Unidad Didáctica 2

Identificación de ficheros

Contenido

1. Ficheros con datos de carácter personal

Se define como datos de carácter personal cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Así pues, en base a esta definición, el reglamento establece que un fichero que contenga datos de carácter personal sería todo conjunto organizado de datos de personas que pudieran ser identificables, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Pero atendiendo a los términos de esta definición se pueden establecer dos tipos fundamentales de ficheros, los automatizados y los manuales o no automatizados. Para realizar adecuadamente un plan de adecuación de la entidad a la LOPD se debe formar un equipo de trabajo interno, y organizar las funciones que cada miembro debe realizar. Antes de iniciar dicho plan se comprobará en qué grado la entidad cumple con la normativa. Para ello hay que tener muy clara la estructura de la entidad:

- Departamentos de la empresa.
- Sector de actividad.
- Estructura informática.
- Tipo de relación con los clientes, proveedores, distribuidores, colaboradores y empleados.

Ya que los datos personales son el principal objeto del plan de adecuación a la LOPD, para comenzar a localizar la información correspondiente se deben estudiar los aspectos que se citan a continuación:

- Procedencia de los datos.
- Tratamiento al que se someten dichos datos.
- Cancelación, bloqueo o salida de datos.

Es necesario revisar toda la documentación que esté relacionada con la protección de datos, o que contengan datos de carácter personal, de modo que se compruebe el grado de adecuación de la empresa a la LOPD.

Importante

Se debe asegurar de que toda la información que se detecte en la entidad relacionada con el tratamiento de datos personales sea identificada, valorada y analizada.

Es fundamental que las personas que se vayan a encargar del plan de adecuación a la LOPD se organicen para identificar y clasificar la documentación. Deberán analizar los siguientes documentos:

	DOCUMENTOS CON BASE JURÍDICA
Contratos	Con empleados.
	Con clientes.
	Con colaboradores, distribuidores, proveedores, trabajadores autónomos o procedentes de una ETT.
	Con el encargado del tratamiento de datos.
Cláusulas	De información.
	De garantía de los derechos.

DOCUMENTOS CON BASE ORGANIZATIVA
Políticas de privacidad.
Respuesta a los derechos de los afectados.
Notificaciones ya realizadas al RGPD.

DOCUMENTOS O INFORMACIÓN TÉCNICA
Sistemas.
Procedimientos de Seguridad.
Comprobar la existencia del Documento de Seguridad.
Informes de Auditoría.

Una vez se haya recopilado toda la información se tendrán en cuenta solo aquellos documentos que incidan en la protección de datos, o que contengan datos de carácter personal.

El siguiente paso será clasificar toda la documentación obtenida tras el análisis con el propósito de facilitar la identificación de los ficheros que deberán notificarse para su inscripción en la AEPD.

Finalmente se tendrá presente el nivel de seguridad de los ficheros para poner en funcionamiento las medidas de seguridad que correspondan, los procedimientos que se deban llevar a cabo, y todos los aspectos concretos del tratamiento.

2. Tipos de ficheros

A continuación se muestra una clasificación general de los tipos de ficheros de carácter personal. Entre ellos se desarrollan los ficheros automatizados, los manuales, los de titularidad pública y los de titularidad privada.

2.1. Ficheros automatizados. Programas de ordenador

La normativa sobre protección de datos establece que los ficheros automatizados son todo conjunto organizado de datos de carácter personal que permite acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados. Están claramente incluidos dentro de este concepto los ficheros de datos personales que

almacenan la información en soportes informáticos (base de datos, *Word,* hojas de cálculo, etc.) y que se encuentran organizados de manera que se puede acceder a los datos personales utilizando cualquier tipo de aplicación o procedimiento informatizado. Son aquellos cuyo soporte físico no permite su lectura, o escritura directa, sino que se requiere la utilización de un ordenador o dispositivo electrónico intermediario que permita la extracción/introducción, y posterior lectura/escritura de los mismos a través de un periférico como monitor, impresora, teclado, etc.

Nota

Dentro de este grupo también se encuentran los ficheros incluidos en una base de datos contenida en el disco duro de un ordenador, los ficheros contenidos en un CD, DVD, etc.

Los ficheros automatizados son ficheros de datos que se han creado usando un soporte informático. Se pueden distinguir dos tipos:

- Los creados utilizando una herramienta informática determinada para el almacenamiento de datos personales como, por ejemplo, una base de datos.
- Los creados utilizando cualquier soporte que contenga los datos personales de un modo organizado permitiendo el acceso o localización de los clientes como, por ejemplo, una hoja de cálculo.

Una vez que se tenga claro que se cuenta con un fichero de datos automatizado se habrá de notificar para su inscripción en el RGPD. Así mismo se tendrá que implantar las medidas de seguridad pertinentes en los sistemas, equipos y locales donde se realice el tratamiento de los datos.

2.2. Ficheros no automatizados o manuales. Carpetas, fichas, archivos

Por fichero no automatizado se entiende todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea un fichero centralizado, descentralizado o repartido de forma funcional o geográfica.

Los ficheros no automatizados responden a aquellos cuyo soporte físico permite la lectura y escritura directa, sin necesidad de utilizar un dispositivo electrónico intermediario. Aquí se podrían incluir los datos contenidos en soporte papel u otro material imprimible, y que se pueden tener ordenados en una carpeta, cuaderno, fichero, etc.

En el momento de la inscripción del fichero habrá que tener en cuenta los siguientes datos:

- Nombre y descripción del fichero.
- Finalidad y uso del fichero.
- Estructura del fichero.
- Procedencia de los datos.
- Nivel de seguridad del fichero.
- Consentimiento de los afectados.
- Previsión de cesiones de datos.

Finalmente, no será necesario aplicar las medidas de seguridad de carácter técnico, pero sí habrá que aplicar las medidas de seguridad de carácter organizativo o jurídico, informando a los afectados y garantizando que sus derechos están protegidos.

2.3. Ficheros temporales

Son ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional, o como paso intermedio durante la realización de un tratamiento.

Ejemplo

Una lista de clientes creada en una hoja de cálculo para enviar una actualización puntual del precio de un producto, y que después no se vuelve a utilizar. O el empleo de esa misma hoja de cálculo para exportar los datos que contiene a una base de datos permanente.

Una vez se han utilizado deben ser borrados o destruidos y, aunque sean temporales, deberán cumplir con el nivel de seguridad que les corresponda de acuerdo a los datos que contengan.

2.4. Ficheros de titularidad privada

Son aquellos de los que son responsables las personas, empresas o entidades de derecho privado, independientemente de quién aporte el capital o los recursos económicos. También se consideran ficheros de titularidad privada los de las corporaciones de derecho público que no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

Por lo tanto, los ficheros de titularidad privada son los que cualquier particular o empresa privada crea para el desarrollo de sus actividades legítimas, es decir, aquellos ficheros en los que el responsable es una persona privada física o jurídica.

2.5. Ficheros de titularidad pública

Son aquellos de los que son responsables los órganos constitucionales o con relevancia constitucional del estado, las instituciones autonómicas con funciones análogas a los mismos, las administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de estas y las corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público. Ej: (gobierno, comunidades autónomas, ayuntamientos, administraciones públicas, etc.)

3. Otros ficheros y tratamientos específicos

3.1. Tratamiento de datos personales a través de sistemas de cámaras o videocámaras

La seguridad y la vigilancia no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que exige respetar la normativa existente en materia de protección de datos.

Las imágenes se consideran un dato de carácter personal en virtud de lo establecido en el artículo 3 de la LOPD 15/1999 que considera como dato de carácter personal la información gráfica o fotográfica.

La utilización de estos sistemas de grabación debe ser proporcional al fin perseguido, que, en todo caso, deberá ser legítimo, es decir, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En este sentido, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de la proporcionalidad, es necesario ver si cumple los siguientes requisitos:

- Juicio de la idoneidad. Si tal medida es susceptible de conseguir el objetivo propuesto.
- Juicio de necesidad. Si, además, es necesaria en sentido que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia.
- Juicio de proporcionalidad. Si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Ámbito objetivo

El tratamiento objeto de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos (BOE 12 de diciembre) comprende la grabación, captación, transmisión, conservación y almacenamiento de imágenes incluida su reproducción en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquellas.

Nota

Se considera identificable a una persona cuando su identidad puede determinarse mediante los tratamientos a los que se refiere dicha instrucción.

El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las fuerzas y cuerpos de seguridad se regirá por las disposiciones sobre la materia.

No se considera objeto de regulación de esta instrucción el tratamiento de imágenes en el ámbito personal y doméstico.

Legitimación

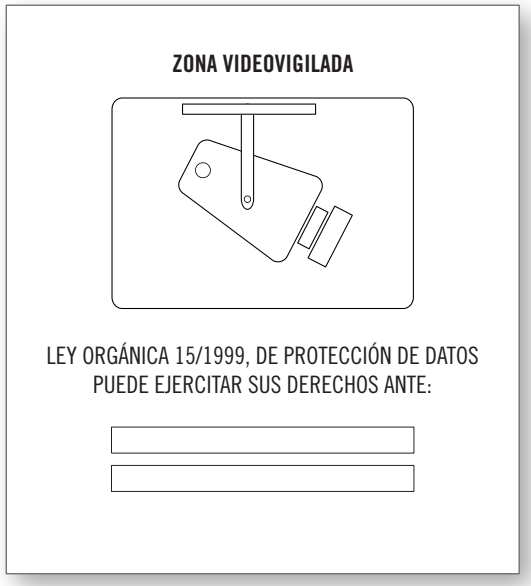
Solo será posible el tratamiento de los datos objeto de la instrucción cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la actual LOPD.

Sin perjuicio de lo establecido en el apartado anterior, la instalación de cámaras y videocámaras deberá respetar los requisitos exigidos por la legislación vigente en la materia.

Información

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, y deberán:

- Colocar en las zonas videovigiladas al menos un distintivo informativo ubicado en un lugar visible tanto en espacios abiertos como cerrados. El distintivo informativo a que se refiere el artículo 3.a de la instrucción deberá incluir una referencia a la Ley Orgánica 15/1999, de Protección de Datos, mencionando la finalidad para la que se tratan los datos (ZONA VIDEOVIGILADA), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.



- Tener a disposición de los interesados impresos en los que se detalle la información prevista en el artículo 5.1 de la LOPD. A continuación se muestra el modelo de cláusula informativa que establece el artículo 3 en su apartado b de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Modelo cláusula informativa

Art. 3, apartado B. Instrucción 1/2006, de 8 de Noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

FICHERO PRIVADO

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de Diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado "..." y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.

2. Que el destinatario de sus datos personales es:
a. La empresa de seguridad...
b. El dueño del establecimiento...

3. Que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante el responsable del fichero.

4. Que el responsable del fichero tratamiento es " (... nombre o razón social...)"o su representante D/Dª. "..." ubicado en C/ ...

Modelo cláusula informativa

FICHERO PÚBLICO

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de Diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado "..." del que es responsable ese organismo, creado por Resolución... (BOE...) y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.

2. Que el destinatario de sus datos personales es la empresa de seguridad...

3. Que puede ejercitar sus derechos de acceso, cancelación y oposición ante el responsable del fichero.

4. Que el responsable del fichero tratamiento es " (... nombre o razón social...)"o su representante D/Dª. "..." ubicado en C/ ...

Principios de calidad, proporcionalidad y finalidad del tratamiento

De acuerdo con el artículo 4 de la LOPD, las imágenes solo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas que hayan justificado la instalación de cámaras y videocámaras.

Solo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende.

Derechos de las personas

Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la LOPD, el afectado deberá remitir al responsable del tratamiento una solicitud en la que hará constar su identidad junto con una imagen actualizada.

El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que se especifiquen los datos que han sido objeto del tratamiento sin que afecte a los derechos de terceros.

El interesado al que se denieguen total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior podrá reclamar su tutela ante el director de la Agencia de Protección de Datos.

Cancelación

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

Notificación de ficheros

La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos para su inscripción en el registro de la misma.

No se considerará como fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Seguridad y secreto

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración o acceso no autorizado.

El responsable de la instalación deberá adoptar las medidas de índole técnicas y organizativas necesarias que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Por tanto,

quien haya contratado los servicios de una empresa de seguridad debe cumplir con el deber de garantizar la seguridad de las imágenes en los términos establecidos por la LOPD y su reglamento de desarrollo.

Con carácter general los ficheros de videovigilancia suelen tener un nivel básico. No obstante, el responsable del fichero debe tener en cuenta que deberá evaluar el nivel de seguridad según lo dispuesto por el artículo 81 del reglamento en función del contenido y finalidad del fichero.

Ejemplo

Puede darse el caso de que la captación de imágenes desborde el marco de la vigilancia y se utilice con fines de selección de personal o para verificar la respuesta a determinados estímulos, en psicología o medicina, con lo que el nivel de seguridad sería medio o alto.

Las imágenes facilitadas a la autoridad judicial o fuerzas y cuerpos de seguridad del estado con motivo de un delito se convierten en datos relativos a investigaciones policiales y los ficheros de estas autoridades tendrían que aplicar un nivel alto de seguridad.

Hasta la entrada en vigor de la Ley 25/2009, de 27 de diciembre, solo era conforme a la legislación de protección de datos personales la utilización de dispositivos de videovigilancia si se había contratado con empresas de seguridad privada, debidamente autorizadas por el Ministerio del Interior.

La "Ley Ómnibus" reforma la Ley de Seguridad Privada, liberalizando esta actividad determinando que la venta, entrega, instalación o mantenimiento de estos sistemas podrá llevarse a cabo por particulares y empresas distintas de las de seguridad privada siempre que la instalación no implique una conexión con las centrales de alarma.

Se modifica por tanto la exigencia de recurrir a empresas de seguridad autorizadas por el Ministerio del Interior y de notificar el contrato a dicho ministerio.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora, esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho departamento.

En el tratamiento de imágenes deberán cumplirse las normas establecidas en la legislación de protección de datos de carácter personal, entre las que se incluyen el deber de informar a los interesados, la inscripción de ficheros y la implantación de medidas de seguridad.

La interpretación de la mencionada disposición determina que cualquier particular o empresa cuya actividad no sea la propia de una empresa de seguridad privada podrá vender, entregar, instalar y mantener equipos técnicos de seguridad sin necesidad de cumplir las exigencias previstas en la Ley de Seguridad Privada para tales empresas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior. Así mismo, cualquier persona que tenga acceso a los datos por razón del ejercicio de sus funciones deberá observar la debida reserva y sigilo en relación con las mismas.

3.2. Tratamiento de los datos sobre violencia doméstica y de género

La Orden INT/1911/2007 sobre violencia doméstica y de género (BOE 29 de junio) tiene por finalidad mejorar la eficacia en la protección de las víctimas de violencia doméstica y de género, facilitar el seguimiento de las circunstancias de riesgo que concurren en ellas, alertar de su evolución, permitiendo que se adopten medidas de protección adecuadas, y prevenir el riesgo de nuevas agresiones.

Los usos previstos en la orden son la protección de víctimas, prevención de infracciones penales relacionadas con la violencia doméstica y de género, y tratamiento penitenciario a los agresores.

Las personas o colectivos sobre los que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos son las personas que sean víctimas de hechos susceptibles de ser tipificados como violencia doméstica y de género, y las personas incursas en procedimientos judiciales e investigaciones policiales por hechos relacionados con la violencia doméstica y de género.

Estructura básica del fichero

Las descripciones de los tipos de datos de carácter personal incluidos en el fichero son:

- **Datos relativos a la comisión de infracciones penales relacionadas con la violencia doméstica y de género:** infracciones y antecedentes penales de los presuntos autores y situación penitenciaria de los mismos relativa a la concesión de permisos o a la puesta en libertad de los internos que se encuentren sujetos a medidas judiciales de alejamiento o prohibición de comunicación con la víctima.
  Datos de carácter identificativo: DNI/NIF, pasaporte, así como otros documentos de identidad, fotografía, domicilios, teléfonos y correo electrónico.
  Datos de características personales: datos de filiación, familiares, fecha y lugar de nacimiento, sexo, nacionalidad, situación laboral, profesión, nivel educativo y estado civil.

Procedimiento de recogida de datos de carácter personal

Las fuerzas y cuerpos de seguridad y la Dirección General de Instituciones Penitenciarias serán las únicas competentes para introducir y modificar los datos.

Los datos procederán de las denuncias presentadas ante las fuerzas y cuerpos de seguridad, de los atestados policiales y de resoluciones dictadas por las autoridades judiciales y penitenciarias.

Conservación y cancelación de datos con arreglo a lo dispuesto en el artículo 22.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Se cancelarán los datos cuando finalice la vigencia de la medida judicial de protección (ya se trate de medida cautelar o cumplimiento de condena en centro penitenciario o en medida alternativa).

El acceso a la información contenida en la base de datos quedará limitado a los sujetos y finalidades siguientes:

- Los órganos judiciales del orden penal y los juzgados de violencia sobre la mujer podrán acceder a la información que precisen para la tramitación de causas penales, así como para la adopción, modificación, ejecución y seguimiento de medidas de protección de dichas víctimas a través del secretario judicial o de un funcionario adscrito a la oficina judicial por él designado.
- El Ministerio Fiscal podrá acceder a la información precisa para la tramitación de causas penales, así como para la adopción, modificación, ejecución y seguimiento de las medidas de protección de dichas victimas a través de los fiscales destinados en las fiscalías de los órganos jurisdiccionales competentes.
- La policía judicial y las unidades policiales especializadas en violencia de género podrán acceder a la información necesaria para el desarrollo de las actuaciones que le estén encomendadas en relación con la persecución y seguimiento de las conductas que tienen acceso a esta base de datos y para el control y ejecución de las medidas de protección a las víctimas a través de los funcionarios autorizados que desempeñen estas funciones.
- La Dirección General de Instituciones Penitenciarias, a través de los directores de los centros penitenciarios o de los centros de inserción social, podrán acceder a la información relativa a los quebrantamientos de condena, medidas de seguridad o medidas cautelares que se produzcan durante los permisos penitenciarios o durante la situación de libertad condicional de los internos que se encuentren sujetos a medidas judiciales de alejamiento o prohibición de comunicación con la víctima de violencia doméstica o de género.

- Las Delegaciones y Subdelegaciones del Gobierno podrán acceder a la información necesaria para garantizar el efectivo cumplimiento de las medidas de protección, provisionales o definitivas, adoptadas por los órganos jurisdiccionales a través del responsable de la unidad de protección a las víctimas de la violencia doméstica o de género, o a través de las personas designadas por dicho responsable.

El acceso a los datos del registro central se llevará a cabo telemáticamente, mediante procedimientos de identificación y autentificación.

Nota

El sistema de acceso deberá dejar constancia de la identidad de los usuarios que accedan, de los datos consultados, del momento de acceso y del motivo de la consulta.

El órgano administrativo ante el que se pueden ejercitar los derechos de acceso, rectificación, cancelación, y oposición, es el Ministerio del Interior-Secretaria de Estado de Seguridad.

3.3. Tratamiento de los datos personales de la historia clínica del paciente

La norma a desarrollar en el presente apartado es la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica (BOE 15 de noviembre).

Ámbito de aplicación

La ley tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros sanitarios,

públicos y privados, en materia de autonomía del paciente y de la información y documentación clínica.

Los principios básicos de esta ley

Respecto a los principios que rigen la normativa cabe destacar los siguientes:

- La dignidad de la persona humana y el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica.
- Toda actuación en el ámbito de la sanidad requiere el consentimiento de los pacientes o usuarios.
- El paciente tiene derecho a decidir libremente después de recibir la información adecuada.
- Todo paciente o usuario tiene derecho a negarse al tratamiento, excepto en los casos determinados por la ley.
- Los pacientes tienen el deber de facilitar los datos sobre su estado físico de manera leal o verdadera.
- Todo profesional que interviene en la actividad asistencial está obligado, no solo a la correcta prestación de sus técnicas, sino al cumplimiento de los deberes de información y documentación clínica y al respeto de las decisiones adoptadas libre y voluntariamente por el paciente.
- La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida.

El derecho a la información asistencial

Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la ley. La información clínica será verdadera y se comunicará al paciente de forma comprensible. El médico responsable garantizará el cumplimiento del derecho a la información.

Titular del derecho a la información asistencial

El titular del derecho a la información es el paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita. Además, la ley establece los siguientes puntos:

- Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando implique un riesgo para la salud pública o para su salud individual.
- Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud.
- Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, el consentimiento será verbal o por escrito según lo previsto en la ley.

Sabía que...

Además de todos los derechos descritos anteriormente, los pacientes y usuarios del sistema nacional de salud, tanto en atención primaria como en la especializada, tendrán derecho a la información previa para elegir médico y centro con arreglo a los términos y condiciones que establezcan los servicios de salud competentes.

La historia clínica

La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y demás profesionales que han intervenido en ellos. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte: papel, audio, visual. Las administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad de la historia clínica.

Las comunidades autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

A continuación se enumeran los derechos que la ley otorga a cada paciente:

- El contenido de la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente.

Nota

La historia clínica es un instrumento destinado a garantizar una asistencia adecuada al paciente, cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

Todo paciente o usuario tiene derecho a que quede constancia por escrito en el soporte técnico más adecuado. Tendrá como fin principal facilitar la asistencia sanitaria dejando constancia de todos los datos que permitan el conocimiento veraz y actualizado del estado de salud.

El personal de administración y gestión de los centros sanitarios solo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación, y planificación tiene acceso a las historias clínicas en el cumplimiento de las funciones de comprobación de calidad de la asistencia. Este personal respetará los derechos del paciente y cualquier otra obligación del centro en relación a los pacientes y usuarios o la propia administración sanitaria.

El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto. Las comunidades

autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso.

Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, como mínimo cinco años contados desde la fecha de alta de cada proceso asistencial.

- Derechos de acceso a la historia clínica. El paciente tiene derecho de acceso a la documentación de la historia clínica y a obtener copia de los datos que figuren en ella con las reservas señaladas en la ley.

  El derecho de acceso del paciente a la historia clínica puede ejercitarse por representación debidamente acreditada. Este derecho a la documentación clínica no puede ejercitarse en perjuicio del derecho de terceras personas, ni en perjuicio de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para la salud se limitará a los datos pertinentes.
- Derechos relacionados con la custodia de la historia clínica. El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, integración, recuperación y comunicación de la información sometida al principio de confidencialidad.
- El régimen sancionador. Las infracciones de lo dispuesto por la ley quedan sometidas al régimen sancionador previsto en el Capítulo VI del Título de la Ley 14/1986 General de Sanidad, sin perjuicio de la responsabilidad civil o penal, y de la responsabilidad profesional o estatutaria procedentes en derecho.

4. Niveles de seguridad de los ficheros

El nivel de seguridad de un fichero se establece atendiendo a la naturaleza de los datos que contenga. En este sentido, y con el fin de determinar el nivel de seguridad de los ficheros con datos de carácter personal, se debe remitir al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento que desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de

Protección de Datos de Carácter Personal. Este reglamento establece en su artículo 81 los siguientes niveles de seguridad:

- La medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.
- Dichos niveles se establecen atendiendo a la naturaleza de la información tratada en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Aplicación de niveles

Nivel alto. Ficheros o tratamientos con datos

Se consideran datos con nivel alto de seguridad los relativos a:

- Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico.
- Recabados con fines policiales sin consentimiento de las personas afectadas.
- Derivados de actos de violencia de género.

También se aplicarán las medidas de nivel alto a los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

Importante

Para esta categoría de ficheros deberá disponerse de un registro de accesos.

Nivel medio. Ficheros o tratamientos con datos

Se consideran datos con nivel medio de seguridad los relativos a:

- La comisión de infracciones administrativas o penales.
- Aquellos que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito).
- Los de administraciones tributarias y que se relacionen con el ejercicio de sus potestades tributarias.
- Entidades financieras para las finalidades relacionadas con la prestación de servicios de sus competencias.
- Entidades gestoras y servicios comunes de seguridad social que se relacionen con el ejercicio de sus competencias.
- Mutuas de accidentes de trabajo y enfermedades profesionales de la seguridad social.
- Aquellos que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas.

Nivel básico

Se consideran de nivel básico los siguientes datos (siempre que no constituyan un perfil de la persona):

- Identificativos (DNI/NIF, nombre y apellidos, dirección, teléfono, firma/huella, imagen/voz, marcas físicas).
- Características personales (datos de estado civil, familia, fecha/lugar de nacimiento, características físicas/antropométricas, edad, sexo, nacionalidad, lengua materna).
- Circunstancias sociales (características de alojamiento/vivienda, situación militar, propiedades/posesiones, aficiones y estilo de vida, pertenencia a clubes o asociaciones, licencias, permisos, autorizaciones).
- Académicos y profesionales (formación, titulaciones, historial de estudiante, experiencia profesional, pertenencia a asociaciones profesionales).

- Datos de detalles de empleo (profesión, puestos de trabajo, historial del trabajador).
- Información comercial (actividades y negocios, licencias comerciales, suscripciones a publicaciones/medios de comunicación, creaciones artísticas, literarias, científicas o técnicas).
- Datos económicos-financieros y de seguros (ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, datos bancarios, tarjetas de crédito, planes de pensiones, jubilación, datos económicos de nómina, datos de deducciones impositivas/impuestos, hipotecas, subsidios, beneficios, historial de créditos).
- Datos de transacciones (bienes y servicios suministrados por el afectado, transacciones/indemnizaciones).

Se consideran ficheros de nivel básico aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros. (Letra a del apartado 5 del artículo 81 del Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).
- Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con la finalidad del fichero. (Letra b del apartado 5 del artículo 81 del Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, modificado por la disposición adicional cuarta del Real Decreto 3/2010 por el que se regula el esquema nacional de seguridad en el ámbito de la administración electrónica).
- Los ficheros o tratamientos que contengan datos de salud que se refieran exclusivamente al grado o condición de discapacidad o a la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

5. Casos prácticos

Caso práctico empresa A

En el capítulo anterior se describieron una serie de empresas para la realización de los supuestos prácticos. La primera de ellas era una distribuidora de un operador de telefonía móvil. La base de datos de los clientes de esta empresa estaba contenida en un fichero automatizado dentro del sistema de información que el dueño implantó para la gestión de su empresa. En este caso se tratará de determinar a qué nivel de seguridad pertenecerá dicho fichero partiendo del análisis del tipo de información que se recoge en el mismo. Para ello se recuerdan los datos de los clientes que se guardan en la base de datos:

Tabla: Clientes

	Nombre del Campo	Tipo de Datos	Descripción del campo
1	Nombre_cliente	Alfabético	De unos 50 caracteres
2	DNI	Alfanumérico	De 9 caracteres
3	Domicilio	Alfanumérico	De 100 caracteres
4	Teléfono_fijo	Numérico	De 9 caracteres
5	Teléfono_móvil	Numérico	De 9 caracteres
6	Tarjeta/ Contrato tipo	Alfanumérico	De 25 caracteres
7	Fecha_nacimiento	Fecha	De 10 caracteres

Como se puede observar, el fichero recoge simplemente los datos personales elementales para identificar a un cliente (nombre, DNI y domicilio), además de su número de teléfono (fijo o móvil) y la fecha de nacimiento que será utilizada para determinar su edad a la hora de enviarle información sobre nuevos productos, ya que los catálogos de novedades son distintos según vayan destinados a jóvenes o a personas adultas.

Además se observa un campo llamado "Tarjeta/Contrato tipo", el cual indica si el cliente ha comprado un móvil con tarjeta de recarga o si por el contrario ha adquirido un móvil por contrato y a qué tipo de contrato pertenece en ese caso.

Por lo tanto, el fichero necesitaría cumplir solamente las medidas de seguridad de nivel básico.

Caso práctico empresa B

El segundo supuesto trata de una aseguradora llamada "LOPD Seguros S. L." propiedad de Antonio Pérez Pérez. La base de datos estaba contenida también en soporte informático, por lo que efectivamente se trataría de un fichero automatizado.

Pero además de este fichero la empresa mantenía un fichero manual en el que se guardaban diversos documentos de los clientes en soporte papel, como facturas de reparaciones, partes médicos, etc. Este fichero estará regulado por la normativa contenida en el actual RLOPD 1720/2007, cosa que no ocurría con el anterior Reglamento de Seguridad 994/1999, ya derogado.

Para determinar el nivel de seguridad del fichero automatizado recordaremos los datos que se guardaban en la base de datos.

A continuación se insertará una tabla de ficheros automatizados.

Tabla: Clientes

	Nombre del campo	Tipo de datos	Descripción del campo
1	Nº_de_póliza	Numérico	De 8 caracteres
2	Fecha_ vencimiento	Fecha	De 10 caracteres
3	DNI_ Tomador	Alfanumérico	De unos 9 caracteres
4	Nombre_ tomador	Alfabético	De 50 caracteres
5	Domicilio	Alfanumérico	De unos 100 caracteres
6	Tipo_de _Seguro	Alfanumérico	De unos 25 caracteres
7	Beneficiario	Alfabético	De unos 50 caracteres
8	Importe _prima	Numérico	De unos 6 caracteres

Además de este fichero automatizado la empresa tiene otro fichero manual que es el siguiente:

Tabla: Otra documentación

	Nombre del campo	Tipo de datos	Descripción del campo
1	Nombre_del _tomador	Alfabético	De unos 50 caracteres
2	Domicilio	Alfanuméricos	De 100 caracteres
3	DNI_Tomador	Alfanumérico	De 9 caracteres
4	Tipo de Seguro	Alfanumérico	De 25 caracteres
5	Factura de reparación	Alfanumérico	De 25 caracteres
6	Parte médico	Alfanumérico	De 100 caracteres
7	Tratamiento	Alfabético	De 100 caracteres

La base de datos de clientes contiene mayoritariamente datos personales que quedarían clasificados en nivel de seguridad básico. Los datos que hacen referencia a servicios financieros, como son los seguros contratados por el cliente, se considerarán en un nivel de seguridad medio.

Además el fichero manual: otra documentación, recoge datos referentes a los partes médicos de los clientes, que contratan un seguro, los cuáles están protegidos con medidas de nivel alto.

Caso práctico empresa C

Por último, el tercer supuesto trata sobre una clínica dental llamada "LOPD Odontos S. L." cuyo propietario es Fernando Ruiz Ruiz. La base de datos de pacientes e información clínica está también en soporte informático, por lo que se trataría de un fichero automatizado.

A continuación se muestran las tablas con los datos:

Tabla: Ficha Pacientes			
	Nombre del campo	**Tipo de datos**	**Descripción del campo**
1	Número_ cliente	Numérico	8 caracteres
2	Nombre y apellidos	Alfabético	50 caracteres
3	Fecha_visita	Fecha	6 caracteres
4	Dirección	Alfanumérico	50 caracteres
5	Teléfono	Numérico	9 caracteres
6	Motivo	Alfabético	100 caracteres
7	Doctor	Alfabético	30 caracteres

Tabla: Datos clínicos			
	Nombre del campo	**Tipo de datos**	**Descripción del campo**
1	Número_Paciente	Numérico	De 8 caracteres
2	Nombre-Paciente	Alfabética	De 30 caracteres
3	Grupo sanguíneo	Alfabética	De 3 caracteres
4	Sexo	Alfabética	De 6 caracteres
5	Operaciones	Alfanumérico	De 100 caracteres
6	Enfermedades_padecidas	Alfabético	De 100 caracteres
7	Alergias	Alfanumérico	De 100 caracteres
8	Intolerancias	Alfanumérico	De 100 caracteres
9	Otros datos clínicos	Alfanumérico	De 200 caracteres
10	Tratamiento	Alfanumérico	De 200 caracteres

Otras pruebas clínicas			
	Nombre del campo	**Tipo de datos**	**Descripción del campo**
1	Nº Paciente	Número	De 8 caracteres
2	Nombre Paciente	Alfanumérico	De 50 caracteres
3	DNI	Alfanumérico	De 9 caracteres
4	Radiografías	Prueba radiológica	----------
5	Estudio Ortodoncia	Prueba documental	De 200 caracteres
6	Analíticas	Alfanumérico	De 200 caracteres

Por tanto, y en vista de la naturaleza que presentan los datos de las tres tablas, el fichero "Ficha pacientes" se consideraría de nivel básico porque contiene solo datos de carácter identificativo y tanto el fichero "Datos clínicos" (automatizado), como el fichero "Otras pruebas clínicas" (no automatizado o manual) quedarían clasificados en su totalidad de nivel de seguridad alto, ya que contienen datos de salud.