Colegio Oficial de Psicólogos de Madrid

Guía de Protección de Datos Personales en Psicología: Implicaciones y Buenas Prácticas

6E78BC9
6E78BC9
6E78BC9
6E78BC9

Colegio Oficial de Psicólogos de Madrid

Guía de Protección de Datos Personales en Psicología: Implicaciones y Buenas Prácticas

Edita: Colegio Oficial de Psicólogos de Madrid
C/. Cuesta de San Vicente, 4 - 28008 Madrid
http://www.copmadrid.org - Email: copmadrid@cop.es
ISBN: 978-84-87556-81-4
Diseño y maquetación: Gráficas Nitral

El Colegio Oficial de Psicólogos de Madrid está comprometido con el uso de un lenguaje igualitario y no sexista. No obstante, en aras de la brevedad del texto y la facilidad de lectura, en el resto de esta Guía se entenderá que «colegiados» hace referencia a colegiados y colegiadas, «psicólogos» a psicólogos y psicólogas, etc.

Índice

1

Presentación

6E78BC9
6E78BC9
6E78BC9
6E78BC9

La Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (en adelante LOPD), impone una serie de obligaciones legales para aquellos profesionales que traten con datos de carácter personal. Así mismo, el Real Decreto 1720/2007 desarrolla la mencionada ley orgánica y establece una serie de medidas destinadas a garantizar la protección de datos.

Los psicólogos en su práctica profesional, manejan datos considerados de carácter personal, datos que afectan de lleno a la esfera íntima del individuo. Un mal tratamiento de estos datos puede atentar gravemente contra el derecho a la intimidad de los pacientes/clientes.

Además, es de vital importancia adecuarse a la normativa de protección de datos, ya que establece elevadas sanciones por su incumplimiento.

El objetivo de esta *Guía de Protección de Datos Personales en Psicología: Implicaciones y Buenas Prácticas*, es identificar las cuestiones específicas a resolver en cada una de las etapas de la intervención psicológica para adecuar el ejercicio de la profesión a la legislación de protección de datos, con las peculiaridades que determinan otras legislaciones que regulan la profesión, como puede ser 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.

Esta guía quiere ser una referencia útil para todos los profesionales de la Psicología, sea cual sea el campo de intervención psicológica o la forma de ejercicio, aunque por las implicaciones evidentes de la Ley en esta especialidad se orienta con mayor medida al área de clínica. No obstante, se dispone en la página web del Colegio Oficial de Psicólogos de Madrid de guías que recogen las peculiaridades en otras áreas de intervención.

El documento se ha estructurado en dos apartados principales, uno con las peculiaridades específicas de cada forma de ejercicio (por cuenta propia o por cuenta ajena), y otro con los aspectos comunes. Se espera así facilitar la lectura y su uso, para que cada profesional pueda obtener la información que necesita conforme a su situación.

Fernando Chacón Fuertes
Decano del Colegio Oficial de Psicólogos de Madrid

6E78BC9
6E78BC9
6E78BC9
6E78BC9

2

Introducción

El documento presente tiene la finalidad de identificar las prácticas a realizar en materia de protección de datos de carácter personal en el ámbito de la intervención profesional en Psicología. 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 de la intervención psicológica.

Figura 1
Fases de intervención

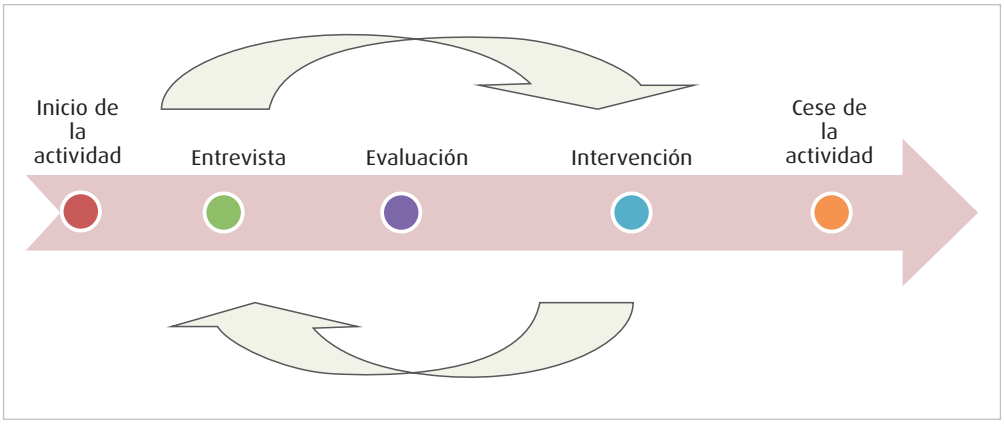
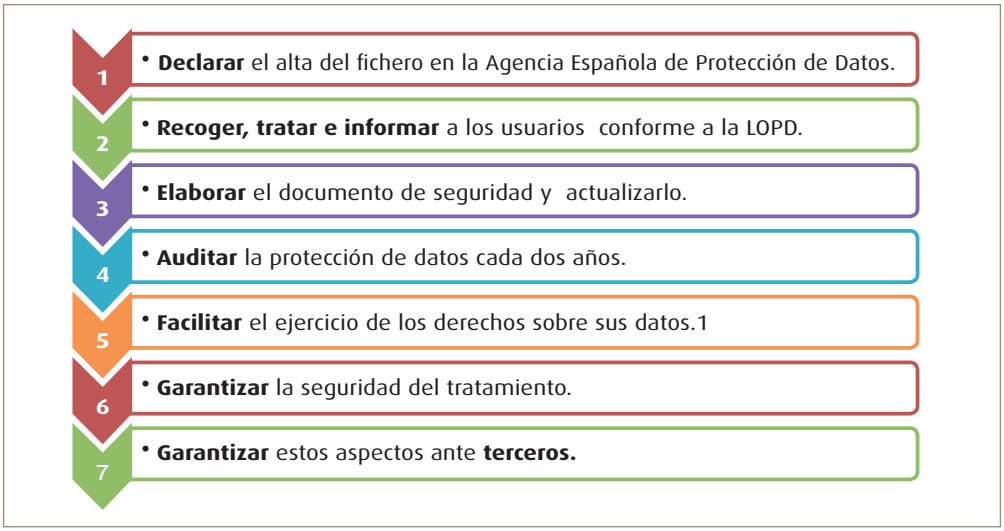


Figura 2
Principales obligaciones



El marco normativo específico y los modelos de referencia figuran en los Anexos correspondientes, con la finalidad de facilitar la comprensión de las cuestiones clave en cada etapa de

(1) 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.

la intervención. Es importante señalar que el nuevo Reglamento General de Protección de Datos (Reglamento UE 2016/679) entró en vigor en mayo de 2016 y será aplicable a partir de mayo de 2018. En este periodo de transición será preciso adaptar los tratamientos a dicha legislación por lo que se irá actualizando este documento en dicho sentido a medida que la Agencia Española de Protección de Datos vaya facilitando más información.

No obstante, se trata de indicaciones que cada profesional debe adaptar a su práctica profesional específica, cumpliendo con la responsabilidad del cumplimiento de la legislación vigente.

Figura 3
Cuestiones pertinentes en cada fase de la intervención

6E78BC9
6E78BC9
6E78BC9
6E78BC9

3

Glosario

6E78BC9
6E78BC9
6E78BC9
6E78BC9

Para facilitar la lectura de la guía, a continuación incluimos la definición de algunos conceptos fundamentales en materia de protección de datos.

Definiciones REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **Datos de carácter personal:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
- **Tratamiento:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Responsable del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
- **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- **Consentimiento del interesado:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

6E78BC9
6E78BC9
6E78BC9
6E78BC9

4

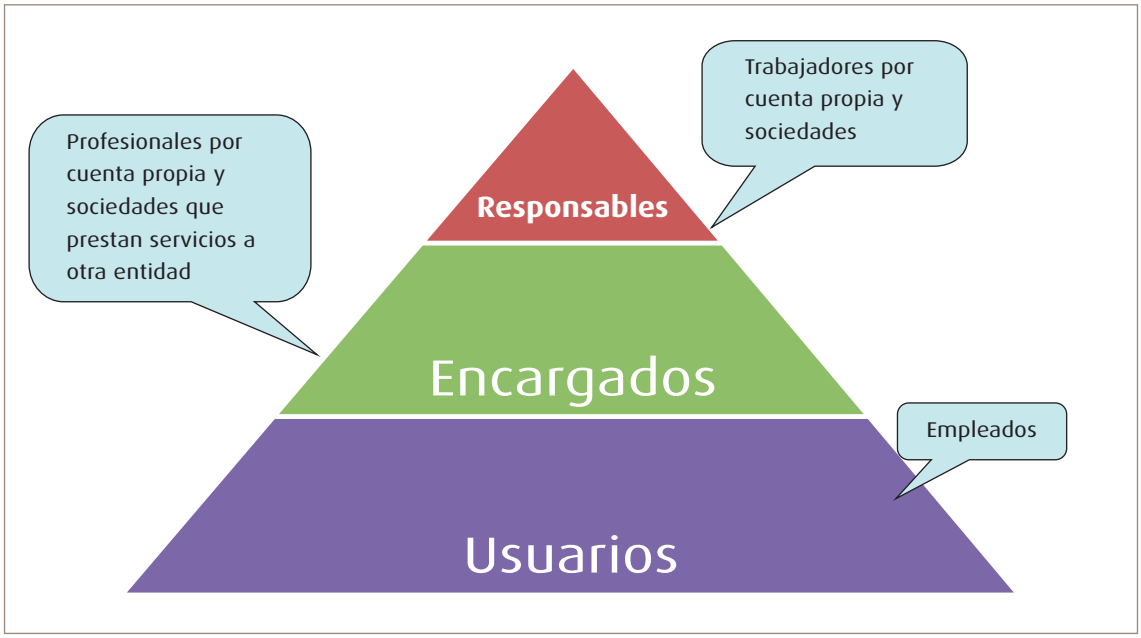
Formas de ejercicio profesional y responsabilidad en el tratamiento de los datos

A lo largo del desarrollo de la actividad profesional, los diferentes regímenes de ejercicio (por cuenta propia o por cuenta ajena) 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, uno 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:

Figura 4
Responsabilidad del tratamiento



4.1 Profesionales por cuenta propia

Los **profesionales autónomos** son las figuras **responsables de sus propios ficheros,** ya que son quienes deciden sobre la finalidad, contenido y tratamiento de los datos de carácter personal de sus clientes/pacientes. En la misma situación se considera a los profesionales que comparten la misma ubicación profesional, si bien cada profesional constituye una sociedad económica independiente, ya que, aunque compartan un mismo espacio de trabajo, cada uno es responsable de sus propios ficheros.

Además, son responsables de los ficheros aquellos profesionales por cuenta propia que atienden a clientes de una empresa determinada sin mantener una relación de dependencia con ésta, como es el caso de aquellos que atienden a clientes de una compañía aseguradora

sanitaria. Por tanto, los profesionales por cuenta propia, son los responsables de las historias clínicas de sus pacientes, y cuando cese su actividad en la compañía deberán, responsabilizarse de la custodia de las historias clínicas o formalizar los pasos necesarios para la cesión de los datos a la empresa.

4.2 Sociedad profesional

Este caso ser refiere a cuando varios psicólogos forman una sociedad profesional y el cliente/paciente contrata los servicios con la sociedad, no con uno de los profesionales de forma específica. En este caso los ficheros serían responsabilidad de la sociedad.

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

Al trabajar por cuenta ajena, los profesionales tienen un contrato laboral con una empresa o sociedad, tienen por tanto una relación de dependencia y existe una relación laboral con la empresa, que es la que tiene la responsabilidad de los ficheros. Estos profesionales están obligados a 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. Si el paciente quisiera seguir con el profesional, deberá solicitar su historia clínica y facilitársela directamente al 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.

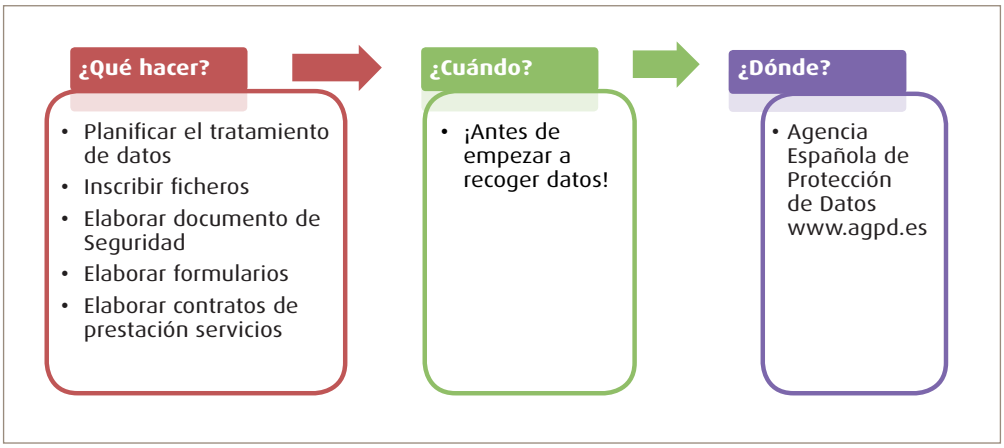
6E78BC9
6E78BC9
6E78BC9
6E78BC9

5

Inicio y cese de actividad en profesionales autónomos y responsables en las sociedades profesionales

Al iniciarse la actividad como psicólogo (Reglamento de trabajadores autónomos), hay algunas cuestiones importantes a tener en cuenta en materia de protección de datos[2].

Figura 5
Inicio de actividad



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

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

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

5.1 Planificar el tratamiento de datos

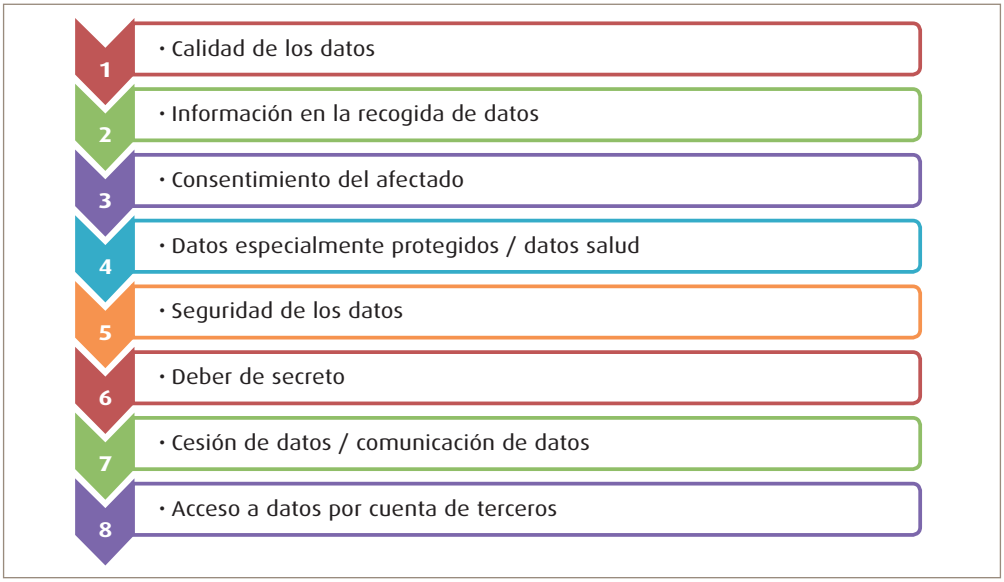
5.1.1 ¿Qué datos es necesario recoger y qué nivel de seguridad tienen?

Solo 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 a cumplir de acuerdo a la Ley de Protección de Datos.

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.

(2) Es fundamental conocer las principales obligaciones en relación a la legislación de protección de datos. Para ello además de este documento, se puede consultar la página web de la Agencia Española de Protección de Datos http://www.agpd.es/, ya que en la presente guía no se pueden desarrollar todos los aspectos con la amplitud que merecen.

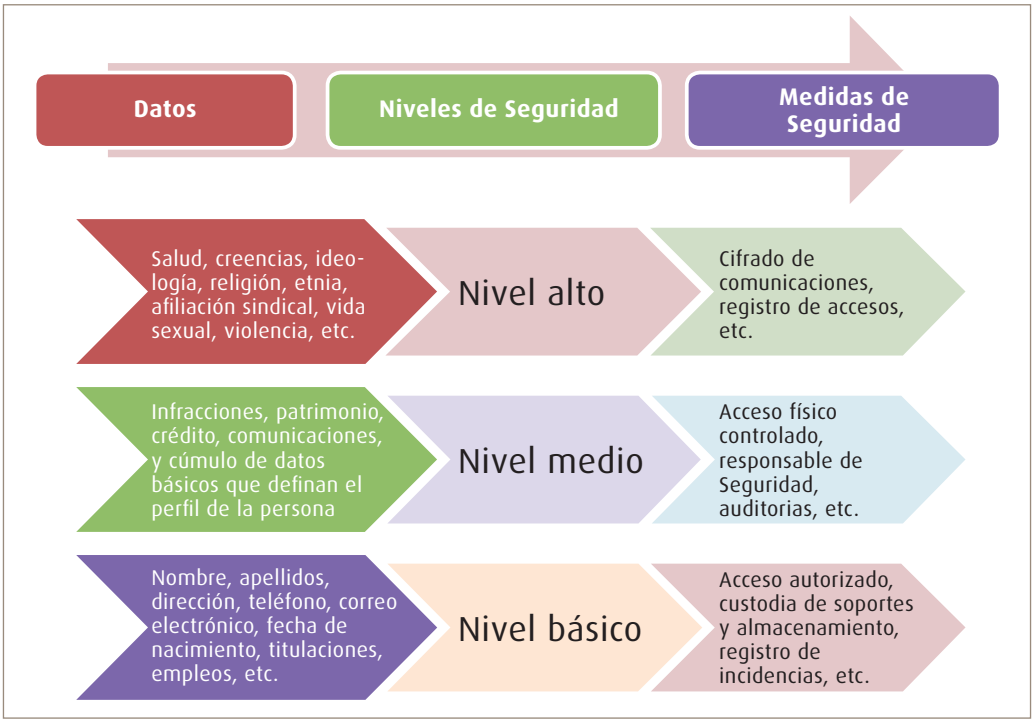
Figura 6
Principios de protección de datos



Los datos de carácter personal relativos a la salud, las creencias, la ideología, religión, origen étnico, 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 situaciones de violencia de género.

Los datos de nivel básico, pero que permiten obtener un perfil de las personas son considerados dentro de un nivel de seguridad medio, como también lo son los datos sobre infracciones

Figura 7
Niveles de seguridad



penales o administrativas, de solvencia patrimonial o de crédito, o si son de Administraciones tributarias, financieras, de la Seguridad Social, de mutuas de accidentes de trabajo, u operadores de servicios 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 de nacimiento, lugar de 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.

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**.

Figura 8
Niveles de seguridad

De los datos anteriormente mencionados como posibles en una historia clínica, solo deberán incluirse los datos que se consideren **relevantes y realmente necesarios** para la finalidad de la historia del paciente-cliente.

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

5.1.2 ¿Quién facilita los datos?

En esta fase, es necesario determinar cuál será el origen de los datos, se analizará 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 las correspondientes autorizaciones para el tratamiento adecuado 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.).

Esta definición también 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.

5.1.3 ¿Acceden terceros a los datos?

En relación al acceso a datos de terceros (contratos de prestación de servicios) se plantean las siguientes cuestiones:

¿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 las 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 realizarán.

El nuevo Reglamento Europeo General de Protección de Datos (RGPD) determina que el responsable del fichero debe elegir un encargado de tratamiento que ofrezca garantías suficientes para aplicar las medidas de seguridad exigidas por el nivel de seguridad del fichero.

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

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

El RGPD contiene obligaciones expresamente dirigidas a los encargados de tratamiento, como es mantener un registro de actividades de tratamiento.

¿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 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.

¿Qué debe incluir un contrato de prestación de servicios?

En el contrato se deben anexar las cláusulas referentes a protección de datos. Deberá hacerse referencia a lo siguiente:

- Tratamiento de los datos personales únicamente conforme a las instrucciones del responsable del fichero.
- Cumplimiento de las normas de seguridad que, de acuerdo a la normativa vigente, el responsable del fichero y el encargado del tratamiento están obligados a implantar.
- Destrucción de 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.

El nuevo Reglamento Europeo indica qué contenido se debe incluir en cualquier contrato de prestación de servicios, el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

La Agencia de Protección de Datos ha elaborado algunas directrices para elaborar los contratos de prestación de servicios en este periodo transitorio hasta mayo del 2018, en que será aplicable, momento en el que la Agencia facilitará modelos de clausulados oficiales.

5.1.4 ¿Se realizarán cesiones de datos a terceros?

También habrá que definir si se tienen que ceder datos a terceras personas, y si dicha cesión requiere el consentimiento o no. Como regla general, los datos solo 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 (como las procedentes de fuentes accesibles al público, al Defensor del Pueblo, del Menor, jueces, Ministerio fiscal, Tribunal de Cuentas o las relativas a datos de salud para solucionar emergencias, así como las realizadas entre Administraciones públicas en el ejercicio de sus competencias, o fines estadísticos, históricos, científicos anonimizados. Para más información sobre este aspecto se puede consultar el art. 11 de la LOPD. Es importante recordar que aun no necesitándose consentimiento, sí 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.

5.2 Otros aspectos a planificar del tratamiento de los datos

5.2.1 ¿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.
- 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.

El nuevo Reglamento Europeo (RGPD) añade requisitos adicionales en cuanto a la necesidad de informar :

- La base jurídica o legítima o legitimación del tratamiento.
- El plazo o criterios de conservación de la información.
- La existencia de decisiones automatizadas o elaboración de perfiles
- La previsión de transferencias a terceros países.
- El derecho a presentar una reclamación ante las autoridades de control.
- Los datos de contacto del Delegado de Protección de Datos, en su caso.

Si los datos no se obtienen directamente del propio interesado, habrá que informar de:

- El origen de los datos.
- La categoría de los datos.

La Agencia Española ha elaborado una guía para facilitar los cambios que supone el nuevo Reglamento, puedes consultarla aquí.

Al ser el responsable del fichero el que debe probar que ha cumplido con el deber de información, es necesario conservar el soporte que acredite su cumplimiento durante el tiempo que persista el tratamiento de los datos.

5.2.2 ¿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 deberá 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.

El sistema que se utilice deberá dejar huella del consentimiento, así como de las modificaciones realizadas por el usuario.

5.2.3 ¿Qué personas accederán a los datos y qué 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 tendrán. Por ejemplo, el profesional que realiza la intervención psi-

cológica necesitará acceder a la historia clínica completa, pero el personal administrativo solo 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 solo a los datos que necesite para su trabajo, siempre teniendo en cuenta los principios de protección de datos.

5.3 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-clientes atendidos. 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.

5.3.1 ¿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.

Es necesario cumplimentar un formulario desde la web de la AEPD. Para ello basta con seguir los pasos indicados en el asistente para notificación de ficheros –una aplicación que guía la introducción de datos– en el apartado CANAL DEL RESPONSABLE, opción **Acceso al Servicio Electrónico NOTA**.

Figura 9
Inscripción de fichero

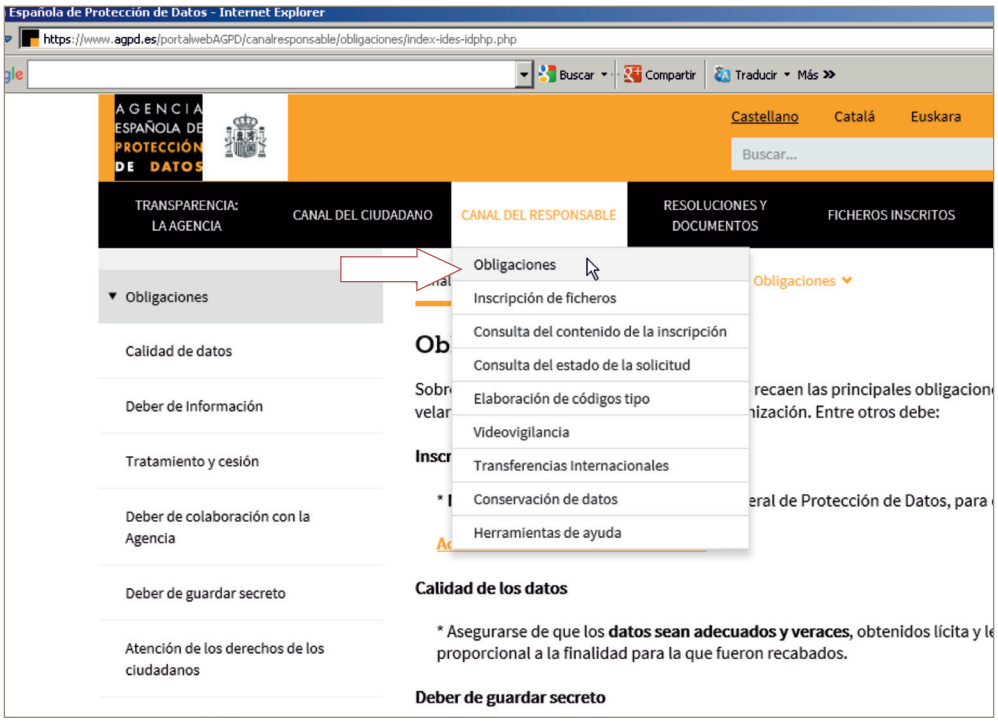


Figura 10
Inscripción de fichero

Una vez leída la información de las pantallas de introducción, aparece otra pantalla con dos opciones, se seleccionará la opción «*Iniciar Nueva Notificación*» (siempre es posible volver a la notificación si no se termina el proceso con la opción «*Reanudar una notificación*»).

Figura 11
Inscripción de ficheros

Al seleccionar «*Iniciar Nueva Notificación*» nos mostrará dos opciones, «titularidad pública» y «titularidad privada».

En nuestro caso se marcará la opción «**Titularidad privada**», y se elegirá el modo de presentación que se desee, puede ser con certificado electrónico o, en caso de no disponer de él, seleccionando el modo sin certificado electrónico.

Figura 12
Inscripción de fichero

Una vez seleccionado el tipo y modo de envío de la notificación, aparecerá la pantalla desde la que se accede al trámite.

Figura 13
Inscripción de fichero

En la misma página de la Agencia Española de Protección de Datos se puede consultar una Guía rápida, para resolver las dudas que surjan en el proceso de notificación del fichero.

Según se vayan rellenando casillas se irán desplegando más apartados con información a cumplimentar.

Para el caso de la notificación del fichero «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 al caso particular de cada profesional, puede facilitar el proceso de notificación del fichero.

Figura 14
Inscripción de fichero

Al finalizar de cumplimentar el formulario según la opción que se haya escogido en el inicio, habrá que enviar la declaración a la AEPD por una de estas dos vías:

- Sin certificado electrónico

Si se ha escogido esta 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 enviará la hoja de solicitud que confirma que la notificación ha sido enviada correctamente. En esta 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 enviarla a la AEPD c/Jorge Juan 6, 28001 Madrid. También es posible entregarla en la sede de la Agencia de Protección de Datos o cualquier registro público.

- Con certificado electrónico

Si se dispone de certificado digital, una vez cumplimentada la notificación y la hoja de solicitud, se finalizará el formulario y se firmará electrónicamente siguiendo las instrucciones de la aplicación.

5.4 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 debe cumplir en un tratamiento de datos para garantizar la seguridad y confidencialidad de estos. 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.

5.4.1 ¿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, 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 Española de Protección de Datos.

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

5.4.2 ¿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.

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 (si se ha contratado 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.
5. Procedimientos de notificación, gestión y respuesta a incidencias.
6. Procedimientos de realización de copias de respaldo y de recuperación de los datos.
7. Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para su destrucción.
8. 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.

5.4.3 ¿Cómo se conservarán los datos y qué medidas 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 según el sistema de tratamiento utilizado para almacenar los datos.

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.

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

Tabla 1
Medidas de seguridad

MEDIDAS	FICHERO NO AUT.	FICHERO AUT.
1. Documento de seguridad (cualquier nivel de seguridad)	Sí	Sí
2. Responsable de seguridad	Sí (medio y alto)	Sí (medio y alto)
3. Funciones y obligaciones del personal (cualquier nivel de seguridad)	Sí	Sí
4. Registro de incidencias (cualquier nivel de seguridad)	Sí	Sí

Medidas de seguridad

MEDIDAS	FICHERO NO AUT.	FICHERO AUT.
5. Control de acceso (cualquier nivel de seguridad)	Sí	Sí
6. Registro de acceso lógico/registro de acceso de documentación	Sí (alto)	Si (alto)
7. Identificación y autenticación (cualquier nivel de seguridad)	No	Sí
8. Criterios de archivo (cualquier nivel de seguridad)	Sí	No
9. Control de acceso físico/almacenamiento información	Sí (medio y alto)	Sí (medio y alto)
10. Copias de respaldo y recuperación (cualquier nivel de seguridad)	No	Sí
11. Dispositivos de almacenamiento (cualquier nivel de seguridad)	Sí	No
12. Custodia de soportes (cualquier nivel de seguridad)	Sí	No
13. Gestión de soportes y documentación (cualquier nivel de seguridad)	Sí	Sí
14. Auditoría periódica (nivel medio y alto)	Sí	Sí
15. Copia o reproducción (nivel alto)	Sí (nivel alto)	No
16. Distribución de soportes/traslado de documentación (nivel alto)	Sí (nivel alto)	Sí (nivel alto)
17. Telecomunicación (nivel alto)	No	Sí (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 de 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 controlar las medidas de seguridad del documento. No supone delegación de responsabilidad.

Registro de 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 de incidencia, momento de la incidencia, persona que lo detecta, persona que lo comunica. Además, en los ficheros con niveles medio o alto deberá consignarse:
  - procedimientos realizados de recuperación de los datos
  - personas que ejecutaron el proceso
  - los datos restaurados
  - y si ha sido un grabado manual.

Gestión y distribución de soportes y documentos.- Deberá 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 solo para los usuarios con acceso autorizado. Además:

- La salida de soportes y documentos (incluidos los adjuntos de los correos electrónicos) deberá ser autorizada por el responsable del fichero, o encontrarse la persona que lo realiza debidamente autorizada 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:
  - el tipo de documento o soporte,
  - la fecha y hora,
  - el emisor,
  - el tipo de información que contienen,
  - la forma de envío,
  - 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 adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido.
- La eliminación de cualquier documento o soporte deberá realizarse evitando el acceso a esta o su recuperación posterior.

Copias de respaldo y recuperación.- Se establecerán procedimientos de:

- Copias de seguridad (mínimo, semanales, excepto que no se hubieran producido cambios). La generación de copias o la reproducción de los documentos solo podrá ser realizada por personal autorizado en el documento de seguridad, si son de nivel alto. En el caso 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 estas o su recuperación posterior.
- Recuperación de los datos, que garantice 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.

Auditorías bienales.- 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 Española de Protección de Datos.

El informe deberá dictaminar sobre las medidas de seguridad y controles, identificando deficiencias y proponer medidas correctoras o complementarias necesarias.

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

Control acceso.- 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:
- usuario,
- fecha y hora,
- fichero accedido,
- tipo de acceso,
- y si ha sido autorizado o denegado.

El período mínimo de conservación de los datos será de dos años.

El responsable de seguridad deberá controlar el registro de accesos y revisarlo mensualmente y elaborará un informe de los servicios y problemas detectados.

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 establecerá una periodicidad para cambiar las contraseñas, no superior a un año. Además, en ficheros con nivel medio o 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. La 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, se presentan 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 (véase píe de página 12). Como pauta, debe aplicarse el criterio previsto en la 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 registrado 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 mecanismos 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. Estas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos. De no poder cumplirse estas deberán implantarse medidas alternativas, motivándolo en el documento de seguridad.

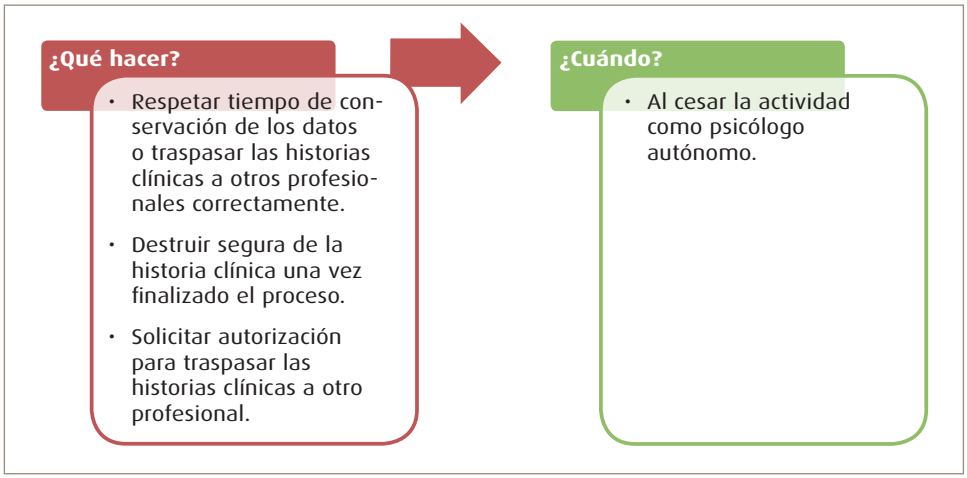
5.4.4 ¿Qué medidas técnicas se han de aplicar a los ordenadores?

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 exponga en su descripción técnica el nivel de seguridad que permita alcanzar (básico, medio o alto). Para la historia clínica se requiere que pueda alcanzar un **nivel alto**.

5.5 Cuestiones a resolver en el momento de cese la actividad como Responsable del fichero

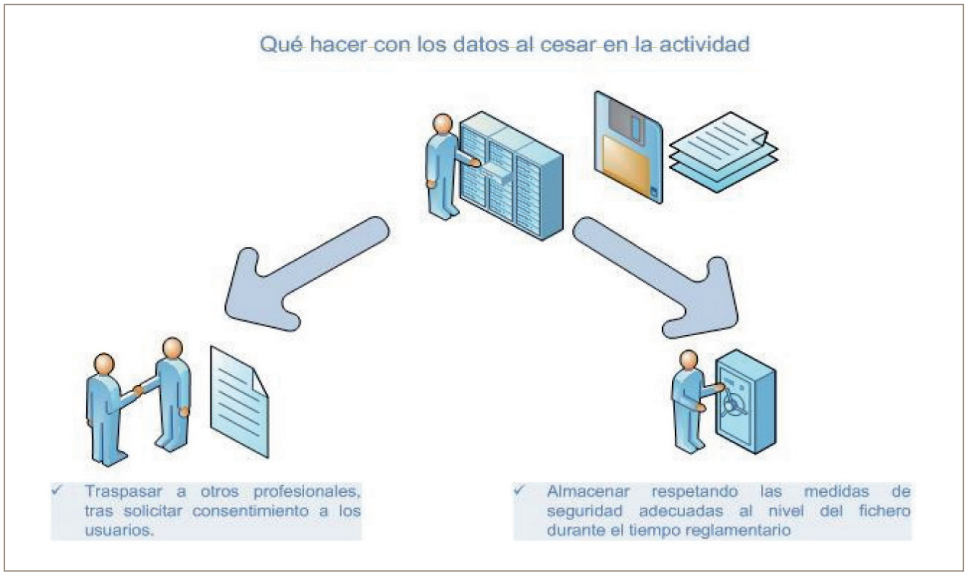
Figura 15
Cese de actividad por cuenta propia



5.5.1 ¿Cuánto 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.

Figura 16
Cese de actividad por Cuenta Propia



Dicha ley determina que se deberá conservar la historia clínica por un periodo de al menos cinco 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. 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.

5.5.2 ¿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.

5.5.3 ¿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.

6

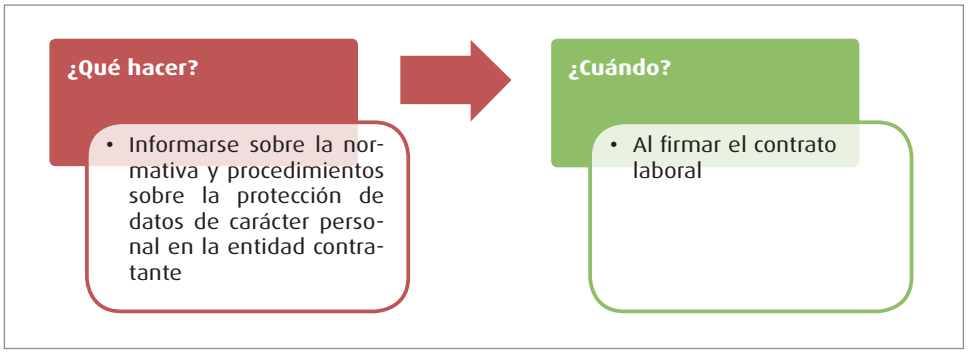
Inicio y cese de actividad de profesionales por cuenta ajena y autónomos con contrato de prestación de servicios

Tanto en el caso del profesional por cuenta ajena como en el del autónomo con contrato de prestación de servicios, el responsable del fichero es la persona que contrata, pero sí 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.

6.1 Profesional por cuenta ajena

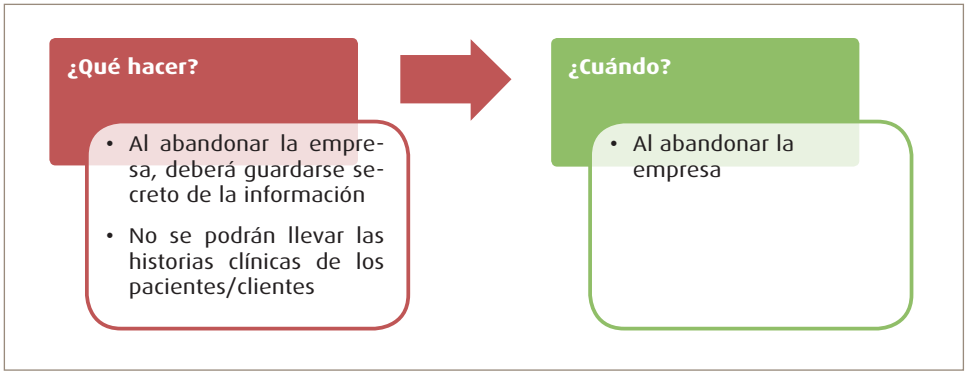
La firma del contrato es el momento de solicitar información sobre todos los aspectos en materia de protección de datos. Se deberá solicitar al responsable del fichero, para tener clara la actuación en cada momento, evitando dudas e improvisaciones, puede ser que el responsable solicite que se firme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

Figura 17
Inicio de la actividad por cuenta ajena



Al trabajar por cuenta ajena, los profesionales tienen un contrato laboral con una empresa o sociedad. Tienen por tanto una relación de dependencia y existe una relación laboral con la empresa, que es la que 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. Si el paciente quisiera seguir con el profesional, deberá solicitar su historia clínica y facilitársela directamente al profesional que abandona la empresa.

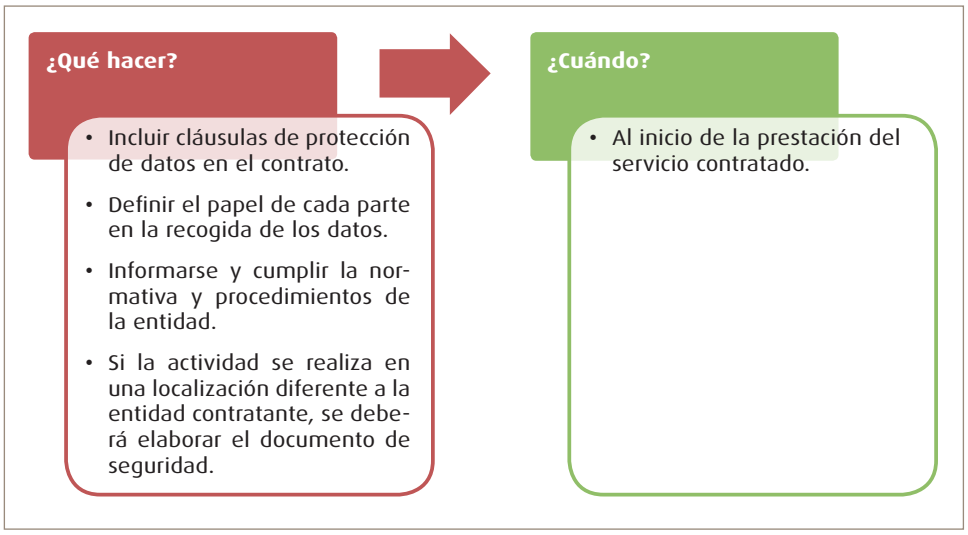
Figura 18
Cese de la actividad por cuenta ajena



6.2 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 claros todos los aspectos en materia de protección de datos.

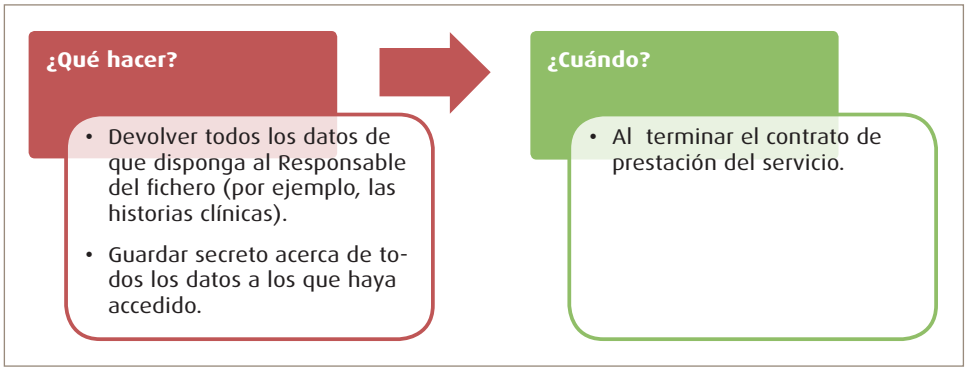
Figura 19
Inicio de actividad con contrato de prestación de servicios



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 este. Si los servicios se prestan en los locales del responsable del fichero, en el documento de seguridad de este 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 de este e incorporando las medidas de seguridad a implantar según el nivel de seguridad del fichero.

Figura 20
Cese de prestación del servicio contratado



En el momento del cese de la prestación del servicio contratado, se deberán devolver todos los datos de que se disponga (las historias clínicas, por ejemplo), y si algún paciente quisiera seguir el tratamiento con el profesional, deberá ser el propio paciente/cliente quien solicite al responsable del fichero una copia de su historia clínica y se la facilitará con posterioridad al profesional. En ningún caso, podría disponer el profesional de otra manera de la historia clínica ya que es responsabilidad del responsable del fichero.

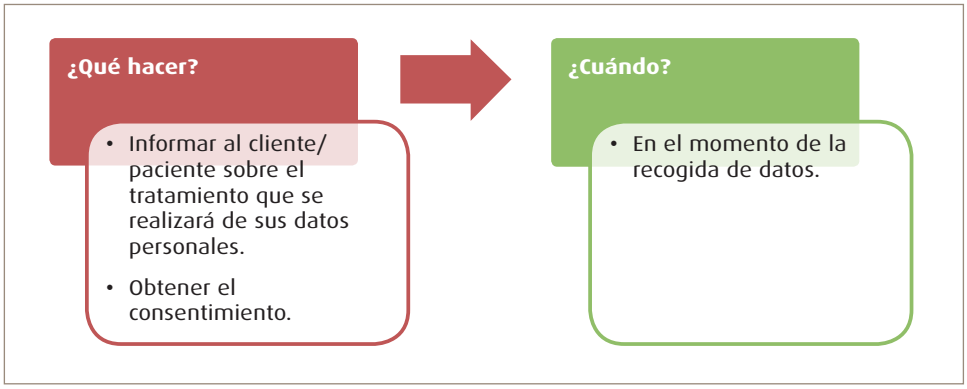
Como se ha visto, las cuestiones a abordar al inicio y al cese de la actividad sí que varían mucho dependiendo de la forma de ejercicio, sin embargo en el resto de fases de una intervención psicológica los aspectos a tener en cuenta son similares. A continuación se verá cómo realizar un tratamiento adecuado de los datos en el resto de fases de la intervención.

7

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 han planificado.

Figura 21
Entrevista inicial

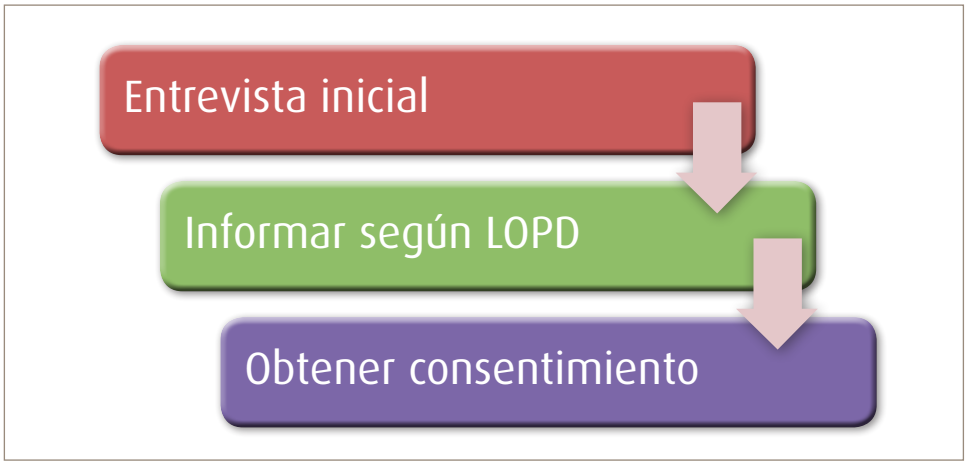


7.1 Información sobre el tratamiento de los datos y obtención del consentimiento

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 nota informativa informando sobre el tratamiento de los datos. 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, solo será necesario 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

Figura 22
Entrevista inicial



gestionar las citas, no podemos utilizar ese dato para enviar publicidad, deberá pedirse permiso de forma concreta para ese uso.

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.

7.2 Consentimiento de menores de edad

El Real Decreto 1720/2007 de desarrollo de la LOPD, indica que en 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 en 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 pueden recabar datos que permitan obtener información sobre los demás miembros del grupo familiar sin el consentimiento de los titulares de los datos, aunque sí 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.

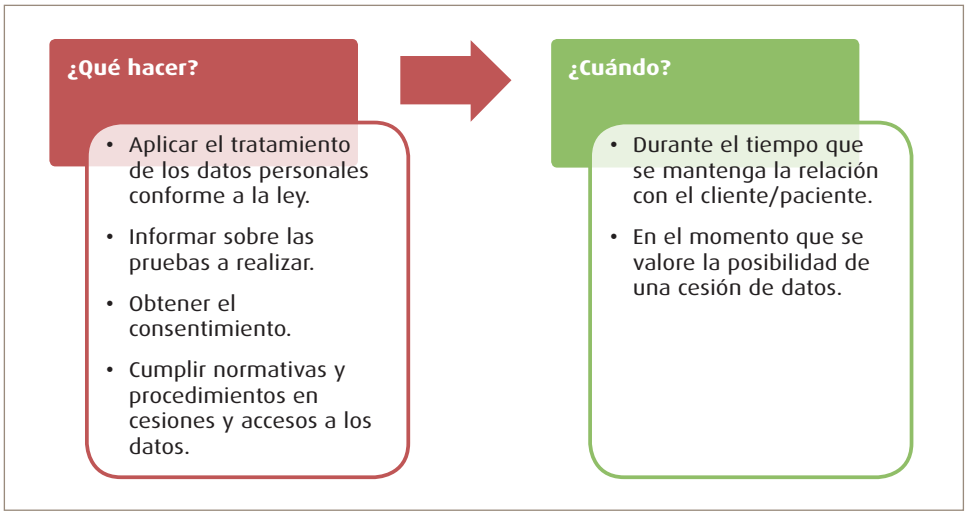
6E78BC9
6E78BC9
6E78BC9
6E78BC9

8

Evaluación psicológica y derivación de pacientes

Durante la evaluación psicológica, hay que realizar un tratamiento adecuado según la normativa de protección de datos. Además, hay que prestar particular atención a los siguientes aspectos:

Figura 23
Evaluación psicológica



8.1 ¿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 legalmente establecidas en función de la edad.

En el caso de evaluación de un menor, se debe informar a todas las partes con patria potestad.

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

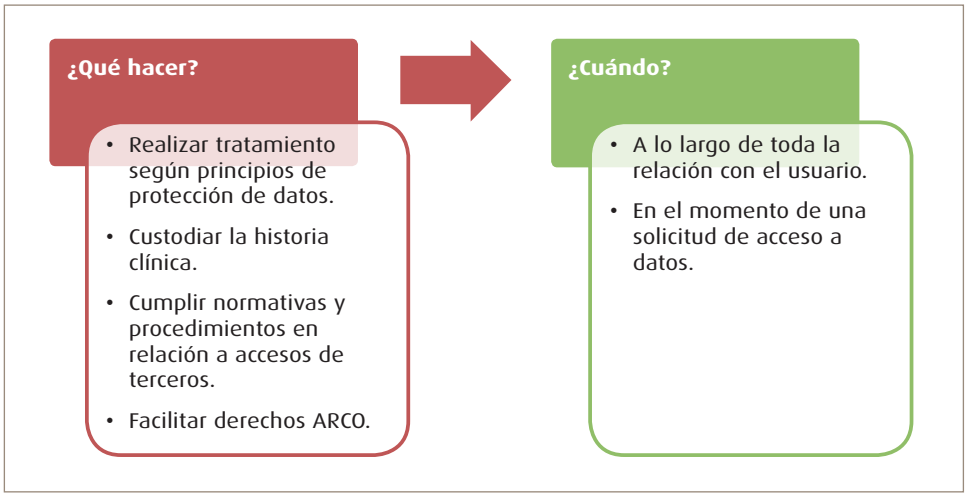
Tras la evaluación psicológica se puede concluir que es más conveniente que la intervención la realice otro profesional. Si es necesario facilitar datos sobre el paciente/cliente, se deberá informar al paciente y solicitar su consentimiento para facilitar dichos datos, o que sea el propio paciente/cliente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

9

Intervención psicológica

El tratamiento de los datos en la fase de intervención, se deber realizar respetando los principios de protección de datos y cumpliendo con todas las medidas de seguridad que establece la legislación.

Figura 24
Intervención psicológica



9.1 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.

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.

Por otro lado también en conveniente guardar de forma separada las anotaciones personales del psicólogo, ya que no pertenecen a la historia clínica.

9.2 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 este. 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 II se puede encontrar un modelo de cláusula de confidencialidad.

La historia clínica, al contener datos especialmente delicados, necesita un especial cuidado para garantizar su confidencialidad. Hay que asegurar que solo podrán acceder a los datos las personas autorizadas. Para ello, además de implantar las 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.

9.3 Derechos de acceso, rectificación y cancelación de los datos

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 guardarlos aparte si no se desea que formen parte de la historia clínica, ya que luego puede resultar más complejo tratar de separarlos si el paciente/cliente 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 de la petición de acceso a la información).

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 hace menos de 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 ha de rea-

lizarse y deberá ir acompañada de la documentación justificativa de lo solicitado. La solicitud debe resolverse en el plazo de 10 días a contar desde su recepción.

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 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 solo por el afectado, pero puede ejercerlos a través de un representante voluntario, expresamente designado para ello. En este caso deberá constar claramente acreditada la identidad del representado mediante presentación del DNI y la autorización conferida por aquel.

9.3.1 ¿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 en el Anexo II.

9.3.2 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»*, según indica el artículo 13 del reglamento de la LOPD.

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

Pacientes/clientes con dieciséis años cumplidos o emancipados

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

Pacientes/clientes 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/clientes 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 sus posibilidades de comprensión.

9.3.3 Derechos de acceso de familiares y terceras personas

Los familiares pueden acceder a la historia clínica si el paciente/cliente lo autoriza de forma expresa o tácita, por tanto ningún familiar puede acceder a la información del paciente/cliente 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 sí se podrá poner en conocimiento de personas vinculadas por razones familiares o de hecho.

9.3.4 Derechos de acceso a la historia clínica de una persona fallecida

En este caso se podrán facilitar los datos a personas vinculadas al paciente/cliente 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 las anotaciones subjetivas de los profesionales, ni las facilitadas por terceros.

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

9.3.5 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.

9.3.6 Derecho de acceso a órganos judiciales, Defensor del Pueblo, Defensor del Menor

Deberá facilitarse tan solo los datos estrictamente solicitados. Los jueces deberán limitar su petición de 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/cliente, ya que es una de las excepciones indicadas en la LOPD a dicha exigencia. En el artículo 11.2 d) de la LOPD, se 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».

9.3.7 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 solo

se deberá dar acceso a los que resulten necesarios, y solo para los fines de una investigación concreta.

9.4 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 solo la información que sea relevante y pertinente para la finalidad del informe. Los informes no deben ser utilizados para ninguna finalidad diferente a aquella para la que se recogieron los datos. En este enlace se pueden consultar los criterios generales que debe cumplir un informe psicológico.

9.4.1 ¿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 fundamentados y contrastados. Así mismo, no deben incluirse datos excesivos o no pertinentes a la finalidad del informe (por ejemplo en un informe pericial habría que dar respuesta al objeto de la pericia).

9.4.2 ¿Quién puede tener acceso a los informes?

Solo debe tener acceso a un informe la persona que lo ha solicitado. 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 tienen 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 este el informe, sin perjuicio del derecho a conocer el contenido 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 informar de la parte correspondiente a sus declaraciones o sus aportaciones en pruebas psicológicas.

9.4.3 ¿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.

En caso de realizarse la entrega del informe a través de telecomunicación, deberán 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.

9.4.4 Confidencialidad en un informe pericial

En el caso de informe pericial, obviamente se inició 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 solo 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)*, en este tipo de evaluación el perito debe informar de la limitación de la confidencialidad a la persona a la que se está evaluando y de que la información será utilizada para una evaluación forense.

6E78BC9
6E78BC9
6E78BC9
6E78BC9

10

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 su elaboración.

- 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 desarrollan todas las medidas de seguridad a implantar en los ficheros (tanto técnicas como organizativas, y 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: Thompson.

  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.

  Además, los colegiados cuentan en el Colegio Oficial de Psicólogos de Madrid con un servicio de asesoramiento sobre protección de datos, Lola Manzano, protecciondedatos@cop.es, teléfono 91 541 99 99.

11

Referencias bibliográficas

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

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

Agencia Española de Protección de Datos. (2017). Guía Rápida Notificación de ficheros. Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/documentacion/common/pdfs/Guia_rapida_NOTA.pdf

Agencia Española de Protección de Datos. (2017). Guía del Reglamento General de Protección de Datos para Responsables del Tratamiento. Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

Agencia Española de Protección de Datos. (2017). Guía del Reglamento General de Protección de Datos para Responsables del Tratamiento. Disponible en: https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

Agencia Española de Protección de Datos. (2017). Guía Responsables del Tratamiento. Disponible en: https://www.aepd.es/media/guias/guia-directrices-contratos.pdf

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. Madrid: autor.

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.

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

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm. 298, 14 de diciembre de 1999.

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 de enero de 2008.

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).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

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.

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 legibles, las advertencias a que se refiere el aparado anterior.

No será necesaria la información a que se refieren las letras b), c) y d) 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 de 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 estos 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.

Solo 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 apartados 2 y 3 de este Artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, 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.

Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en 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.

6E78BC9
6E78BC9
6E78BC9
6E78BC9

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 según LOPD. En este enlace se puede encontrar información sobre las recomendaciones para adaptar el siguiente texto a lo indicado en el Reglamento Europeo (aplicable a partir de mayo de 2018)

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 (ref. "tratamiento de datos"), indicando su nombre, dirección, petición, 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.

Modelo para dejar constancia escrita de que se ha informado al cliente/paciente para incluir en la historia clínica y como cartel explicativo en la consulta

---

El paciente ha sido informado de todos los extremos legalmente exigidos en materia de protección de datos.

Se informa a los pacientes que los datos que faciliten serán incorporados a su historia clínica, para su mejor asistencia, siendo los destinatarios de la información el psicólogo/psicólogos de este centro sanitario/consulta, implicados en su proceso asistencial.

El mantenimiento y custodia de su historia clínica es responsabilidad del (centro/sanitario), calle_____ nº_____, donde los afectados o interesados pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición, en su caso, conforme a lo legalmente previsto.

Modelo de cláusulas a incluir en un contrato de acceso a datos por terceros según LOPD. En este enlace se puede encontrar información sobre las recomendaciones para adaptar el siguiente texto a lo indicado en el Reglamento Europeo (aplicable a partir de mayo de 2018)

(Incluir el nombre de la persona contratada), como encargado del tratamiento, tal y como se define en la letra g) del artículo 3 de la 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 adoptará las medidas de seguridad que le correspondan según el Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD (incluir el nombre de la persona contratada), se compromete, en su caso, 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.

(Incluir el nombre de la persona contratada) declara expresamente que conoce quedar obligado 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. (Incluir el nombre de la persona contratada) se compromete explícitamente a formar e informar a su personal en las obligaciones que de tales normas dimanan.

(Incluir el nombre de la persona contratada) 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.

(Incluir el nombre de la persona contratada) aportará una memoria descriptiva de las medidas que adoptará para asegurar la confidencialidad e integridad de los datos manejados y de la documentación facilitada. Asimismo, deberá comunicar a (Incluir el nombre del responsable del fichero, contratista), 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 (Incluir el nombre de la persona contratada) 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 a (Incluir el nombre de la persona contratada) para el exclusivo fin de la realización de las tareas objeto de este contrato, quedando prohibido para (Incluir el nombre de la persona contratada) 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.

(Incluir el nombre de la persona contratada) se compromete a no dar información y datos proporcionados por (Incluir el nombre del responsable del fichero, contratista) para cualquier otro uso no previsto en el presente contrato. En particular, no proporcionará, sin autorización escrita de (Incluir el nombre del responsable del fichero, contratista), copia de los documentos o datos a terceras personas.

Todos los estudios y documentos elaborados durante la ejecución del presente contrato serán propiedad de (Incluir el nombre del responsable del fichero, contratista), quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello (Incluir el nombre de la persona contratada).

Específicamente, todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo del contrato, corresponden únicamente a (Incluir el nombre del responsable del fichero, contratista).

El resultado de las tareas realizadas, así como el soporte utilizado (papel, fichas, cd etc.) serán propiedad del (Incluir el nombre del responsable del fichero, contratista).

Modelo de 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 compromiso de confidencialidad

D./Dª_____,de profesión _____provisto/a de DNI_____, y con domicilio en (incluir dirección).

DECLARO:

1. Que presto mis servicios laborales/profesionales en el centro sanitario/consulta (incluir nombre centro).
2. Que, en el ejercicio de mis funciones, tengo acceso autorizado a datos de carácter personal y demás información confidencial a la que tengo acceso autorizado, en el ejercicio de mis funciones, así como el deber de guardarlos y, en general, a la adopción de las obligaciones y deberes relativos al tratamiento de datos personales, en virtud de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa vigente.
3. Que tengo conocimiento de que las obligaciones mencionadas anteriormente subsistirán aún después de finalizar mis relaciones con el centro sanitario/la consulta de referencia.
4. Que conozco la responsabilidad personal que podría derivarse frente al centro sanitario/la consulta y a sus pacientes, a los efectos de resarcir los daños y perjuicios que se pudieran ocasionar, derivados de un incumplimiento culpable de las obligaciones en materia de protección de datos de carácter personal propias de mi puesto de trabajo.

En_____, a _____

Fdo.:_____

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

D./Dª_____ provisto/a de DNI_____, y con domicilio en (incluir dirección).

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 (incluir dirección).

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 (incluir nombre de la entidad), 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_____ provisto/a de DNI_____, y con domicilio en (incluir dirección).

DECLARO: haber sido informado/a que mis datos personales serán tratados y quedarán incorporados en los ficheros del centro sanitario/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 médico/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 (incluir dirección), cuyo responsable es (incluir nombre del responsable).

Con la firma del presente escrito CONSIENTO de forma expresa que mis datos, cuando fuese necesario, puedan ser comunicados o cedidos a (Incluir nombre), como servicios sanitarios en general que complementan las actuaciones psicológicas 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 sanitarios en general, y son los siguientes: (incluir datos que se van a recoger).

La finalidad concreta que motiva la cesión o comunicación de datos es la siguiente: (incluir finalidad).

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 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.

En_____, a _____

Fdo.:_____

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 (incluir dirección), en nombre y por cuenta propia/en nombre y representación de (incluir nombre), con N.I.F./ 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 (Incluir nombre), con N.I.F./C.I.F._____

Ambas partes, de común acuerdo, convienen.

1. Que (incluir nombre) ha decidido cesar en su actividad profesional, por (indicar causa... jubilación, causas económicas), y como consecuencia de ello cede las historias clínicas de sus pacientes/clientes a (incluir nombre).
2. En tales circunstancias, el cesante ha procedido a notificar este hecho a todos sus pacientes/clientes, recabando su consentimiento expreso con carácter previo a este acto.
3. (Incluir nombre) se compromete a continuar con el seguimiento de las referidas historias clínicas o se ocupará de su archivo, al menos, durante el plazo legalmente establecido.
4. (Incluir nombre) 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 psicológicos, 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 (incluir dirección).

En_____, a _____

Fdo.:_____

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 (incluir dirección).

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

Por medio de este documento, CONSIENTO 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 (incluir nombre) 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 psicológicos, 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 (incluir dirección).

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 _____ Código 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____

Fdo.:_____

---

[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____

Fdo.:_____

[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____

Fdo.:_____

[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.

ANEXO III
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!

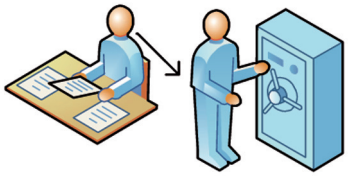
3

Pantallas y ordenadores:

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

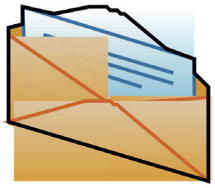


Al retirarse del puesto de trabajo:

Guardar el expediente en un cajón o armario bajo llave.

¡No dejar expedientes sobre la mesa!

5



Al enviar correos electrónicos

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 o contratar empresas con garantías LOPD.

ANEXO IV
Adaptación al Reglamento General Europeo de Protección de Datos

"Esta guía se elaboró siguiendo las directrices de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se trató de incluir la información sobre el Reglamento General de Protección de Datos disponible en el momento de elaboración de la guía, y se actualizará cuando se apruebe la nueva Ley orgánica de protección de datos que la sustituya. En el documento anexo a esta guía se ha tratado de facilitar la adaptación a lo indicado en el RGPD, comentando las principales novedades y obligaciones que conlleva."

Colegio Oficial de Psicólogos de Madrid
Cuesta de San Vicente, 4, 5º. 28008 Madrid
formacion.online@cop.es

Depósito Legal:

Nota aclaratoria: En beneficio de una mayor facilidad y claridad en la lectura y comprensión del texto, se utilizará un lenguaje igualitario y no sexista. No obstante, se explicita que, en el uso de términos como los profesionales, los estudiantes, los responsables, los psicólogos,... y cualquier otro que se encuentre en este documento, se hace referencia a hombres y mujeres, e incluye el masculino y el femenino.

1. Índice

1. ¿Qué es el Reglamento General Europeo de Protección de Datos?

El **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016** (Reglamento General de Protección de Datos o RGPD) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE **se debe empezar a aplicar partir de mayo de 2018.**

El RGPD trata de homogeneizar la normativa de protección de datos para todos los estados miembros de la Unión Europea. Al ser un Reglamento, es una norma de efecto directo que no requiere transposición a la legislación de cada estado, es decir, es de **aplicación directa**, pero que sí ofrece a los estados miembros cierta flexibilidad en algunos aspectos, como por ejemplo elegir la edad de consentimiento de los menores de edad, que queda abierta a los estados para decidir dentro del margen de 13 a 16 años o determinar quién está obligado a disponer de un Delegado de Protección de Datos DPD/DPO. Es por eso que la legislación española también va a cambiar para determinar los matices que considere oportunos.

El 24 de noviembre de 2017, el Congreso de los Diputados remitió a las Cortes Generales el **21/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (PLOPD)** que sustituirá a la actual LOPD, y que se prevé que entrará en vigor en **mayo de 2018** a la vez que el RGPD. Por ello, algunos aspectos están ya claros, pero otros dependerán de lo que indique la nueva legislación española.

En este **periodo transitorio** hasta mayo de 2018, hay que ir adaptándose y adoptando las medidas pertinentes para poder cumplir con la nueva legislación, sin dejar de cumplir la legislación actual, ya que seguirá vigente hasta esa fecha.

La Agencia Española de Protección de Datos ha creado un apartado donde reúne toda la información sobre el RGPD, y al que se puede acceder desde este **enlace**.

Desde el Colegio Oficial de Psicólogos de Madrid os mantendremos informados de cualquier cambio que se produzca hasta esa fecha.

2. ¿Qué cambios implica?

Los **principios y conceptos del RGPD** son en realidad muy parecidos a los de la anterior directiva y a los de la LOPD y el Real Decreto de aplicación de la LOPD (RDLOPD), por lo que si como Responsables del Tratamiento se está cumpliendo actualmente con la legislación vigente, se parte de una muy buena base para adaptarse al RGPD.

A. Principios de Protección de Datos

Los principios generales que rigen a la hora de interpretar y aplicar el RGPD son básicamente los mismos que en la LOPD y el RDLOPD (y que aparecen en la Guía de protección de datos personales en psicología: implicaciones y buenas prácticas) con alguna novedad, eso sí. Además varía la forma de nombrarlos o el encuadre que tienen en el Reglamento, y generan nuevas obligaciones, pero se refieren a lo mismo. Por ejemplo el "*Principio de calidad*" que se explica en la mencionada guía, en el nuevo Reglamento se desglosa en varios, el de *licitud, limitación de la finalidad, minimización, exactitud, limitación del plazo de conservación;* o el principio de *"Derecho de información",* ahora se incluye en el de *transparencia,* pero básicamente son los mismos conceptos que ya hemos visto.

A continuación podemos ver los Principios de protección de datos según el Reglamento General de Protección de Datos.

1. Principio de responsabilidad proactiva/Enfoque de riesgos
2. Principio de lealtad
3. Principio de transparencia o información
4. Principio de licitud y consentimiento
5. Principio de limitación de la finalidad en la recogida de datos
6. Principio de minimización
7. Principio de exactitud
8. Principio de limitación del plazo de conservación
9. Principio de seguridad de la información

No nos vamos a detener en todos los principios, puesto que se trata básicamente de lo que aparece en la Guía, pero sí vamos a ver con más detalle alguno por ser novedoso. En el siguiente apartado veremos las nuevas obligaciones que surgen de estos principios con la nueva legislación.

Dos conceptos nuevos que constituyen la **mayor innovación** del nuevo Reglamento Europeo, y que suponen un cambio importante en la forma de afrontar la protección de datos.

- El principio de responsabilidad proactiva
- El enfoque de riesgos

La Guía del Reglamento de Protección de Datos para Responsables de tratamiento editada por la Agencia de Protección de Datos ofrece estas definiciones de estos conceptos.

Principio de responsabilidad activa	Enfoque de riesgos
El RGPD describe este principio como la necesidad de que el responsable del tratamiento **aplique medidas técnicas y organizativas apropiadas** a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben **determinar de forma explícita la forma en que aplicarán las medidas** que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.	El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el **riesgo para los derechos y libertades** de las personas. De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten. La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

Otros cambios importantes son:

Tratamiento de datos de menores

El RGPD establece nuevas pautas para el tratamiento de datos de menores de edad, por ejemplo en el ámbito de los servicios de la sociedad de la información, como es el caso de las **redes sociales**, será legal el tratamiento siempre y cuando tengan más de **16 años**, pero permite a los estados miembros rebajar esa edad hasta los 13 años, en **el caso de España el proyecto de ley indica que se rebajará de los 14 años actuales a los 13 años**. Por debajo de esa edad se deberá solicitar consentimiento, que deberá ser verificable, se debe así mismo habilitar medios para verificar la edad del menor.

En el caso de los menores es particularmente importante que la información que se le facilite sea **claramente comprensible** para el menor.

Régimen sancionador

Las sanciones se incrementan de forma importante:

LOPD / RDLOPD	RGPD
▪ Entre 401,01 € y 60.101,21 € ▪ Entre 40.101,21 € y 300.00 € ▪ Entre 300.000€ y 601.012,01€ (Tras la modificación de la Ley de Economía Sostenible)	▪ No se hace mención a sanciones mínimas. ▪ Hasta 10.000.000€ o 2% como máximo del volumen de negocio anual global del ejercicio anterior (lo que resulte de mayor cuantía). ▪ Hasta 20.000.000€ o 4% como máximo del volumen de negocio anual global del ejercicio (lo que resulte de mayor cuantía).

El proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, (actualmente en las Cortes Generales) divide las **infracciones** en leves, graves y muy graves (se pueden consultar en los artículos 71-74 del proyecto de Ley).

El proyecto indica que:

> "Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo. 2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta: a) El carácter continuado de la infracción. b) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal. c) Los beneficios obtenidos como consecuencia de la comisión de la infracción. d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción. e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente."

Para más información sobre las el régimen sancionador se puede consultar el **RGPD** y lo relacionado con el proyecto de ley, en el siguiente **enlace**.

Como veis, ahora tenemos una mayor responsabilidad y requiere **no sólo cumplir con las obligaciones y medidas de seguridad** que nos indicaba el RD LOPD según el nivel de seguridad del fichero, sino que hay que **poder acreditar que se ha hecho todo lo posible para garantizar la seguridad del tratamiento**.

Luego veremos con más detenimiento cómo hacerlo, ahora vamos a ver las nuevas obligaciones con el **RGPD**

B. Principales obligaciones

En el cuadro comparamos las obligaciones que tenemos con la LOPD y las que tendremos con la nueva legislación

LOPD / RDLOPD	RGPD
▪ Inscripción de ficheros en la AEPD ▪ Deber de información ▪ Consentimiento para el tratamiento ▪ Contratos con terceros (encargados de tratamiento) ▪ Documento de seguridad e implantación de medidas de seguridad ▪ Facilitar derechos ARCO ▪ Auditoría bienal (nivel medio y alto)	▪ No inscripción de ficheros en AEPD, pero sí Inventario y registro de actividades de tratamiento ▪ Cambios en el deber de información, más aspectos a informar y formato en capas. ▪ Cambios en el deber de informar en los contratos con terceros y la responsabilidad de los encargados, garantizar la adecuación del encargado ▪ Nuevas formas de licitud del tratamiento ▪ Responsabilidad Proactiva: ✓ Privacidad desde el diseño y por defecto ✓ Análisis de riesgo y evaluaciones de impacto. ✓ Documentar medidas de seguridad ✓ Notificación de violaciones de seguridad a AEPD e interesados ✓ Delegado de protección de datos DPO/DPD ▪ ARCO más nuevos derechos, (limitación del tratamiento, portabilidad de los datos y derecho al olvido ▪ No auditoría bienal, pero sí cuando determine el responsable para garantizar seguridad.

3. ¿Entonces qué tengo que hacer?

A. Lista de verificación

Para que nos sirva de guía para repasar todos los cambios vamos a utilizar la lista de verificación que ofrece la Agencia Española de Protección de Datos en la Guía del Reglamento de Protección de Datos para Responsables de tratamiento, combinándolo con los cambios que hemos comentado en el apartado anterior.

Vamos a ir viendo **paso a paso** qué preguntas tenemos que hacernos para verificar si el tratamiento que ya estamos realizando se ajusta a lo que nos demanda el RGPD o si tenemos que realizar algún cambio y cómo hacerlo.

Inventario y registro de tratamiento

El primer paso será hacer un **inventario de los tratamientos de datos personales** que se realizan para **identificar las áreas de riesgo**, esto es, saber qué datos estamos tratando y cómo los estamos tratando y todos los riesgos que pueden afectar a la seguridad de los datos, para poder aplicar las medidas que les correspondan, las más adecuadas para nuestro tratamiento en concreto. Ya no nos sirve como con la legislación actual de protección de datos, únicamente aplicar las medidas de seguridad según el nivel de seguridad determinado por el tipo de datos (básico, medio y alto), según lo indicado por la LOPD y su reglamento de desarrollo, ahora somos nosotros los que determinamos **qué medidas son las más adecuadas** valorando todo lo relacionado con el tratamiento que hacemos. Nuestra responsabilidad será decidir, tras analizar todos los posibles riesgos, qué haremos para proteger el tratamiento y por supuesto tenemos que **poder acreditarlo ante la Agencia Española de Protección de Datos**, documentándolo.

Para realizar este inventario de tratamientos, si ya hemos inscrito nuestros ficheros, podemos utilizar la herramienta propuesta por la Agencia de Protección de Datos para facilitar la labor de los responsables de tratamiento, y **solicitar una copia de la información que facilitamos en su momento al inscribir los ficheros.** Esta información puede guiar la realización del inventario de tratamiento, y ayudarnos en el análisis de riesgos.

Podemos acceder a dicha herramienta desde este enlace. Si tenemos certificado electrónico nos facilitarán la información en formato electrónico (XML o Excel), si no lo tenemos nos pueden facilitar la información por correo postal.

El reglamento se centra más en las **actividades de tratamiento** que realizamos que en los ficheros. Estas **actividades de tratamiento** podrían asimilarse a lo que, con la actual legislación, llamamos **finalidades del fichero**. Antes notificábamos un fichero y explicábamos las finalidades para las que recogíamos los datos, con el nuevo reglamento el foco se pone en las actividades de tratamiento.

Con esa información y detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos podríamos empezar a elaborar el **inventario**.

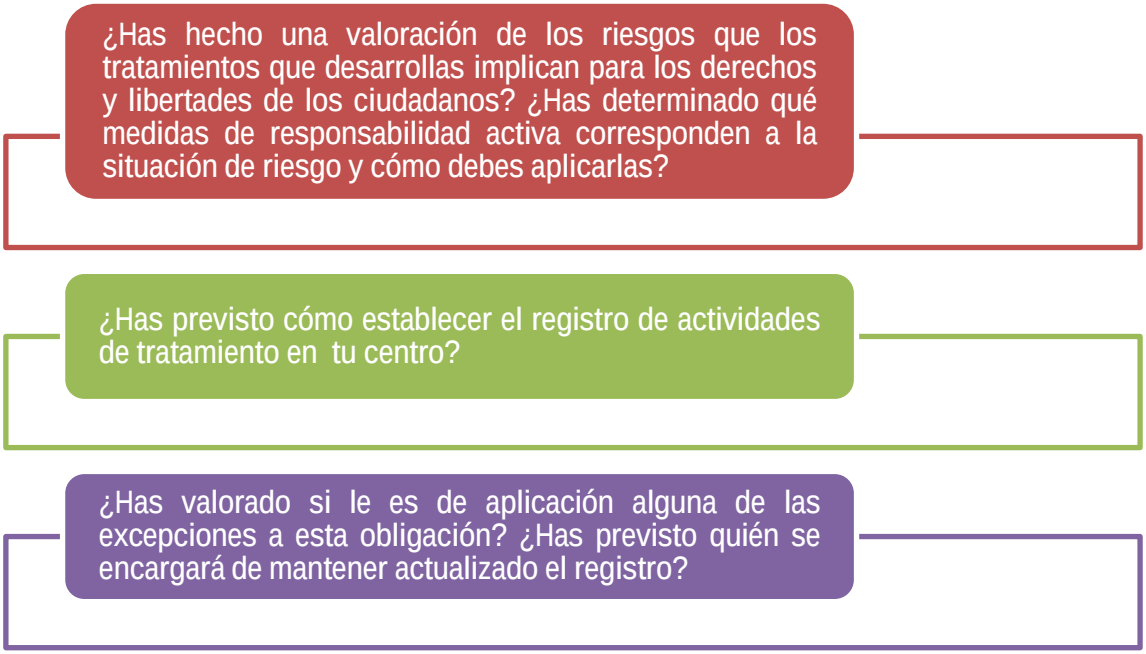
Si no hemos realizado ya la inscripción y por tanto no podemos descargar esa información, la *Guía del Reglamento de Protección de Datos para Responsables de tratamiento* propone para guiarnos, partir pensando las operaciones de tratamiento concretas vinculadas a una finalidad básica común de todas ellas (por ejemplo, "gestión de clientes", "gestión contable" o "gestión de recursos humanos y nóminas") o con arreglo a otros criterios distintos.

En este registro de actividades **el responsable debe** como mínimo:

- Describir qué datos recoge
- Con qué fin se tratan
- A quién o quiénes los comunica
- Si los transfiere a terceros países
- Qué medidas técnicas y organizativas aplica para preservar su seguridad, y cuándo podrá suprimirlos.
- En su caso, los datos de contacto del delegado de protección de datos

Para tratamientos muy sencillos, de escaso riesgo, que no implican datos sensibles como los de salud, se puede utilizarla la herramienta Facilita, pero en nuestro caso lo normal es que tengamos que hacer un análisis de riesgos, y por tanto no nos serviría esta aplicación. La Agencia pretende modificar la herramienta Facilita para que se pueda utilizar en casos más complejos que impliquen datos sensibles, pero de momento no puede utilizarse.

Las preguntas pertinentes en este momento son las siguientes



Nuevas formas de licitud del tratamiento

Al ver las obligaciones, conocimos que el RGPD contempla otras bases legales para tratar con datos de carácter personal distintas al consentimiento del interesado. Las bases legítimas son las siguientes.

- Consentimiento.
- Relación contractual.
- Intereses vitales del interesado o de otras personas.
- Obligación legal para el responsable.
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Hay que pensar por tanto cuál de ellas se adapta mejor al tipo de tratamientos que llevamos a cabo. Hay que tener en cuenta que aunque no se necesite consentimiento si por ejemplo la base jurídica es una relación contractual en la que es necesario tratar datos para prestar el servicio que ofrezcamos, **no dejamos de tener la obligación de informar, y de dejar constancia de haber realizado dicha comunicación.**

En el caso del **consentimiento** tiene que ser "**inequívoco**". Esto quiere decir que debe realizarse a través de una **manifestación del interesado o mediante una clara acción afirmativa**. A diferencia del Reglamento de Desarrollo de la LOPD, n**o se admiten formas de consentimiento tácito o por omisión**, ya que se basan en la inacción.

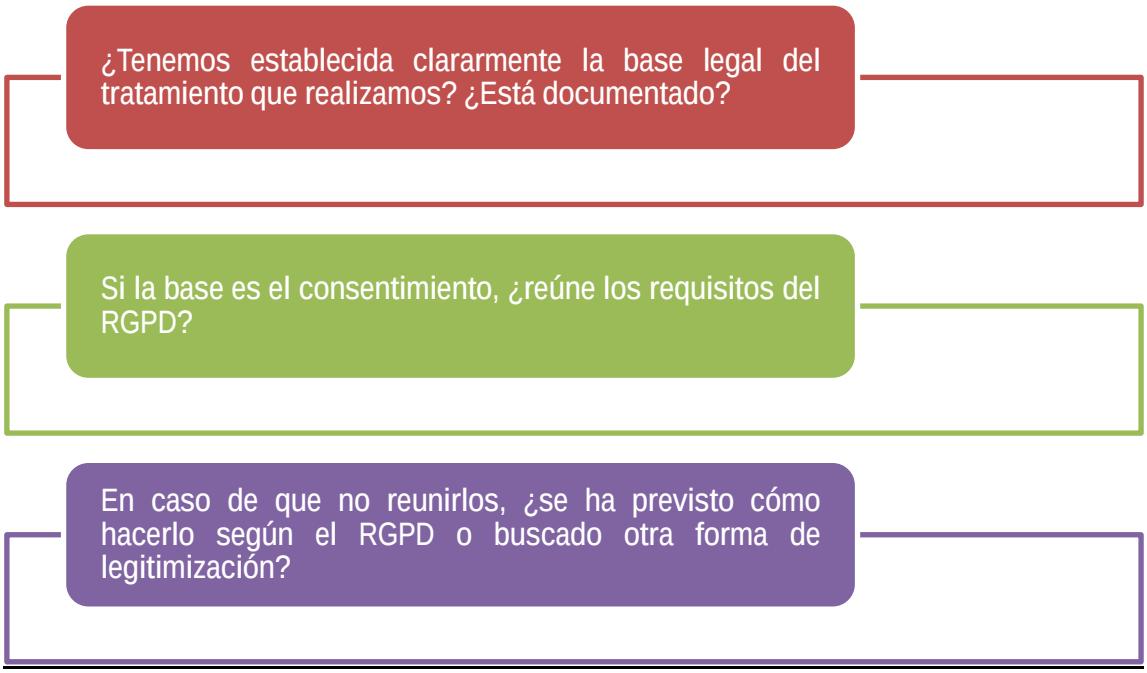
En algunos casos, como cuando el responsable trata los datos para elaborar perfiles, si trata datos sensibles o si realiza transferencias internacionales de datos, debe de ser además **explícito**.

El Considerando 32 del RGPD dice lo siguiente:

> "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.":

Si has estado recogiendo el consentimiento de esta forma, no hará falta hacer nada. Si no es así, habría que solicitarlo o buscar otra fuente de legitimación para tratar los datos.

En este momento debemos hacernos las siguientes preguntas



Cambios en la forma de informar

En la Guía de protección de datos personales en psicología: implicaciones y buenas prácticas) se indica que hasta ahora, 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.
- 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.

El nuevo Reglamento europeo (RGPD) añade **requisitos adicionales** en cuanto a la necesidad de informar:

- La base jurídica o legítima o legitimación del tratamiento.
- El plazo o criterios de conservación de la información.
- La existencia de decisiones automatizadas o elaboración de perfiles
- La previsión de transferencias a Terceros Países.
- El derecho a presentar una reclamación ante las Autoridades de control.

- Los datos de contacto del Delegado de Protección de Datos.

Si los datos no se obtienen directamente del propio interesado, habrá que informar de:

- El origen de los datos.
- La categoría de los datos.

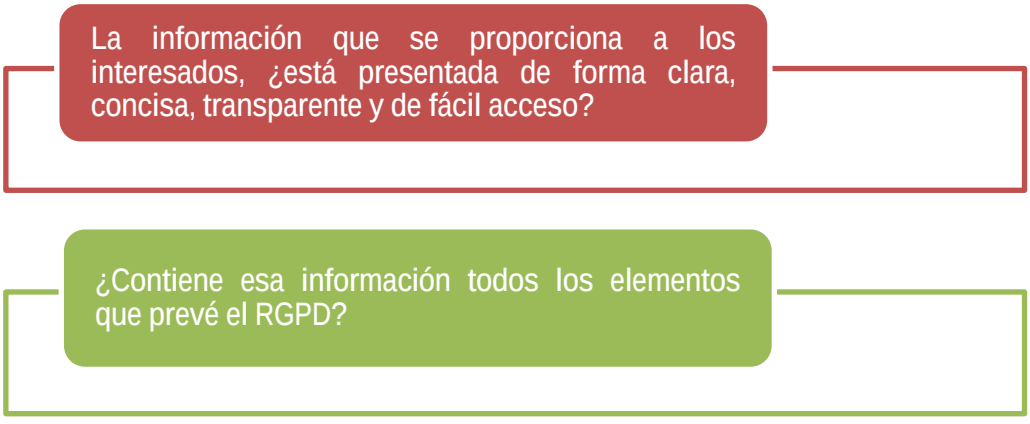
Al ser el responsable del fichero el que debe probar que ha cumplido con el deber información, es necesario **conservar el soporte que acredite su cumplimiento** durante el tiempo que persista el tratamiento de los datos.

El RGPD da **importancia a la forma de comunicar la información**, nos dice que debe facilitarse la información con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso, nada de fórmulas farragosas de difícil interpretación.

Las Autoridades de protección de datos proponen que se utilice un **formato de dos capas**, una primera capa con la **información básica** y otra en la que **ampliamos la información**. Proponen que se presente la información en formato de **tabla**, similar a la utilizada para presentar la información nutricional de los alimentos.

La Agencia Española de Protección de Datos ha elaborado una **Guía** para facilitar los cambios que supone el nuevo reglamento, y en la que se puede ver de forma detallada toda la información que hay que facilitar a los usuarios.

Las cuestiones que hay que plantearse en relación a este aspecto son los siguientes:



Cambios en la facilitación de derechos

En relación a los derechos a facilitar a los clientes/pacientes nos encontramos las siguientes **novedades**:

- La obligación de articular procedimientos que faciliten a los interesados ejercitar sus derechos por medios electrónicos y que puedan acreditar su ejercicio por el mismo medio.
- En caso de considerar que la solicitud de alguno de los derechos es infundado o excesivo, es el responsable el que debe demostrarlo si pretende que tenga un coste para el interesado para compensar los gastos que suponga al responsable facilitar el derecho. El importe que se cobre no puede implicar un ingreso adicional, pero si puede ser el importe del *verdadero coste de la tramitación de la solicitud.*
- Se debe contestar en el plazo de un mes. Se podría ampliar a dos meses cuando la solicitud sea especialmente compleja, y en ese caso se comunicará este aspecto dentro del primer mes. Antes había diferentes plazos según el derecho que se ejerciera, ahora es el mimo plazo (un mes para todos los derechos).
- Si se decide que no se va a atender a la solicitud, se deberá informar y motivar su negativa dentro del plazo de un mes.
- Se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento en todos los casos. En el caso de la historia clínica ya era así también con la anterior legislación.
- Los derechos se podrán atender facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.
- Se deben tomar las medidas oportunas para la identidad de quienes soliciten acceso y de quienes ejerzan los restantes derechos ARCO.
- Da la posibilidad al responsable que trate una gran cantidad de información sobre un interesado que se le especifique la información a que se refiere su solicitud de acceso.
- También da la posibilidad de contar con la colaboración de los encargados de tratamiento para atender al ejercicio de derechos de los interesados, eso sí deberá incluirse este aspecto en el contrato de encargo de tratamiento.

Además los **derechos ARCO** se han ampliado, pasan a ser los siguientes:

- El derecho de acceso
- El derecho de rectificación

- El derecho a supresión ampliado (en el contexto de internet sería el derecho al olvido)
- El derecho a la limitación del tratamiento
- El derecho a la portabilidad de datos
- El derecho de oposición (derecho a la exclusión voluntaria, por ejemplo oposición a que se usen con fines de prospección comercial o investigación o fines estadísticos)
- El derecho a no someterse a la toma de decisiones automatizadas, incluyendo la elaboración de perfiles.

Vamos a ver con más detalle en qué consisten algunos de estos nuevos derechos, o mejor dicho la ampliación de estos derechos:

- **Derecho al olvido.** El derecho al olvido, es nuestro derecho a impedir que se difunda información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia. Por ejemplo cuando una información ya está obsoleta se tiene el derecho a limitar la difusión universal e indiscriminada de esa información, de esos datos personales en los buscadores, incluso cuando en su momento la publicación original fuera legítima, como es el caso de datos publicados en boletines oficiales o informaciones de periódicos amparadas por las libertades de expresión o de información.

  Es una consecuencia de la aplicación del derecho de cancelación de la información, pero en internet, obliga además a los responsables que hayan hecho públicos los datos personales en internet a borrar la información y a adoptar medidas técnicas para informar a otros responsables de la solicitud del interesado de borrar su información personal.

  En este enlace se puede acceder a más información sobre el derecho al olvido.

- **Derecho a la limitación del tratamiento**. Se refiere a que, a petición del interesado, no se apliquen a los datos que ha facilitado alguna de las operaciones de tratamiento que principio correspondan, por ejemplo si se solicita ejercer el derecho de rectificación o de oposición y el responsable todavía no ha contestado, podemos solicitar que mientras no se decida, no se utilicen los datos para nada.

Según la Guía del Reglamento de Protección de Datos para Responsables de tratamiento, los casos en los que se puede solicitar el ejercicio de este derecho son los siguientes:

- ✓ Cuando el tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
- ✓ El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
- ✓ Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

- **Derecho a la portabilidad de los datos.** Es el derecho que puede ejercer un usuario, a solicitar una copia de todos los datos que se hayan facilitado. Esta copia se debe proporcionar al interesado en un formato estructurado, de uso común y lectura mecánica.

  El objeto es facilitar el traspaso de todos los datos de una persona de un responsable de tratamiento a otro, sería por ejemplo el caso de solicitar todos nuestros datos a una compañía telefónica para facilitárselos a otra compañía con la que vamos a contratar el servicio de telefonía. A no ser que no sea posible, los datos se traspasarán directamente de un responsable a otro, sin necesidad de que pasen por el propio interesado.

  Este derecho sólo puede ejercerse en estas circunstancias:

  - ✓ Cuando el tratamiento se efectúe por medios automatizados.
  - ✓ Cuando se base en el consentimiento o en un contrato.
  - ✓ Cuando se solicita en relación a datos que se haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

En este enlace se puede ampliar información sobre el derecho a la portabilidad de los datos y en este otro podéis encontrar preguntas frecuentes sobre el tema.

En relación a los derechos ARCO habrá que revisar los siguientes aspectos:

- ¿Dispones de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos?
- ¿Tienes establecidos procedimientos o mecanismos que te permitan verificar la identidad de quienes solicitan acceso o ejercen los demás derechos ARCO?
- ¿Pueden ejercerse los derechos por vía electrónica?
- ¿Tienes establecidos procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD?
- ¿Has valorado si sería necesaria la colaboración de los encargados para responder a las solicitudes de los interesados y, si es así, tienes previsto incluir esta colaboración en los contratos de encargo?
- ¿Tienes previstos mecanismos para atender a posibles ejercicios del derecho a la limitación del tratamiento, de forma que los datos afectados puedan ser conservados sin ser objeto de las operaciones de tratamiento que corresponderían?
- ¿Has valorado si los tratamientos de datos que realizas pueden ser objeto del derecho a la portabilidad? En caso afirmativo ¿has previsto procedimientos o mecanismos para poder atender a este derecho y proporcionar los datos al interesado (o a otro responsable) en un formato estructurado, de uso común y susceptible de lectura mecánica?

Relaciones responsable-encargado del tratamiento

Otro de los aspectos que cambian son los relacionados con la relación entre el responsable y el encargado de tratamiento.

Uno de los cambios es la obligación de los responsables de **seleccionar un encargado de tratamiento** que nos ofrezca garantías de que van aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento que realicen en nuestro nombre sea conforme con los requisitos del Reglamento.

Para seleccionar el responsable más adecuado, los responsables pueden valorar que los encargados estén **adheridos a códigos de conducta** o **certificados en el marco de los esquemas de certificación previstos por el RGPD**, lo que puede mostrar a las autoridades de control que estamos haciendo todo lo posible para garantizar un tratamiento seguro de los datos.

Además los encargados van a tener en algunos aspectos obligaciones propias que van más allá de las que tienen en el ámbito que los une al responsable y que pueden ser supervisadas separadamente por las autoridades de protección de datos.

Algunas de estas obligaciones son:

- Mantenimiento un registro de actividades de tratamiento.
- Determinar las medidas de seguridad más adecuadas aplicables a los tratamientos que realizan.
- Asignar un Delegado de Protección de Datos en los casos previstos por el RGPD.

Las relaciones entre el responsable y el encargado tienen que basarse en un **contrato o en un acto jurídico** que vincule al encargado respecto al responsable.

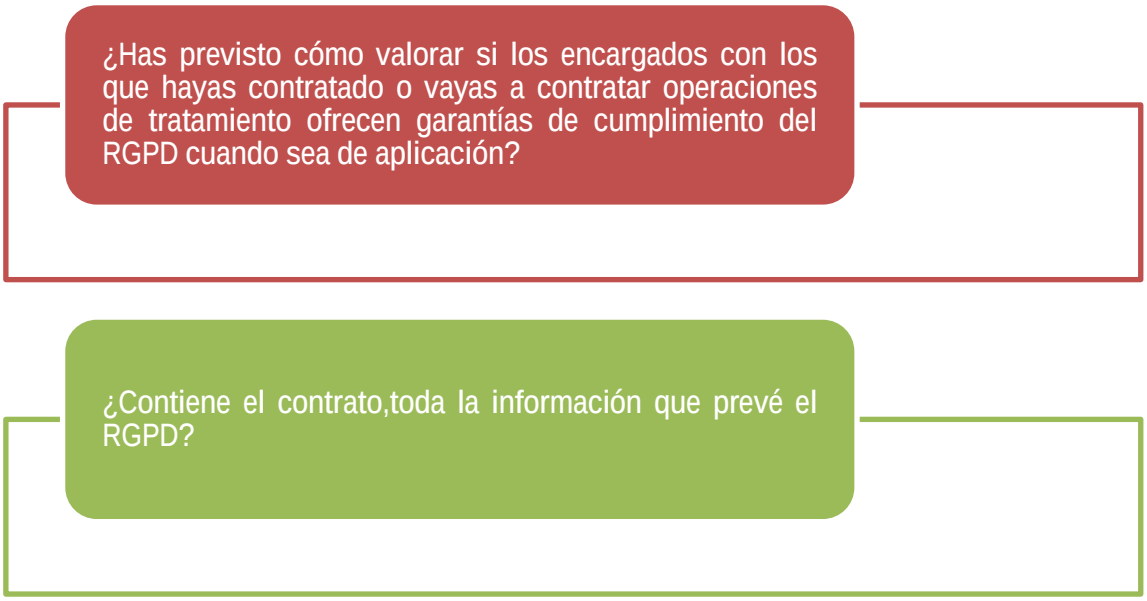
En el contrato debe incluirse información sobre lo siguiente:

- El objeto, duración, naturaleza y la finalidad del tratamientos
- El tipo de datos personales
- El tipo de categorías de interesados
- La obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
- Puede asistir al responsable en la atención al ejercicio de derechos de los interesados, si así se le encarga.

Es importante saber que **los contratos de encargo** concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 **deben modificarse y adaptarse** a estos requisitos.

En este enlace se puede consultar más información sobre la nueva relación encargado-responsable.

A continuación podemos ver algunas de las preguntas que nos tenemos que hacer en relación al encargado de tratamiento.



Protección de Datos desde el Diseño y por Defecto

A continuación vamos a ver otras cuestiones a tener en cuenta en relación a la responsabilidad proactiva, desde el diseño y por defecto.

Las medidas de seguridad se deben aplicar por el responsable con anterioridad a iniciar el tratamiento de datos, se debe empezar a pensar en todo lo relacionado con la protección de datos desde que se empieza un proyecto, desde que se diseña, y durante su desarrollo siempre que implique un tratamiento de datos de carácter personal.

B. Análisis de riesgo y evaluación de Impacto

Al principio del este anexo hablábamos de que el RGPD condiciona la adopción de medidas de seguridad, no en función del nivel de seguridad como hasta ahora indicaba la legislación actual, sino **en función del riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados**.

Hay que aplicar las medidas que después de evaluar los riesgos, nos garanticen que los tratamientos van a ser conformes a lo indicado por el reglamento y poder demostrarlo.

El RGPD determina que algunas medidas de seguridad, como la **evaluación de impacto**, por ejemplo, solo habrá que aplicarlas cuando tras un análisis de riesgos se determina que el tratamiento puede suponer un alto riesgo para los derechos y libertades de las personas. En otros casos las medidas se podrán modular según el tipo de riesgo y el nivel de riesgo que conlleve.

Por tanto es **obligatorio realizar una valoración del riesgo de los tratamientos** que realicen, para poder saber qué medidas hay que aplicar:

El tipo de análisis a realizar dependerá de los tipos, cantidad y variedad de tratamientos que se realicen, de la naturaleza de los datos, del número de interesados que pueden estar afectados.

No es lo mismo una gran organización que requiera por la complejidad del tratamiento que realice utilizar alguna de las metodologías de análisis existentes, como puede ser MAGERIT, que una empresa pequeña con tratamientos poco complejos que podrá realizar una análisis de riesgo sencillo, documentando lo básico, que puede consistir en pararse a pensar en el tratamiento. En esos casos puede ayudar la herramienta que ofrece la Agencia en su página para tratamientos de poco riesgo, Facilita.

Habría que reflexionar sobre aspectos como si se trata con datos sensibles, si se tratan datos de muchas personas, si se elaboran perfiles de personalidad, si se cruzan datos con otras fuentes, etc. Si tras reflexionar, se determinar que no se realizan tratamientos con un elevado riesgo, no deberá aplicar las medidas previstas en esos casos como es la evaluación de impacto.

En este enlace podéis ampliar información sobre análisis de riesgos.

¿Cuándo hay que realizar una evaluación de impacto?

Se debe realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha, de aquellos tratamientos que sea probable que conlleven un **alto riesgo** para los derechos y libertades de los interesados.

Estos son los supuestos que se puede considerar como tratamientos de alto riesgo:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan **efectos jurídicos** sobre los interesados o que **les afecten significativamente** de modo similar
- **Tratamientos a gran escala de datos sensibles** (datos que releven opiniones políticas, creencias religiosas, los relativos a salud o la vida sexual, datos biométricos y genéticos)
- **Observación sistemática a gran escala** de una zona de acceso público
- O siempre que se consideré que puede resultar un tratamiento de alto riesgo.

Para valorar si un tratamiento se realiza a gran escala debe tenerse en cuenta (según el Grupo del Artículo 29, en su designación de Delegados de Protección de Datos):

- El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población
- El volumen de datos y la variedad de datos tratados
- La duración o permanencia de la actividad de tratamiento
- La extensión geográfica de la actividad de tratamiento

Si se valora que el riesgo del tratamiento no va a poder mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable puede consultar con la Agencia.

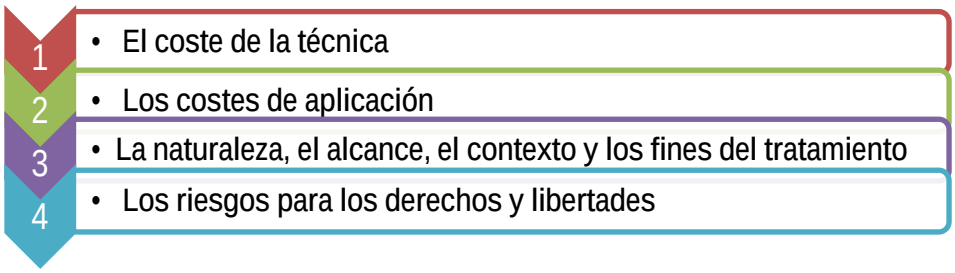
Para más información sobre **evaluaciones de impacto** se puede consultar la siguiente **Guía** editada por la Agencia Española de Protección de Datos.

Está previsto que la Agencia pueda elaborar listas de tratamientos en los que no se precisa evaluación de impacto.

Medidas de seguridad

En cuanto a las medidas de seguridad tanto técnicas como organizativas a implementar, habrá que decidirlas en función del nivel de seguridad que determinemos según los riesgos detectados en el análisis previo, que concluya que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado.

Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta:



En muchos casos vamos a tener que seguir aplicando las mismas medidas que indicaba el anterior Reglamento de protección de datos, puesto que coincidirá el nivel asignado con el anterior criterio marcado por la ley (básico, medio, alto), pero puede ser que tras realizar el análisis de riesgos, determinemos que es necesario completarlas con medidas adicionales, incluso podría darse el caso de poder prescindir de alguna.

Notificación de violaciones de seguridad de los datos

Cuando se produzca una violación o quiebra de la seguridad de los datos, el responsable tendrá que **notificarla a la autoridad de protección de datos competente**, a menos que se valore como improbable que dicha quiebra de la seguridad suponga un riesgo para los derechos y libertades de las personas afectadas y deberá realizarse a ser posible, dentro de las **72 horas siguientes** a que el responsable tenga constancia de ella y por supuesto se deberá dejar debidamente documentada en un registro interno.

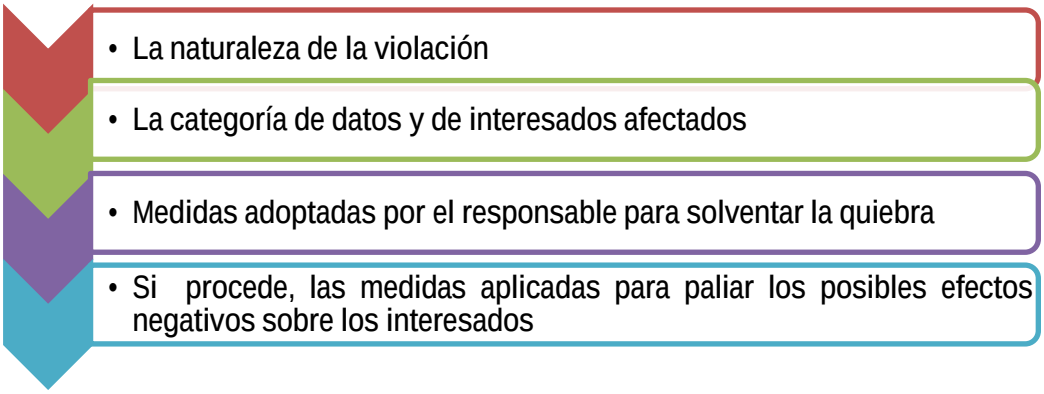
Si la situación fuera muy compleja y no se pudiera hacer en 72 horas, se podrá hacer de forma escalonada según se vaya teniendo más información; eso sí, si se retrasa habrá que explicar el motivo que ha ocasionado el retraso.

La Guía del Reglamento de Protección de Datos para Responsables de tratamiento explica así una violación de seguridad

Violación o quiebra de seguridad

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como "quiebras de seguridad", de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Cualquier incidente no es una violación de seguridad, hay que tener certeza de que se ha producido y tener conocimiento suficiente de su naturaleza y alcance antes de comunicarla a la Agencia. La mera sospecha de que ha existido una quiebra o saber que ha habido algún tipo de incidente sin más, no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones aún no sabemos si hay un riesgo para los derechos y libertades de los interesados. La notificación de contener como mínimo:



Si se valora que la quiebra de seguridad es tal que hay un alto riesgo para los derechos y libertades de las personas, **habrá que comunicárselo también a los afectados**, con el objetivo de que el afectado pueda reaccionar tan pronto como pueda, por ejemplo cambiando sus contraseñas.

Se considera que hay un alto riesgo de que la violación de seguridad ocasione daños importantes a los interesados cuando por ejemplo se desvele información confidencial, como contraseñas o participación en determinadas actividades o se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

Puede ser que la misma Agencia tras conocer la violación de seguridad, se ponga en contacto con el responsable para indicarle que comunique la quiebra de seguridad a los afectados.

No será necesario notificar a los interesados cuando:

- Se hayan tomado con anterioridad a la quiebra de seguridad medidas técnicas u organizativas que hagan ininteligibles los datos a terceros, por ejemplo cuando se hayan encriptado los datos.
- Cuando con posterioridad a la quiebra se aplican medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Si la notificación supone un esfuerzo desproporcionado, en ese caso se podría sustituir por una comunicación pública.

La Agencia habilitará un canal para realizar las notificaciones de violaciones de seguridad.

Delegado de Protección de Datos (DPD)

Delegado de protección de datos
Es una figura encargada de orientar, asesorar, así como supervisar al responsable de actividades de tratamiento sobre el cumplimiento del RGPD, también realizará labores de mediación entre los usuarios y el responsable y será la persona de contacto con las Autoridades de control, podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

El RGPD establece como obligatoria la figura del **Delegado de Protección de Datos** en los siguientes casos:

- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

El RGPD da la opción a los estados miembros de marcar la obligación de DPD en otros casos. En España el **Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (PLOPD)** en lo relativo a nuestro ámbito, añade la obligación **para los centros sanitarios.** Aún es un proyecto de ley y no será definitivo por tanto hasta mayo, pero de momento si está prevista esa obligación de delegado de protección de datos en los centros sanitarios.

Así mismo también da la posibilidad de que se opte por contar con un delegado de protección de datos de forma voluntaria, para garantizar el cumplimiento del reglamento y evitar también las elevadas sanciones que marca el nuevo reglamento.

Para más información sobre el DPD, su cualificación y funciones se pueden consultar el siguiente enlace.

Transferencias internacionales

Es muy importante comprobar que los servidores de datos de todos los servicios que utilicemos estén situados en territorio europeo, para así garantizar que cumplen con las medidas de seguridad exigidas por la legislación de protección de datos, pero es posible que se realice en países fuera del territorio europeo. Eso sí, no todos los países tienen la misma exigencia en este tema, por lo que habrá que verificar cuidadosamente a qué países va ir la información.

La Guía del Reglamento de Protección de Datos para Responsables de tratamiento indica los siguientes casos en los que es posible transferir datos fuera del Espacio Económico Europeo:

- A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales) sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado.
- Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino,
- Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

En este enlace se puede encontrar más información sobre transferencias internacionales.

Para verificar todos los aspectos relacionados a la protección de datos proactiva se puede reflexionar sobre los siguientes aspectos:

¿Ha revisado las medidas de seguridad que aplica a sus tratamientos a la luz de los resultados del análisis de riesgo de los mismos?

¿Considera que puede seguir aplicando las medidas de seguridad previstas en el Reglamento de la LOPD?

¿Ha valorado suficientemente la posibilidad de introducir medidas adicionales en función del tipo de tratamiento o del contexto en que se realiza?

Atendiendo al tipo de tratamientos que realiza, ¿ha establecido mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos?

¿Tiene previstas medidas de reacción frente a los diferentes tipos de quiebras de seguridad, incluidos los procedimientos para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados?

¿Ha establecido procedimientos para notificar las violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados?

¿Dispone de un registro o herramienta similar en que pueda documentar los incidentes de seguridad que se produzcan, aunque no sean notificados a las autoridades de protección de datos?

¿Ha valorado si los tratamientos que realiza requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados?

¿Dispone de una metodología para la realización de la Evaluación de Impacto?

Según el tipo de tratamiento que realiza y los resultados del análisis de riesgos previo, ¿tiene que nombrar un Delegado de Protección de Datos?

¿Ha establecido los criterios para seleccionar al Delegado de Protección de Datos y, en particular, para valorar sus cualificaciones profesionales y sus conocimientos?

El puesto de DPD tal y como está configurado en su organización, ¿respeta los requisitos de independencia en el ejercicio de las funciones, posición en el organigrama, ausencia de conflicto de intereses y disponibilidad de los recursos necesarios establecidos por el RGPD?

¿Ha hecho pública la designación del DPD y sus datos de contacto y los ha comunicado a la autoridad de protección de datos?

¿Ha establecido procedimientos para que los interesados contacten con el DPD?

6E78BC9
6E78BC9
6E78BC9
6E78BC9

Colegio Oficial de Psicólogos de Madrid

www.copmadrid.org