter personal, debe adecuarse a los principios de protección de datos que determina el título II de la LOPD y que a continuación se extractan.

Artículo 4. Principio de calidad de los datos

Los datos de carácter personal sólo se pueden recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. De ser inexactos, serán cancelados y sustituidos de oficio por los datos rectificados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuáles hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos extractan.

Artículo 5. Derechos de información en la recogida de datos

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar,

salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

Cuando se utilicen cuestionarios y otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refieren las letras b),c) y d) del aparado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del primer apartado del presente artículo.

No será de aplicación lo dispuesto en el aparado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado

El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación, laboral o administrativa y sean necesarios para su mantenimiento do cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del Artículo 7 apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que un ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos

De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con esto datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y

creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los 7 apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. Seguridad de los datos

El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una Ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso a los datos por cuenta de terceros

No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará

con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

ANEXO II. Modelos de textos en materia de protección de datos.

A continuación se incluyen algunos modelos de textos para facilitar la labor de adecuación a la Ley de Protección de Datos, los textos se han obtenido de la publicación de la Agencia de Protección de Datos de la Comunidad de Madrid, " *Protección de datos personales para Servicios Sanitarios Públicos"* adaptándolos en algunos casos a la intervención psicológica.

Modelo de texto a incluir en formularios de recogida de datos

Sus datos personales serán incorporados y tratados en el fichero automatizado (NOMBRE FICHERO), inscrito en la Agencia de Protección de Datos Española (www.agpd.es), con la finalidad de (INCLUIR FINALIDAD DEL FICHERO), pudiéndose realizar las cesiones previstas en la Ley. El órgano responsable del fichero es (NOMBRE EMPRESA, CENTRO O CONSULTA) con domicilio en (DIRECCIÓN EMPRESA CENTRO O CONSULTA), ante el cual los interesados podrán ejercer sus derechos de acceso, cancelación, rectificación y oposición, dirigiendo un escrito al (NOMBRE EMPRESA, CENTRO O CONSULTA), a la dirección mencionada, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (ref. "tratamiento de datos"), indicando su nombre, dirección y petición.

Modelo de cláusulas a incluir en un contrato de acceso a datos por terceros

- ✓ El contratista, como encargado del tratamiento, tal y como se define en la letra g) del artículo 3 de ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, declara expresamente que conoce quedar obligado al cumplimiento de lo dispuesto en la citada LOPD y especialmente en lo indicado en sus artículos 9, 10, 12 y adoptara las medidas de seguridad que le correspondan según el Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD.
- ✓ El/los adjudicatario/s en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (y, muy especialmente, de lo indicado en su artículo 12). El/los adjudicatario/s se comprometen explícitamente a formar e informar a su personal en las obligaciones que de tales normas dimanan.
- ✓ Igualmente, serán de aplicación las disposiciones de desarrollo de las normas anteriores que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia, y aquellas normas del Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD.
- ✓ La empresa adjudicataria declara expresamente que conoce quedar obligada al cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, expresamente, en lo indicado en su artículo 10, en cuanto al deber de secreto, así como lo dispuesto en la Ley 8/2001 de la Comunidad de Madrid y, especialmente, lo indicado en su artículo 11. La empresa adjudicataria se compromete explícitamente a formar e informar a su personal en las obligaciones que de tales normas dimanan.
- ✓ La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no

hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

- ✓ El/los licitador/es aportarán una memoria descriptiva de las medidas que adoptarán para asegurar la confidencialidad e integridad de los datos manejados y de la documentación facilitada. Asimismo, el/los adjudicatario/s deberán comunicar a "el organismo contratante", antes de transcurridos siete días de la fecha de comunicación de la adjudicación, la persona o personas que serán directamente responsables de la puesta en práctica y de la inspección de dichas medidas de seguridad, adjuntando su perfil profesional.

- ✓ Si la empresa adjudicataria aporta equipos informáticos, una vez finalizadas las tareas el adjudicatario, previamente a retirar los equipos informáticos, deberá borrar toda la información utilizada o que se derive de la ejecución del contrato, mediante el procedimiento técnico adecuado. La destrucción de la documentación de apoyo, si no se considerara indispensable, se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, efectuándose esta operación en el lugar donde se realicen los trabajos.

- ✓ La documentación se entregará al adjudicatario para el exclusivo fin de la realización de las tareas objeto de este contrato, quedando prohibido para el adjudicatario y para el personal encargado de su realización, su reproducción por cualquier medio y la cesión total o parcial a cualquier persona física o jurídica. Lo anterior se extiende asimismo al producto de dichas tareas.

- ✓ El/los adjudicatario/s se comprometen a no dar información y datos proporcionados por "el organismo contratante" para cualquier otro uso no previsto en el presente Pliego. En particular, no proporcionará, sin autorización escrita de "el organismo contratante", copia de los documentos o datos a terceras personas.

- ✓ Todos los estudios y documentos elaborados durante la ejecución del presente contrato serán propiedad de "el organismo contratante", quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el/los adjudicatario/s autor/es de los trabajos.

- ✓ Específicamente, todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo del contrato resultante de la adjudicación del presente concurso, corresponden únicamente a "el organismo contratante".

- ✓ El resultado de las tareas realizadas, así como el soporte utilizado (papel, fichas, disquetes, etc.) serán propiedad del "organismo contratante".

Modelo compromiso de confidencialidad para contratos de trabajo

El trabajador se compromete a guardar secreto sobre las informaciones confidenciales y los datos de carácter personal de los que tenga conocimiento en el ejercicio de las funciones que le sean encomendadas, de conformidad con lo establecido en el artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el artículo 11 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, incluso tras haber finalizado su relación profesional con la empresa.

El trabajador deberá cumplir con el resto de principios y obligaciones establecidos por la normativa de Protección de Datos.

Igualmente, el trabajador estará obligado a atender las instrucciones relativas a la seguridad de los datos de carácter personal contenidas en las políticas de seguridad y en el documento de seguridad y difundidas, en su caso, por el responsable del fichero o el responsable de seguridad, de conformidad con lo establecido en el Real Decreto 1720/2007, de 21 de diciembre, por el que se

aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

☐ Modelo de consentimiento de los usuarios para la cesión de datos a las compañías de seguro libre de asistencia sanitaria

D. Dª _____, de profesión _____provisto/a de DNI_____, y con domicilio en_____

DECLARO haber sido informado/a que mis datos personales serán tratados y quedarán incorporados en los ficheros del centro sanitario/de la consulta, con la finalidad de facilitar la prestación de los servicios psicológicos, en cumplimiento a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal.

Los destinatarios de la información son el psicólogo o psicólogos de este centro sanitario/consulta, implicados en su proceso asistencial.

Asimismo, he sido informado/a que puedo ejercitar los derechos de acceso, rectificación y, en su caso, cancelación u oposición, ante el centro sanitario/la consulta, en_____.

Con la firma del presente escrito dejo constancia de haber sido informado/a previamente, y CONSIENTO de forma expresa que mis datos puedan ser comunicados o cedidos a_____, como compañía de seguro libre de asistencia sanitaria.

Únicamente se comunicarán a dicha entidad aquellos datos personales que sean los pertinentes, adecuados y no excesivos para cumplir, desarrollar y controlar las obligaciones que para asegurado y entidad aseguradora vienen establecidas en el contrato de seguro de salud por el que se garantiza la prestación sanitaria.

En _____, a_____

Fdo.:_____

☐ Modelo de consentimiento para comunicar o ceder los datos de los afectados o interesados a terceros implicados en el diagnóstico, prevención o tratamiento

D. Dª _____, de profesión_____provisto/a de DNI_____, y con domicilio en_____

DECLARO: haber sido informado/a que mis datos personales serán tratados y quedarán incorporados en los ficheros del centro sanitario/de la consulta, con la finalidad de facilitar la prestación de los servicios médicos, en cumplimiento a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal.

Los destinatarios de la información son el médico o médicos/psicólogo de este centro sanitario/consulta, implicados en su proceso asistencial.

Asimismo, he sido informado/a que puedo ejercitar los derechos de acceso, rectificación y, en su caso, cancelación u oposición, ante el centro sanitario/la consulta, en _____, cuyo responsable es_____.

Con la firma del presente escrito CONSIENTO de forma expresa que mis datos, cuando fuese necesario, puedan ser comunicados o cedidos a _____, como servicios médicos o sanitarios en general que complementan las actuaciones médicas llevadas a cabo por este centro sanitario/esta consulta. Los datos a comunicar son los pertinentes, adecuados y no excesivos para la prestación de los referidos servicios médicos o sanitarios en general, y son los siguientes:_____

La finalidad concreta que motiva la cesión o comunicación de datos es la siguiente:_____

La persona física o jurídica a la que se ceden los datos se comprometerá a no ceder a su vez dichos datos a ningún tercero, ni siguiera para su conservación.

Del mismo modo, he quedado informado de la obligación que tienen tales servicios médicos o sanitarios para la creación y conservación de un fichero con los datos personales cedidos y cuya responsabilidad sería de aquellos, según lo dispuesto en la legislación estatal o autonómica en esta materia.

Modelo de documento de cesión de historias clínicas

De una parte, D./Dª_____, colegiado/a nº _____, provisto/a de D.N.I._____, y con domicilio en _____, en nombre y por cuenta propia/en nombre y representación de _____, con NFI/CIF_____.

De otra, D./Dª._____, colegiado/a nº _____ provisto/a de D.N.I. _____, y con domicilio en _____en nombre y por cuenta propia/en nombre y representación de _____, con N.I.F./C.I.F._____

Ambas partes, de común acuerdo, convienen.

1. Que_____ ha decidido cesar en su actividad profesional, por_____(jubilación, causas económicas,_____), y como consecuencia de ello cede las historias clínicas de sus pacientes a_____.

2. En tales circunstancias, el cesante ha procedido a notificar este hecho a todos sus pacientes, recabando su consentimiento expreso con carácter previo a este acto.

3. _____ se compromete a continuar con el seguimiento de las referidas historias clínicas de sus pacientes a _____

4. _____ se obliga a que los datos personales contenidos en las historias clínicas serán tratados y quedarán incorporados en los ficheros del centro sanitario/de la consulta, con la finalidad de facilitar la prestación de los servicios médicos, en cumplimiento a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal.

A tal efecto, permitirá el ejercicio de los derechos de acceso, rectificación y, en su caso, cancelación u oposición, ante el centro sanitario/la consulta, en _____

En_____, a_____
Firmado_____

☐ Modelo de consentimiento para comunicar o ceder las historias clínicas por cese de actividad profesional

D./Dª._____, provisto/a de DNI_____, y con domicilio en _____

DECLARO haber sido informado/a que D./Dª. _____, colegiado/a nº _____, provisto/a de DNI _____ y con domicilio en _____, en nombre y por cuenta propia/en nombre y representación de _____-, con NIF_____-, va a cesar en el ejercicio de su actividad profesional.

Por medio de este documento, COSIENTO expresamente que la historia clínica abierta a mi nombre en el referido centro sanitario/consulta en la que constan datos relativos a mi salud, sea cedida a_____ para que continúe con el seguimiento de la misma o se ocupe de su archivo, al menos, durante el plazo legalmente establecido.

De ese modo, mis datos personales serán tratados y quedarán incorporados en los ficheros del centro sanitario/de la consulta, con la finalidad de facilitar la prestación de los servicios médicos, en cumplimiento a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal.

Asimismo, he sido informado/a que puedo ejercitar los derechos de acceso, rectificación y, en su caso, cancelación u oposición, ante el centro sanitario/la consulta, en_____.

En _____,a _____

Fdo.:_____

Modelos para facilitar los derechos de acceso, rectificación y cancelación (obtenido de la Agencia Española de Protección de datos)

EJERCICIO DEL DERECHO DE ACCESO[1]
DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: .....
Dirección ante el que se ejercita el derecho de acceso: .....nº .....
C.Postal ..... Localidad ..... Provincia .....C.I.F./D.N.I. .....

DATOS DEL INTERESADO O REPRESENTANTE LEGAL[2]

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los artículos 12 y 13 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Segunda de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso.

Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En .....a.....de.....de 20..... Firmado:

[1] Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Organismo Público o entidad privada) que es quien dispone de los datos. La Agencia Española de Protección de Datos no dispone de sus datos personales sino solamente de la ubicación del citado responsable si el fichero está inscrito en el Registro General de Protección de Datos.

[2] También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

Sus datos personales serán incorporados y tratados en el fichero automatizado (NOMBRE FICHERO), inscrito en la Agencia de Protección de Datos Española (www.agpd.es), con la finalidad de (INCLUIR FINALIDAD DEL FICHERO), pudiéndose realizar las cesiones previstas en la Ley. El órgano responsable del fichero es (NOMBRE EMPRESA, CENTRO O CONSULTA) con domicilio en (DIRECCIÓN EMPRESA CENTRO O CONSULTA), ante el cual los interesados podrán ejercer sus derechos de acceso, cancelación, rectificación y oposición, dirigiendo un escrito al (NOMBRE EMPRESA, CENTRO O CONSULTA), a la dirección mencionada, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (ref. “tratamiento de datos”), indicando su nombre, dirección y petición.

EJERCICIO DEL DERECHO DE RECTIFICACIÓN[1]

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: .....

Dirección:..... nº ..... C. Postal ..... Localidad ..... Provincia ..... C.I.F./D.N.I. .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL[2]

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de rectificación sobre los datos anexos, aportando los correspondientes justificantes, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el artículo 15 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Tercera de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

Que se proceda a acordar la rectificación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada. Que en caso de que se acuerde, dentro del plazo de diez días, que no procede acceder a practicar total o parcialmente las rectificaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la citada Ley

Orgánica 15/1999. Que si los datos rectificados hubieran sido comunicados previamente se notifique al responsable del fichero la rectificación practicada, con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

En .....a.....de.....de 20.....

Firmado:

1 Consiste en la petición dirigida al responsable del fichero con el fin de que los datos personales respondan con veracidad a la situación actual del afectado.

2 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

Sus datos personales serán incorporados y tratados en el fichero automatizado (NOMBRE FICHERO), inscrito en la Agencia de Protección de Datos Española (www.agpd.es), con la finalidad de (INCLUIR FINALIDAD DEL FICHERO), pudiéndose realizar las cesiones previstas en la Ley. El órgano responsable del fichero es (NOMBRE EMPRESA, CENTRO O CONSULTA) con domicilio en (DIRECCIÓN EMPRESA CENTRO O CONSULTA), ante el cual los interesados podrán ejercer sus derechos de acceso, cancelación, rectificación y oposición, dirigiendo un escrito al (NOMBRE EMPRESA, CENTRO O CONSULTA), a la dirección mencionada, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (ref. “tratamiento de datos”), indicando su nombre, dirección y petición.

EJERCICIO DEL DERECHO DE CANCELACIÓN[1]

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: .....Dirección:.....
.....
..... nº ..... C. Postal ..... Localidad ..... Provincia .....C.I.F./D.N.I. .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL[2]

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de cancelación, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los artículos 15 y 16 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la

Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Tercera de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

Que se proceda a acordar la cancelación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada. Que en caso de que se acuerde dentro del plazo de diez días que no procede acceder a practicar total o parcialmente las cancelaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la citada Ley Orgánica 15/1999. Que si los datos cancelados hubieran sido comunicados previamente se notifique al responsable del fichero la cancelación practicada con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

En .....a.....de.....de 20.....

Firmado:

1 Consiste en la petición de cancelación de un dato que resulte innecesario o no pertinente para la finalidad con la que fue recabado. El dato será bloqueado, es decir, será identificado y reservado con el fin de impedir su tratamiento.

2 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

Sus datos personales serán incorporados y tratados en el fichero automatizado (NOMBRE FICHERO), inscrito en la Agencia de Protección de Datos Española (www.agpd.es), con la finalidad de (INCLUIR FINALIDAD DEL FICHERO), pudiéndose realizar las cesiones previstas en la Ley. El órgano responsable del fichero es (NOMBRE EMPRESA, CENTRO O CONSULTA) con domicilio en (DIRECCIÓN EMPRESA CENTRO O CONSULTA), ante el cual los interesados podrán ejercer sus derechos de acceso, cancelación, rectificación y oposición, dirigiendo un escrito al (NOMBRE EMPRESA, CENTRO O CONSULTA), a la dirección mencionada, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (ref. “tratamiento de datos”), indicando su nombre, dirección y petición.