Unidad Didáctica 4

Las medidas de seguridad

Contenido

1. Datos especialmente protegidos

Los datos especialmente protegidos, también conocidos como *"datos sensibles"* son una categoría de información que por su especial influencia en la intimidad, derechos fundamentales y las libertades públicas del individuo requieren de una mayor protección que el resto de los datos personales. Su tratamiento se encuentra regulado en el art. 7 de la LOPD y son los siguientes:

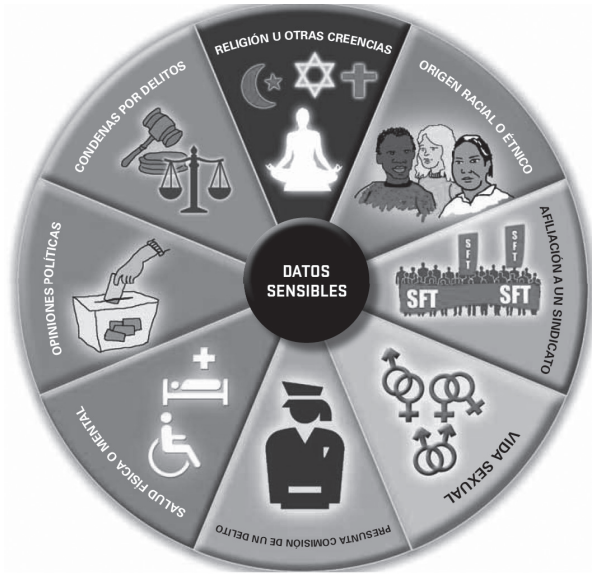
- Datos que revelen la ideología, afiliación sindical, religión y creencias.
- Datos que hagan referencia al origen racial, la salud o la vida sexual.
- Datos relativos a la comisión de infracciones penales o administrativas.

El responsable del fichero debe tratar los datos especialmente protegidos en las condiciones previstas en el art. 7 de la LOPD, dichas condiciones son las siguientes:

- **Derecho a no declarar sobre la ideología, afiliación sindical, religión o creencias.** De acuerdo con lo establecido en el art. 16.2 de la Constitución Española, nadie podrá ser obligado a declarar sobre su ideología, afiliación sindical, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento para el tratamiento de esta información se advertirá al interesado acerca de su derecho a no prestarlo. (Art. 7.1 de la LOPD).
- **Tratamiento de los datos que revelen ideología, afiliación sindical, religión o creencias.** El tratamiento de estos datos solo podrá realizarse con el consentimiento expreso y por escrito del interesado. 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. (Art. 7.2 de la LOPD).
- **Tratamiento de los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual.** Este tipo de datos solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. (Art. 7.3 de la LOPD).

Ejemplo: datos de origen racial son el color de la piel o raza concreta a la que pertenece el sujeto. Datos de salud son enfermedades padecidas, análisis clínicos, radiografías, etc. Datos de vida sexual son hábitos sexuales, prácticas de riesgo, uso de anticonceptivos, etc.

- **Tratamiento de los datos de carácter personal relativos a la comisión de infracciones penales o administrativas.** Este tipo de datos solo podrá ser incluido en los ficheros de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
  La LOPD entiende que se debe proteger estos datos, porque si se vulneran los tratamientos de los expedientes sancionadores se puede atentar gravemente contra el derecho a la intimidad. (Art. 7.5 de la LOPD).
- **Ficheros prohibidos.** Se debe mencionar que 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. (Art. 7.4 de la LOPD).
- **Excepciones.** No obstante podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, y los que hagan referencia al origen racial, a la salud, y a la vida sexual, 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, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. (Art. 7.6 de la LOPD).



Datos especialmente protegidos

2. Medidas y documento de seguridad

Las empresas deben adoptar las medidas de carácter técnico, organizativo y/o jurídico que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Estas medidas se fijan en función del nivel de seguridad correspondiente al fichero, y en función del soporte del mismo (automatizado o no automatizado).

Importante

Debe tenerse en cuenta que los niveles de seguridad son acumulativos, es decir, los ficheros de nivel alto deben cumplir las medidas previstas para los ficheros de nivel alto, medio y básico, y los ficheros de nivel medio deben hacer lo propio con respecto a los niveles medio y básico.

Existen tres niveles de seguridad en función de la mayor o menor sensibilidad de los datos recogidos en ellos, tal y como muestra la siguiente tabla.

NIVEL BÁSICO

Nombre · Apellidos · Datos de contacto (dirección, teléfono, e-mail, etc.). Cualquier otro dato que no sea nivel medio o alto.

NIVEL MEDIO

Datos relativos a la comisión de infracciones administrativas o penales · Datos de los que sean responsables las administraciones tributarias · Datos de los que sean responsables las entidades financieras · Datos de los que sean responsables las entidades gestoras y servicios comunes de la seguridad social · Datos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas · Datos que ofrezcan una definición de las características o personalidad de los ciudadanos y permitan evaluar aspectos de su personalidad o comportamiento.

NIVEL ALTO

Ideología · Afiliación sindical · Religión y creencias · Origen racial · Salud y vida sexual · Datos recabados para fines policiales sin consentimiento de las personas afectadas · Datos derivados de actos de violencia de género.

2.1. Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Medidas de seguridad de nivel básico

Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. Esto lo prevé el art. 81.1 del R. D. 1720/2007, de 21 de diciembre, que desarrolla la Ley Orgánica 15/1999 de Protección de Datos. Lo que se pretende es que cualquier dato

personal esté protegido con medidas de seguridad. Las medidas de nivel básico se desarrollan en el Título VIII en su Capítulo I y se muestran a continuación.

Funciones y obligaciones del personal

Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento (art. 89 del R. D. 1720/2007).

La empresa considerará la necesidad de obtener formalmente la aceptación de las normas y procedimientos por parte de sus empleados. La finalidad de esta medida es evitar la ilegalidad en el tratamiento de datos por parte de la plantilla.

El trabajador con acceso a los datos debe notificar al responsable del fichero cualquier incidencia de seguridad de las que tenga conocimiento y guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

A continuación, se muestra un ejemplo de plantilla que deberá entregarse al personal para que conozca sus obligaciones respecto a la protección de datos.

OBLIGACIÓN DEL DEBER DE SECRETO PROFESIONAL

En desarrollo de la relación laboral que D./Dª. **(NOMBRE DEL TRABAJADOR)** mantiene con **(NOMBRE EMPRESA),** tendrá acceso a datos de carácter personal cuyo tratamiento está sometido a las condiciones y requisitos establecidos en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Por ello, D./Dª **(NOMBRE TRABAJADOR),** se compromete a guardar secreto sobre todo los datos de carácter personal y cualquier información o circunstancias a los que haya tenido acceso en el ejercicio de las funciones que le hubiesen sido asignadas.

Las anteriores obligaciones se extienden a cualquier fase del tratamiento de los citados datos, y subsistirán aún después de concluidas las funciones en el marco en los cuales ha tenido acceso a los datos o concluida su vinculación con **(NOMBRE DE LA EMPRESA).**

Plantilla de obligación del deber de secreto profesional

Registro de incidencias

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

(Art. 90 del R. D. 1720/2007).

Es decir, se debe mantener un registro en el que se anote cualquier anomalía que afecte o pudiera afectar a la seguridad, a la integridad, confidencialidad o disponibilidad de los datos.

El registro de incidencias permite disponer de un control completo, exacto y detallado de cualquier problema que pueda ocurrir dentro de los sistemas de información que traten con datos de carácter personal con el fin de definir las responsabilidades y medidas correctivas a ejecutar en caso de ocurrir dichas irregularidades.

Sabía que...

No llevar ese registro significa un incumplimiento de la Ley de Protección de Datos. Actualmente son muchas las empresas que incumplen la normativa a consecuencia de no llevar este registro de incidencias y que por tanto están expuestas a una sanción por parte de la Agencia de Protección de Datos.

A continuación se exponen algunos ejemplos de posibles incidencias de seguridad que se pueden producir en las empresas y que deberían reflejarse en el registro de incidencias:

- Modificaciones/accesos no autorizados a la información.
- Pérdida de información.
- Copias indebidas de datos en los puestos de trabajo.
- Mal funcionamiento durante la realización de copias de seguridad.
- Accesos no autorizados a las salas donde se ubiquen los sistemas y soportes informáticos (oficina, caja de seguridad, etc.).
- Intento no autorizado de salida de soportes.
- Destrucción total/parcial de soportes físicos.
- Conocimiento por terceros del identificador de usuario y contraseña.
- Existencia de sistemas sin las debidas medidas de seguridad.

MODELO DE NOTIFICACIÓN DE INCIDENCIAS	
Incidencia Nº: **0000002** (A cumplimentar por responsable seguridad)	
Fecha de notificación:	
Tipo de incidencia:	Fecha y hora en que se produce /detecta * (* tachar lo que no proceda)
Descripción detallada de la incidencia:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)	
Persona(s) a quien(es) se comunica:	Persona que realiza la comunicación: Fdo:
MEDIDAS CORRECTORAS APLICADAS: Fecha Hora	

Control de acceso

El control de acceso hace referencia a la autorización, es decir, a los permisos que puedan tener los usuarios para realizar determinadas acciones sobre los recursos. Se podría dividir en control de acceso lógico (a los sistemas automatizados) o físico (a sistemas no automatizados o a las propias instalaciones donde están los sistemas).

El personal que acceda a datos personales solo podrá acceder a aquellos datos que sean necesarios en el ejercicio de sus funciones. Se pretende controlar y gestionar el acceso al sistema de información provisto de datos personales.

El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y accesos autorizados a cada uno de ellos.

El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.

Exclusivamente, el personal autorizado para ello en el documento de seguridad podrá conceder, alterar, o anular el acceso autorizado sobre los datos y recursos conforme a los criterios establecidos por el responsable del fichero.

Nota

En el supuesto de que exista personal ajeno al responsable del fichero que tenga acceso a los datos personales deberá estar sometido a las mismas condiciones y obligaciones de seguridad del personal propio. (Art. 91 del R. D. 1720/2007).

Identificación y autenticación

El reglamento de la ley establece que el responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer los procedimientos de identificación y autenticación necesarios para dichos accesos, es decir, disponer de mecanismos adecuados que impidan el acceso de usuarios no autorizados al sistema.

La identificación es el reconocimiento de la identidad del usuario y la autenticación es la comprobación de su identidad. Es decir, se tendrá acceso autorizado al sistema de información a través del nombre de usuario (identificación) y contraseña de acceso asociada al nombre de usuario (autenticación).

El responsable del fichero será la persona encargada de adoptar las medidas necesarias para la correcta identificación y autenticación de los usuarios a través de mecanismos que permitan identificar de forma inequívoca y personalizada a todo usuario que intente acceder al sistema de información, además de verificar que el usuario está autorizado para esta labor.

Si el mecanismo de autenticación se basa en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad.

En el caso de las contraseñas se debe asegurar que las mismas sean robustas, que no sean fácilmente deducibles, y que no estén a la vista del resto de empleados.

Usuario y contraseña

Consejo

Es conveniente fijar unos requisitos que deben cumplir las cadenas utilizadas como contraseña (longitud mínima, combinación de caracteres alfanuméricos, etc.).

En el documento de seguridad se establecerá la periodicidad con la que tienen que ser cambiadas las contraseñas (que nunca podrá ser superior a un año). Tales contraseñas se almacenarán de forma ininteligible. (Art. 93 del R. D. 1720/2007).

Gestión de soportes y documentos

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados, y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento, deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

Con dicha medida se pretende establecer un procedimiento o un régimen de salidas de soportes para evitar la cesión no permitida de datos personales.

Cuando se proceda al traslado de documentación se tomarán todas las medidas necesarias para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

En el supuesto de que hubiera que desechar cualquier documento o soporte que contenga datos de carácter personal se procederá a su

destrucción o borrado, siempre tomando las medidas necesarias para evitar el acceso a la información contenida en el mismo o su posterior recuperación.

Los soportes que contengan datos personales considerados especialmente sensibles se podrán identificar utilizando sistemas de etiquetado comprensibles que permitan al personal con acceso autorizado a los mismos identificar su contenido, pero dificultando la identificación para el resto de personas. (Art. 92 del R. D. 1720/2007).

Ejemplo

Fecha de actualización: 31 de enero de 2012.

Identificador del soporte: NOM-31012012.

Descripción del soporte: copia de seguridad de los datos de nóminas de los empleados de la empresa a fecha de 31 de diciembre de 2012.

Responsable del fichero al que pertenece: Sr. Manuel Gómez (Jefe de Personal).

Ubicación actual: caja de seguridad nº 2, estantería nº 3, oficina central, Sevilla.

Copias de respaldo y recuperación

La copia de seguridad o copia de respaldo de un fichero *(backup)* es la copia de los datos que permite restaurarlos en el caso de una pérdida de información.

Las pérdidas de información son frecuentes en el entorno empresarial, y pueden tener su origen en diferentes causas: descuido de un empleado que elimina información involuntariamente, pérdida del soporte físico que contiene el archivo (CD, DVD, ordenador portátil, etc.), infección por malware, etc.

Es naturalmente obligatorio realizar copias de seguridad de los datos y hay establecidas una serie de medidas que se deben adoptar para cumplir con el reglamento:

- Como mínimo se deben realizar semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
- Hay que establecer procedimientos que aseguren la recuperación de los datos para poder garantizar en todo momento su reconstrucción al estado en el que se encontraban al tiempo de producirse la pérdida o destrucción. En el supuesto de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados se deberá proceder a grabar manualmente los datos, quedando constancia motivada de este hecho en el documento de seguridad con la finalidad de poder realizar las copias de respaldo y recuperación que facilitarán que los datos estén siempre actualizados y adecuados a la realidad.
- Cada seis meses el responsable del fichero deberá verificar la correcta definición, funcionamiento y aplicación de los procedimientos de realización de las copias de respaldo y de recuperación de datos.
- Si se van a cambiar o modificar los sistemas de gestión que tratan los datos, las pruebas que se realicen no podrán efectuarse con datos reales a no ser que se garanticen las medidas de seguridad aplicables y se anote en el documento de seguridad. Si así se hace habrá que realizar una copia de seguridad previa. (Art. 94. R. D. 1720/2007).

CD de copia de seguridad

Medidas de seguridad de nivel medio

Las medidas de seguridad de nivel medio se desarrollan en el Capítulo III del R.D. 1720/2007, de 21 de diciembre, reguladora de la Ley Orgánica de Protección de Datos, y son las que se muestran a continuación.

Responsable de seguridad

Es la persona encargada de coordinar y controlar las medidas contenidas en el documento de seguridad. Podrá designarse uno o varios responsables de seguridad. Esta designación puede ser única para todos los ficheros o tratamientos de datos, o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá constar claramente en el documento de seguridad.

Nota

El reglamento pretende con esta medida que todos los procedimientos y normas que aparecen en el documento de seguridad y que estén establecidos en la entidad que tratan los datos personales se centralicen a través del responsable de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con el Real Decreto 1720/2007. (Art. 95 del R. D. 1720/2007).

Auditoría

La normativa actual determina la obligación de realizar una auditoría bienal a partir de nivel medio, tanto en tratamientos automatizados como no automatizados. Esto implica la necesidad de someterse, al menos cada

dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad previstas en el RDLOPD.

La empresa deberá considerar la participación de personal interno experto en la materia (por ejemplo, departamento de auditoría interna, en caso de existir), o bien contratar los servicios de un auditor externo con conocimientos en esta área.

En la realización de la auditoría se tendría que tener en cuenta:

- El cumplimiento que el responsable del fichero de datos personales hace de las medidas que se describen en este reglamento.
- La adecuación a la normativa de protección de datos vigentes en cada momento del documento de seguridad y los procedimientos que establezca.

La auditoría terminará con un informe que abarcará los siguientes aspectos:

- Adecuar las medidas y controles de seguridad de los datos personales implantados por el responsable a la ley y su desarrollo reglamentario destinados al personal y a los equipos y sistemas de información.
- Identificar las deficiencias encontradas en la auditoría, y en su caso, proponer las medidas necesarias para paliar las deficiencias.
- Especificar las diferentes evidencias derivadas de la auditoría sobre las que se basen los dictámenes y recomendaciones propuestas.
- El informe de auditoría deberá ser analizado por el responsable de seguridad que comunicará las conclusiones al responsable del fichero para que adopte las medidas correctoras necesarias.
- Este informe deberá quedar a disposición de la Agencia de Protección de Datos, o en su caso, de las autoridades de control de las comunidades autónomas.

Deberá realizarse dicha auditoría con carácter extraordinario siempre que se efectúen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad.

Nota

Esta medida de seguridad es muy importante, ya que no solo establece las medidas de seguridad en la entidad que gestiona si no también las medidas de control que muestran la adecuación de las medidas implantadas en el documento de seguridad. (Art. 96 del R.D. 1720/2007).

Gestión de soportes y documentos

La gestión de soportes establece una serie de cuestiones adicionales a su medida análoga de nivel básico:

Se deberá disponer de un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer las siguientes cuestiones:

- Tipo de documento o soporte.
- Fecha y hora de entrada del documento o soporte.
- El emisor del soporte.
- El número de documentos o soportes en el envío.
- El tipo de información que contienen.
- Forma de envío de los documentos o soportes.
- Persona que se encarga de la recepción del soporte y que debe estar autorizada para ello. Debe reflejarse así en el documento de seguridad.

Además se deberá disponer también de un registro de salida de soportes informáticos que permita conocer los siguientes aspectos:

- Tipo de documento o soporte.
- Fecha y hora de salida del documento o soporte.
- Destinatario del soporte.
- Número de documentos o soportes en el envío.
- Tipo de información que contienen los documentos o soportes.

- Forma de envío de los documentos o soportes.
- Persona que se encarga de la emisión del soporte y que debe estar autorizada para ello, lo que debe constar en el documento de seguridad. (Art. 97 del R. D. 1720/2007).

NOMBRE DE LA EMPRESA	**REGISTRO Y AUTORIZACIÓN DE ENTRADA DE SOPORTES**
ENTRADA DEL SOPORTE: 000003	Fecha: Hora:
SOPORTE	
Tipo de soporte y número	
Contenido	
Fecha de creación	
ORIGEN Y FINALIDAD	
Finalidad	
Origen	
FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	
AUTORIZACIÓN	
Persona responsable de la recepción	
Cargo\Puesto	
Observaciones	
Firma	

Modelo de registro y autorización de entrada de soportes

Identificación y autenticación

Se refuerza la medida de identificación y autenticación que se prevé en el nivel de seguridad básico.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información, lo que supone bloquear el identificador de usuario después de un número limitado de intentos de acceso.

Nota

Lo que se pretende con esta medida de nivel medio es tener a todos los usuarios del sistema controlados, y evitar la posibilidad de un acceso no autorizado a los datos. (Art. 98 del R. D. 1720/2007).

Control de acceso físico

Se establecen medidas físicas para garantizar un control de acceso a los locales donde se ubiquen los sistemas de información con datos personales. Los usuarios que pueden acceder físicamente a estos lugares deben de identificarse en el documento de seguridad. (Art. 99 del R. D. 1720/2007).

Registro de incidencias

Esta medida de seguridad establece una serie de cuestiones adicionales a su medida análoga de nivel básico regulada en el art. 90 del reglamento. Establece cómo se deberán consignar los procedimientos realizados de recuperación de los datos, indicando lo siguiente:

- La persona que ejecutó el proceso.
- Los datos restaurados.
- Los datos que han sido necesarios grabar manualmente en el proceso de recuperación.

Para poder ejecutar los procedimientos de recuperación de los datos será necesaria la autorización del responsable del registro.

<table>
<tr><td colspan="2">EMPRESA</td><td colspan="2">Impreso de notificación de incidencias</td></tr>
<tr><td colspan="3">Incidencia Nº: 0000002 (A cumplimentar por responsable seguridad)</td><td></td></tr>
<tr><td colspan="4">Fecha de notificación:</td></tr>
<tr><td colspan="2">Tipo de incidencia:</td><td colspan="2">Fecha y hora en que se produce /detecta *

(* tachar lo que no proceda)</td></tr>
<tr><td colspan="4">Descripción detallada de la incidencia:</td></tr>
<tr><td colspan="4">Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)</td></tr>
<tr><td colspan="4">Recuperación de datos: (Procedimiento realizado: Datos restaurados: Datos grabados manualmente):

Persona que ejecutó el proceso:
Firma del Responsable del fichero: Fdo:</td></tr>
<tr><td colspan="2">Persona(s) a quien(es) se comunica:</td><td colspan="2">Persona que realiza la comunicación:

Fdo:</td></tr>
<tr><td colspan="2">NOTIFICACIÓN A PERSONAL TÉCNICO:

Fecha
Hora</td><td colspan="2">CORRECCIÓN DE LA ANOMALÍA:

Fecha Hora</td></tr>
<tr><td colspan="4">¿SE APLICAN MEDIDAS CORRECTORAS? SI ☐ NO ☐</td></tr>
<tr><td rowspan="2">SEGUIMIENTO</td><td>DESCRIPCIÓN:</td><td colspan="2">ACCIONES A REALIZAR:</td></tr>
<tr><td>COMPROBACIÓN DE LA EFICACIA</td><td colspan="2">REALIZADA POR:

Firma y Fecha</td></tr>
</table>

Modelo de notificación de incidencias

Medidas de seguridad nivel alto

Las medidas de nivel alto se desarrollan a lo largo del Capítulo III, en la Sección 3ª del reglamento. Estas medidas deberán contenerse en el documento de seguridad e implementadas por la organización que gestione datos personales altamente protegidos, es decir, datos de:

- Ideología.
- Religión.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.
- Datos recabados para fines policiales y sin el consentimiento de los afectados.
- Datos derivados de actos de violencia de género.
- Datos de tráfico y de localización de los ficheros de los que son responsables los operadores que presten servicios de comunicaciones electrónicas.

Recuerde

Todos los ficheros que contengan estos datos personales deberán reunir, además de las medidas de seguridad de nivel básico y las de nivel medio, las medidas calificadas de nivel alto.

Gestión y distribución de soportes

La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles que permitan a los usuarios, con acceso autorizado a dichos soportes y documentos, identificar su contenido y que dificulten la identificación para el resto de personas.

Siempre que exista una distribución de soportes que contenga datos personales altamente protegidos, las informaciones que contengan estos soportes deberán encontrarse cifradas (existen diferentes técnicas de cifrado de información). Es un método seguro porque a través de una clave se podrá cifrar una información, pero aparecerá en forma de caracteres y símbolos sin sentido. El art. 101 del reglamento da libertad a la hora de elegir un mecanismo para evitar la manipulación de estos datos tan sensibles, por lo que se podrá utilizar cualquier otro mecanismo diferente al cifrado de los datos siempre que se garantice la ininteligibilidad y la no manipulación en el momento en que el soporte se esté transportando.

Consejo

Se recomienda la utilización de las técnicas de cifrado para evitar las complicaciones técnicas, ya que el cifrado se encuentra hoy muy estandarizado y normalizado.

También se cifrarán los datos que contengan los dispositivos portátiles cuando estos se encuentren fuera de las instalaciones que estén bajo el control del responsable del fichero. Deberá evitarse el tratamiento de datos de carácter personal en los dispositivos portátiles cuando no permitan su cifrado, y en el caso de que sea estrictamente necesario se hará constar este hecho en el documento de seguridad exponiendo las causas por las que se lleva a cabo, además se adoptarán las medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Lo que pretende esta medida es evitar el acceso a los datos por parte de terceros no autorizados cuando los soportes estén siendo transportados. (Art. 101 del R. D. 1720/2007).

Copias de respaldo y recuperación

Con el art. 102 del reglamento se pretenden potenciar las medidas de copias de respaldo y recuperación de nivel básico. Lo que quiere decir es que estas copias deben ser almacenadas en un lugar de acceso restringido diferente al lugar donde se encuentran los sistemas informáticos y servidores que contienen datos altamente protegidos, con el objetivo de proporcionar una protección adicional en el caso, por ejemplo, de catástrofes naturales (inundaciones, incendios, etc.). El lugar de almacenamiento debe cumplir con las normas del reglamento que le sean aplicables o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Registro de accesos

Se potencian más aún las medidas de identificación y autenticación y de control de accesos de los niveles básico y medio.

Cuando un usuario acceda a un sistema que contiene datos personales de nivel alto se deberá realizar un registro de accesos en el que se contengan al menos los siguientes puntos:

- Identificación del usuario que ha accedido.
- Fecha y hora en que se ha accedido.
- Fichero al que se ha accedido.
- El tipo de acceso:
  - Acceso para consultar datos.
  - Acceso para modificar datos.
  - Acceso para suprimir datos.
  - Acceso para introducir datos.
- Si el acceso ha sido autorizado o denegado. Si ha sido autorizado se deben registrar las informaciones necesarias para identificar los datos a los que se ha accedido.

Nota

Las informaciones que se contienen en el registro de accesos deben ser guardados por un periodo mínimo de 2 años.

El responsable de seguridad tiene tres funciones en relación al registro de accesos:

- Debe tener el control directo del registro de accesos sin que deba permitir la desactivación ni la manipulación de los mismos.
- Debe revisar periódicamente las informaciones contenidas en el registro de accesos. El periodo de revisión mínimo está previsto que sea de un mes.
- Elaboración de un informe al menos mensual de las revisiones que se han realizado y de los problemas que se hayan producido.

No será necesario el registro de accesos cuando concurran las siguientes circunstancias:

- Qué el responsable del fichero o del tratamiento sea una persona física.
- Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las circunstancias anteriores deberá hacerse constar en el documento de seguridad. (Art. 103 del R. D. 1720/2007).

Telecomunicaciones

Para entender las medidas de seguridad se definen una serie de conceptos:

- **Telecomunicación:** es toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier

naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

- **Red de telecomunicaciones:** son los sistemas de transmisión y los equipos de conmutación y demás recursos que permitan la transmisión de señales entre puntos de terminación definidos mediante cable, medios ópticos o de otra índole. La red de telecomunicaciones más importante es Internet.

  Sabía que: una red LAN, o lo que es lo mismo, una red interna que solo opera dentro de un edificio o entre unas oficinas no se considera una red de telecomunicaciones.

Lo establecido en el art. 104 del reglamento obliga a que siempre que exista una transmisión de datos personales a través de redes públicas y redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

En telecomunicaciones ocurre lo mismo que en la medida de nivel alto referente a la distribución de soportes: no tiene por qué utilizarse el mecanismo del cifrado ya que el legislador da libertad a la hora de elegir otro procedimiento siempre que la ininteligibilidad y la no manipulación de los datos personales estén garantizadas durante la transmisión de estos.

2.2. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Antes de establecer cuáles son las medidas que se han de tomar para proteger la información contenida en los ficheros no automatizados es conveniente definir una serie de conceptos:

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

Están incluidos dentro de este concepto los ficheros de datos personales que almacenan la información en documentos en formato papel y que se gestionan manualmente a través de carpetas y archivadores siempre y cuando estén estructurados conforme a criterios relativos a personas físicas y siempre que dichos criterios permitan acceder sin esfuerzos al contenido de la información.

Ejemplo

El mejor ejemplo de un fichero no automatizado está en los archivadores existentes en la mayoría de las organizaciones en los que se almacenan expedientes de documentos organizados por personas físicas (empleados, clientes, proveedores, etc.) y se estructuran de manera que se puede localizar cada expediente utilizando criterios relativos a personas físicas (búsqueda alfabética, por nombre o apellidos, por ejemplo).

Medidas de nivel básico

El nuevo reglamento incluye en su ámbito de aplicación a los ficheros automatizados (papel), estableciendo su regulación en el Capítulo IV. Además de las medidas de seguridad establecidas en este capítulo se deben aplicar las disposiciones comunes dispuestas en los Capítulos I y II del reglamento destinadas a ficheros automatizados y no automatizados, y por último deben aplicarse las medidas de seguridad de nivel básico para los ficheros automatizados en cuanto a:

- Funciones y obligaciones del personal.
- Registro de incidencias.
- Control de acceso.
- Gestión de soportes.

Las medidas propias o específicas de este tipo de ficheros se describen a continuación.

Criterios de archivo

Tratándose de documentación en soporte papel, el Reglamento de Protección de Datos establece que su archivo deberá realizarse de acuerdo con unos criterios que garanticen su correcta conservación, localización y consulta de la información e implica disponer de pautas concretas para el archivo (criterio alfabético, cronológico, cronológico inverso, etc.), y además se han de utilizar criterios que permitan el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Para determinar dichos criterios de archivo, estos se deberán ajustar, en primer lugar, a los previstos en la legislación específica que regula determinados tipos de ficheros (como puede ser el caso del archivo de facturas, los libros de los registros civiles, o las historias clínicas).

Nota

Cuando no exista ninguna normativa aplicable deberá ser el propio responsable del fichero quien establezca los criterios y procedimientos de actuación que deban seguirse para el archivo. (Art. 106 del R. D. 1720/2007).

Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura, lo que se traduce en la necesidad de que todos aquellos armarios, archivadores, cajones y demás dispositivos análogos en los que vayan a guardarse este tipo de documentos estén provistos de cerraduras con llave o de cualquier otra medida de cierre similar. (Art. 107 R. D. 1720/2007).

Si las características físicas de dichos dispositivos de almacenamiento no permiten adoptar esta medida, el responsable del fichero o tratamiento

adoptará medidas que impidan el acceso de personas no autorizadas a la documentación, para evitar que dicha información sea utilizada o manipulada para fines distintos para los que se obtuvieron.

Custodia de soportes

Cuando la documentación con datos de carácter personal no esté archivada en sus dispositivos de almacenamiento porque se esté trabajando con ella, la persona que se encuentre a su cargo deberá custodiarla e impedir en todo momento que pueda acceder a la misma alguna persona no autorizada. Se trata de una medida que impone una actitud de cautela al personal con acceso a la documentación. (Art. 108 del R. D. 1720/2007).

Medidas de seguridad de nivel medio

Para implantar las medidas de nivel medio es necesario adoptar unas determinadas disposiciones. Estas se muestran a continuación.

El responsable de seguridad

Se trata de la misma figura ya vista para los ficheros automatizados (art. 95 del R. D. 1720/2007), por lo que la misma persona designada para controlar la aplicación de las medidas de seguridad relativas a aquellos ficheros podría también hacerse cargo de la supervisión de los no automatizados.

Auditoría

Los ficheros no automatizados también deben someterse a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad que les son aplicables y que, como mínimo, deberá realizarse cada dos años. Como es lógico, en una misma auditoría pueden revisarse tanto los ficheros automatizados como los no automatizados, no siendo necesaria la realización de dos auditorías separadas.

La auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes

en la organización, y evitar que se puedan manipular o dar un uso distinto a los datos contenidos en este tipo de ficheros.

Medidas de seguridad de nivel alto

Aquellos ficheros no automatizados que contengan datos de nivel alto, además de las medidas de seguridad de nivel básico y medio ya vistas, deberán someterse también a otro tipo de medidas. Estas se muestran a continuación.

Almacenamiento de la información

Cuando los ficheros no automatizados contengan datos de nivel alto, el Reglamento de Protección de Datos establece que los armarios, archivadores u otros elementos en los que estos se almacenen 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. Dichas áreas deberán permanecer cerradas cuando no sea preciso acceder a los documentos incluidos en el fichero.

En cualquier caso, cuando las características de los locales del responsable del fichero o tratamiento no permitan adoptar esta medida, este tendrá que adoptar medidas alternativas que deberán incluirse detallada y motivadamente en el documento de seguridad. (Art. 111 del R. D. 1720/2007).

Copia o reproducción

En este nivel de seguridad, la generación de copias o la reproducción de los documentos únicamente podrán realizarse bajo el control del personal autorizado para ello en el documento de seguridad, por lo que se restringe la posibilidad de que puedan darse copias no controladas de la documentación con datos especialmente sensibles.

Por otro lado, la destrucción de dichas copias o reproducciones deberá realizarse de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Consejo

Así, para el correcto cumplimiento de esta medida, se recomienda el uso de destructoras de papel, o bien, para elevados volúmenes de documentación desechada, la contratación de un servicio de recogida y destrucción de papel correctamente gestionado. (Art. 112 del R. D. 1720/2007).

Acceso a la documentación

Se establece que el acceso a la documentación debe quedar exclusivamente restringido al personal autorizado. Para ello, es necesaria la implementación de mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

Cuando sea un único usuario quien esté autorizado a acceder al fichero no será obligatorio el mantenimiento del registro de accesos, pero tal circunstancia deberá quedar adecuadamente registrada en el documento de seguridad. (Art. 113 del R. D. 1720/2007).

Traslado de documentación

El Reglamento de Protección de Datos impone que siempre que se proceda al traslado físico de la documentación contenida en un fichero, este se lleve a cabo bajo la adopción de medidas dirigidas a impedir el acceso o manipulación de la información que se traslada.

La concreción de las referidas medidas durante el traslado puede ser muy variada, desde el transporte en cajas cerradas y/o precintadas, hasta la constante supervisión del traslado por parte de una o varias personas. (Art. 114 del R. D. 1720/2007).

2.3. Medidas de seguridad aplicables tanto a los ficheros y tratamientos automatizados como a los ficheros y tratamientos no automatizados en los distintos niveles de protección

Disposiciones comunes a ambos ficheros

Documento de seguridad

Concepto

El documento de seguridad es un documento privado pero de acceso público en el que se señalan las políticas de seguridad que se van a seguir por quienes traten datos personales, es decir, recogerá las medidas de índole técnica y organizativa que será de obligado cumplimiento para el personal con acceso a los datos. El documento de seguridad está regulado en el art. 88 para todos los niveles.

Recuerde

Es obligatorio adoptar el documento de seguridad, sea cual sea el nivel de seguridad que corresponda.

El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada uno de ellos.

También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso tendrá el carácter de documento interno de la organización.

Estructura y contenido

El documento de seguridad deberá contener como mínimo los siguientes aspectos:

- Ámbito de aplicación del documento de seguridad con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
- Funciones y obligaciones del personal que tiene acceso a los datos.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimientos de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o la reutilización de los mismos.

En el supuesto de que fuera de aplicación a los ficheros de medidas de seguridad de nivel medio o alto, el documento de seguridad deberá contener:

- La identificación del responsable o responsables de seguridad.
- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el documento.

Cuando exista un tratamiento de datos por cuenta de terceros, el documento deberá contener la identificación de los ficheros o tratamientos que se manejen en concepto de encargo con referencia expresa al contrato o documento que regule las condiciones del encargo, así como la identificación del responsable y del período de vigencia del encargo.

En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en el documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado el manejo del documento de seguridad, salvo lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del art. 12 de la Ley Orgánica de Protección de Datos, con especificación de los ficheros o tratamientos afectados.

El contenido del documento de seguridad debe adecuarse a los cambios de las leyes o reglamentos en materia de seguridad de los datos personales.

Nota

El documento debe mantenerse siempre actualizado y se tiene que revisar siempre que haya cambios importantes en el sistema de información o en la organización del sistema de información.

El responsable del fichero es quien tiene la obligación de realizar el documento de seguridad. En él se tienen que establecer todas las medidas de seguridad que tienen que cumplirse obligatoriamente por las personas que acceden a los datos y los sistemas informáticos.

Control del cumplimiento

De nada serviría disponer de un documento de seguridad si no se controla que, efectivamente, lo que se indica en el mismo cumple lo que dispone el reglamento y que además es lo que se viene realizando en la práctica.

Si los controles se establecen correctamente, su seguimiento se convierte en una auditoría continua, con las ventajas que esto conlleva.

Prestación de servicios sin acceso a datos personales

Se tratará de limitar el acceso de los trabajadores a los datos personales, a los soportes que los contengan, y a los recursos de los sistemas de información cuando se pretendan realizar trabajos que no impliquen el tratamiento de datos personales. Además, cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación de servicios. (Art. 83 del R. D. 1720/2007).

Delegaciones de autorizaciones

Las autorizaciones que se le atribuyen al responsable del fichero o tratamiento podrán ser delegadas en otras personas. Deberá de constar en el documento de seguridad las personas habilitadas para otorgar estas autorizaciones, así como aquellas sobre las que recae la delegación. En ningún momento esto supone una delegación de la responsabilidad del responsable del fichero. (Art. 84 del R. D. 1720/2007).

AUTORIZACIÓN

EMPRESA: _____.

Nombre de quien otorga la autorización y

NIF_____, cuyas competencias son_____,

autoriza a **Nombre de la persona autorizada y NIF**_____, desde **Fecha**_____hasta **Fecha**_____, a **Tipo** de autorización_____ con alcance (pleno o parcial) _____.

OBSERVACIONES (si las hubiera): _____

Ejemplo de autorización

Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento

Cuando los datos personales se traten fuera de los locales del responsable del fichero o tratamiento, o del encargado del tratamiento, o dichos datos se almacenen en dispositivos portátiles se exigirá la autorización previa del responsable del fichero y deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. La autorización tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios. Se determinará un periodo de validez para dicha autorización. (Art. 86 del R. D. 1720/2007).

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

En Málaga, a 22 de junio de 2010

REUNIDOS

De una parte, D/Dª_____ con DNI _____ actuando en nombre y representación de la entidad_____, con C.I.F_____, y domicilio en _____ CP _____ y asumiendo en adelante las funciones de **Encargado de tratamiento.**

Y de otra parte:

Don _____, con DNI _____, actuando en nombre y representación de la entidad _____con C.I.F _____, y domicilio en _____CP _____, asumiendo en adelante las funciones de Responsable del fichero.

Ambas partes, en la calidad en que actúan, se reconocen mutua y legal capacidad para obligarse cuanto a derecho sea menester y acuerdan celebrar el presente **CONTRATO DE ACCESO POR CUENTA DE TERCEROS,**

Continúa en página siguiente >>

<< Viene de página anterior

EXPONEN

I.- Que el Responsable del Fichero es una entidad cuya actividad es _____(ACTIVIDAD DE LA EMPRESA)

II.- Que el Encargado de Tratamiento es una entidad cuya actividad se centra en la prestación de servicios de_____(SERVICIOS PRESTADOS), habiendo sido contratado por el Responsable del Fichero para la prestación de este servicio.

III.- Que para el desarrollo de los servicios para los que ha sido contratado el Encargado de Tratamiento, tendrá el acceso a datos de carácter personal contenidos en los ficheros del Responsable del Fichero.

IV.- Que siendo así, ambas partes han acordado formalizar el presente contrato, en cumplimento de los dispuesto en el Art. 12 de la Ley Orgánica 15/ 1999, de 13 de diciembre de 1999, de protección de datos de carácter personal (en adelante LOPD), para regular, en lo relativo al tratamiento de los datos de carácter personal, la prestación de servicios mencionados, por parte del Encargado de Tratamiento.

De acuerdo con lo anterior, las partes acuerdan el presente contrato, que se regirá de conformidad a las siguientes:

Continúa en página siguiente >>

<< Viene de página anterior

ESTIPULACIONES

P**rimera.- Objeto del contrato**

El objeto del presente contrato es el tratamiento por parte del Encargado de Tratamiento de los datos personales relativos a _____(TIPO DATO/ FICHERO), con la finalidad de prestarle los servicios de _____ (SERVICIOS PRESTADOS).

En ambos supuestos, el Responsable del Fichero facilitará los datos que sean necesarios para la prestación del servicio acordado, y a los que se le dará el tratamiento de los mismos en conformidad con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, y 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.

Segunda.-Tratamiento de datos de carácter personal.

El Responsable del Fichero manifiesta que es titular de ficheros que contienen datos de carácter personal que han sido recabados legalmente, y que, en virtud de los servicios contratados al Encargado de Tratamiento, autoriza y delega su tratamiento, para la prestación de los servicios anteriormente indicados.

Tercera.-Datos a los que se da acceso y nivel de seguridad.

Los datos personales que forman parte de los ficheros del Responsable del Fichero a los que tendrá acceso el Encargado del tratamiento son aquellos que constan en _____(INDICAR FICHERO/S), siendo por tanto el Nivel de Seguridad de los mismos _____(NIVEL).

Continúa en página siguiente >>

<< Viene de página anterior

Cuarta.- Finalidad del tratamiento

El Encargado de Tratamiento, únicamente tratará los datos que se le han encomendado para realizar por cuenta del Responsable del Fichero la prestación de los servicios contratados y, en ningún caso, los utilizará para finalidades distintas a las acordadas.

Quinta.- Medidas de Seguridad

El Encargado de Tratamiento deberá aplicar a los datos contenidos en los Ficheros, las medidas de seguridad establecidas reglamentariamente 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, para así garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Sexta.- Comunicación de Datos a Terceros

Como norma general, el Encargado de Tratamiento no comunicará los datos de carácter personal a los que tiene acceso, en el marco del presente contrato, a un tercero, ni siquiera para su conservación.

En los casos en los que para la prestación de los servicios contratados sea necesario que el Encargado de Tratamiento facilite datos personales, que previamente haya puesto a su disposición el Responsable del Fichero, a entidades cuya intervención sea necesaria para dar cumplimiento a esta relación contractual, dichas entidades se verán sometidas a las mismas reglas de protección de datos y confidencialidad que el Encargado de Tratamiento.

Continúa en página siguiente >>

<< Viene de página anterior

Séptima.- Ejercicio de derechos.

En los casos en los que los titulares de los datos ejerciten sus derechos de acceso, rectificación, cancelación u oposición ante el Encargado de Tratamiento, este deberá dar traslado de la mencionada solicitud, en el plazo máximo de tres días, al Responsable del Fichero a fin de que por el mismo se resuelva, en los plazos establecidos por la normativa vigente.

Octava.- Deber de información mutuo.

Ambas partes, de acuerdo con los dispuesto por la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, se informarán mutuamente de que los datos de las personas de contacto que figura en el encabezamiento del presente contrato, serán incorporados a los ficheros de titularidad de cada una de las partes con finalidad de gestionar dicha relación.

Novena.- Deber de conservación.

El Encargado de Tratamiento conservará los datos de carácter personal a los que haya tenido acceso en razón del servicio prestado, así como cualquier soporte o documento en el que consten, durante el tiempo en que esté vigente dicho servicio o porque así lo disponga la Ley. Finalizado este o resuelto el presente contrato, los datos serán destruidos en su totalidad o devueltos al responsable del fichero, teniendo en cuenta los distintos soportes o documentos donde estos puedan constar: base de datos en discos, ficheros temporales, copias de seguridad, soportes en papel…etc.

Una vez se haya realizado la operación mencionada en el punto anterior, el Encargado del Tratamiento se compromete a entregar una declaración por escrito al Responsable del fichero donde conste que así se ha realizado.

Continúa en página siguiente >>

<< Viene de página anterior

Décima.- Responsabilidad

El Encargado de Tratamiento se compromete a cumplir con las obligaciones establecidas en el presente contrato y en la normativa vigente, en relación con el presente Encargo de tratamiento.

Igualmente, queda exonerado de cualquier responsabilidad que pueda sobrevenirle como consecuencia de inexactitudes, ocultaciones y omisiones en los datos e informes que se le proporcione para la prestación de servicio convenido, no respondiendo de la veracidad de los mismos.

Décimo primera - Totalidad de pactos y conservación de contrato.

El presente documento contiene todos los pactos que gobiernan la relación jurídica entre ambas partes. Cualquier modificación de los mismos deberá ser acordado previamente por ambas partes, debiéndose suscribir un documento al efecto.
En todo caso, en el supuesto de que alguna de las estipulaciones que se contienen en el mismo fuese anulada por decisión judicial o arbitral, ello no afectará a las demás estipulaciones, manteniéndose el contrato plenamente vigente en todo lo no expresamente declarado nulo o anulado. Asimismo, las estipulaciones declaradas nulas o anuladas serán sustituidas por otras que sean válidas y que recojan, dentro de lo posible, y de la manera más parecida posible, el contenido, de las estipulaciones nulas o anuladas.

Continúa en página siguiente >>

<< Viene de página anterior

Décimo segunda.- Cláusula de confidencialidad

En virtud del presente contrato las partes contratantes se obligan a no divulgar ni revelar los datos, especificaciones técnicas, secretos, métodos o sistemas, y en general, cualquier mecanismo relacionado con la información a la cuál tenga acceso y que le sea revelada para la prestación del servicio contratado, en consecuencia se obliga a mantener absoluta confidencialidad de la información que se maneje durante la vigencia de este contrato, y hasta por 5 años después de concluido el mismo, en caso de existir duda sobre si determinada información es considerada como secreto comercial, deberá ser tratada como confidencial.

Ambas partes se obligan expresamente a utilizar todas las medidas que fueren necesarias y convenientes para que su personal cumpla y observe dicha confidencialidad, absteniéndose de divulgar o reproducir total o parcialmente la información que obtenga o produzcan con motivo de la prestación de servicios contenida en el presente contrato.

Los datos, información y resultados que sean revelados por las partes contratantes, son propiedad de cada una de ellas y constituyen secreto industrial, entiéndase por tal cualquier información, incluida pero no limitada, a datos técnicos y no técnicos, fórmulas, prototipos, compilaciones, programas, dispositivos, métodos, técnicas, procesos gráficos, información financiera o listas de los clientes reales o potenciales, así como los proveedores, y por lo tanto ambas partes quedan sujetas a lo establecido por nuestro ordenamiento legal, por lo que no podrán divulgarlas sin la autorización expresa y por escrito de la otra parte, aceptando desde este momento que la violación o incumplimiento de los dispuesto en la presente cláusula, podrá encuadrarse dentro de los supuestos contemplados dentro de las infracciones comprendidas en las leyes civiles y penales correspondientes.

Expresamente convienen las partes en que no se considerará información confidencial aquella que sea de dominio público en la fecha que esta sea publicada. Ambas partes convienen así mismo en que la información contenida en los catálogos de la base de datos se considera dominio público y no se considerará, para efectos de lo establecido en este contrato, como información confidencial.

Continúa en página siguiente >>

<< Viene de página anterior

Décimo tercera.- Duración y resolución del contrato.

El presente contrato tendrá una duración de _____ (DURACIÓN) a contar desde la fecha de formalización del mismo.

Décimo cuarta.- Ley aplicable y designación del fuero aplicable.

El presente contrato se regirá e interpretará conforme a la legislación española en aquello que no esté expresamente regulado, sometiéndose las partes, para las controversias que pudieran surgir en relación con el mismo, a la competencia de los Juzgados y Tribunales de la ciudad de _____con renuncia a cualquier otro fuero que les pudiera corresponder.

Y en prueba de su conformidad, después de leer detenidamente el documento, siendo el número de páginas 5, las partes lo ratifican y firman por duplicado y a un solo efecto, en el lugar y fecha indicados.

EMPRESA S.L. **(QUE PRESTA EL SERVICIO)**	**EMPRESAS CLIENTE**
D./Dª (Encargado de Tratamiento)	D./Dª. (Responsable del Fichero)

Continúa en página siguiente >>

Creación de ficheros temporales o copias de trabajo de documentos

Son aquellos que se han creado exclusivamente para la realización de trabajos temporales o auxiliares.

Ejemplo

Realizar una copia de seguridad temporal ante un corte de suministro que detenga repentinamente el sistema.

Deberán cumplir el nivel de seguridad que les corresponda conforme a lo establecido en el art. 81 del reglamento.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación. (Art. 87 del R. D. 1720/2007).

3. Plazos de implantación de las medidas de seguridad

3.1. Plazo para implantar las medidas de seguridad en ficheros automatizados

Los ficheros que existiesen en la fecha de entrada en vigor del Real Decreto 1720/2007, de 21 de diciembre, regulador de la Ley Orgánica de Protección de Datos deberán implantar:

a. En el plazo de un año desde su entrada en vigor las medidas de seguridad del nivel medio exigibles a los siguientes ficheros:

   - Los ficheros de los que sean responsables las entidades gestoras y servicios comunes de la seguridad social.
   - Los ficheros de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la seguridad social.
   - Los ficheros que contengan un conjunto de datos de carácter personal, que ofrezcan una definición de las características o de la personalidad de los ciudadanos, y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

b. En el plazo de un año desde su entrada en vigor, las medidas de nivel medio, y en el plazo de dieciocho meses, las de nivel alto para los siguientes ficheros:

   - Los que contengan datos derivados de actos de violencia de género.
   - De los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas, respecto de los datos de tráfico y a los datos de localización.

En el supuesto de que el nuevo reglamento exija la implantación de una medida adicional no prevista en el anterior reglamento (Real Decreto 994/1999, de 11 de junio) dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del R. D.

Los ficheros automatizados creados con posterioridad a la fecha de entrada en vigor del R. D. deberán tener implantadas las medidas desde el día de su creación.

3.2. Plazos para implantar las medidas de seguridad en ficheros no automatizados

Los ficheros no automatizados que existieran en la fecha de entrada en vigor del nuevo R.D. deberán implantar:

- Las medidas de seguridad de nivel básico en el plazo de un año desde su entrada en vigor.
- Las medidas de seguridad de nivel medio en el plazo de dieciocho meses de su entrada en vigor.
- Las medidas de seguridad de nivel alto en el plazo de dos años desde su entrada en vigor.

Los ficheros no automatizados creados con posterioridad a la fecha de entrada en vigor del nuevo R. D. deberán tener implantadas desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Todos estos plazos están recogidos en la **Disposición Transitoria Segunda** del Real Decreto 1720/2007, de 21 de diciembre, regulador de la Ley de Orgánica de Protección de Datos.

A continuación se muestra un cuadro resumen de los plazos de implantación de las medidas, tanto en ficheros automatizados como no automatizados.

	PLAZO PARA LA IMPLANTACIÓN DE LAS MEDIDAS DE SEGURIDAD DESDE LA ENTRADA EN VIGOR DEL RD 1720/2007 DE 21 DE DICIEMBRE	
	Ficheros automatizados	**Ficheros no automatizados**
Nivel básico		1 año
Nivel medio	1 año	18 meses
Nivel alto	18 meses	2 años

4. Infracciones y sanciones de la LOPD

El art. 43 establece que la responsabilidad recaerá siempre sobre los responsables de los ficheros y los encargados de los tratamientos que también responderán atendiendo a las infracciones en que hayan incurrido personalmente.

La LOPD personaliza a la hora de las responsabilidades. En el tratamiento de los datos de cualquier entidad intervienen terceras personas que pueden ser ellas quienes cometan una infracción, pues bien, a pesar de que la responsabilidad recaiga sobre la persona que cometió la infracción administrativa, el responsable directo debe ser el responsable o el encargado de tratamiento.

Las infracciones recogidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, han sido modificadas por la Disposición Final Quincuagésima Sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

Los artículos que han sufrido algún tipo de modificación son los siguientes:

- Art. 43.2.
- Art. 44, apartados 2 a 4.
- Art. 45 apartados 1 a 5 y se incluye un nuevo apartado 6, pasando los actuales apartados 6 y 7 a ser los apartados 7 y 8 del mencionado artículo.
- Art. 46, apartados 1 a 3.
- Art. 49.

4.1. Infracciones de la LOPD

Las infracciones de la LOPD se clasifican en leves, graves y muy graves y están recogidas en el art. 44.1 de la LOPD.

A continuación se mostrará cómo han quedado redactados los apartados del 2 al 4 del art. 44 de la LOPD y la sanción que corresponda a cada tipo de infracción.

Infracciones leves. Nuevo art. 44.2 LOPD	**Sanciones**	
	Mínimo	**Máximo**
No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo. No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos. El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado. La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.	**900 €**	**40.000 €**

Infracciones graves. Nuevo art. 44.3 LOPD	Sanciones	
	Mínimo	Máximo
Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente. Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave. La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley. El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición. El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado. El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo. Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.	**40.001 €**	**300.000 €**

Infracciones graves. Nuevo art. 44.3 LOPD	Sanciones	
	Mínimo	Máximo
No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma. La obstrucción al ejercicio de la función inspectora. La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.	**40.001 €**	**300.000 €**

Infracciones muy graves. Nuevo art. 44.4 LOPD	Sanciones	
	Mínimo	Máximo
La recogida de datos en forma engañosa o fraudulenta. Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7. No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello. La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.	**300.001 €**	**600.000 €**

4.2. Las sanciones en la LOPD

Las sanciones en materia de protección de datos se regulan en el art. 45 de LOPD, artículo que ha sido modificado por la disposición final quincuagésima sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

En este nuevo artículo se establecen las siguientes sanciones:

Infracción	Sanción
Leve	Entre 900 a 40.000 €
Grave	Entre 40.001 a 300.000 €
Muy grave	Entre 300.001 a 600.000 €

La cuantía de las sanciones mencionadas anteriormente se graduará atendiendo a los siguientes criterios:

- El carácter continuado de la infracción.
- El volumen de los tratamientos efectuados.
- La vinculación de la actividad del infractor con la realización de tratamientos de datos.
- El volumen de negocio o actividad del infractor.
- Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- El grado de intencionalidad.
- La reincidencia por comisión de infracciones de la misma naturaleza.
- La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
- La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de datos de carácter personal, siendo la infracción consecuencia de una anomalía en el

funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
- Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios mencionados anteriormente, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que en el plazo que el órgano sancionador determine acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

- Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en la ley.
- Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Nota

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

- Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados anteriormente.

- Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
- Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
- Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.
- Cuando el infractor haya reconocido espontáneamente su culpabilidad.

Otra medida que puede tomar el órgano sancionador, además de ejercer la potestad sancionadora, en los supuestos constitutivos de infracción grave y muy grave en el que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y en particular, de su derecho a la protección de datos de carácter personal, es requerir a los responsables de los ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

4.3. Sanciones para las administraciones públicas

Para las administraciones públicas se establece un régimen sancionador específico que aparece regulado en el art. 46 de la LOPD y que ha sido modificado por la Disposición Final Quincuagésima Sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

El contenido del mencionado artículo es el siguiente:

Cuando las infracciones fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador puede proponer dos tipos de actuaciones:

1. Dictar una resolución en la que se propongan medidas a adoptar para que:

   - Cesen los efectos de los hechos infractores.
   - Se corrijan los efectos derivados de la infracción.

   Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente, y a los afectados si los hubiera.

2. Podrá proponer la iniciación de actuaciones disciplinarias si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre el régimen disciplinario de las administraciones públicas.

Recuerde

Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4.4. El procedimiento sancionador

Iniciación del procedimiento

Antes de iniciar el procedimiento sancionador se podrán llevar a cabo actuaciones previas con el objeto de determinar si existen circunstancias que justifiquen la iniciación del procedimiento (como los hechos que pueden dar lugar a la iniciación, identificación de la persona u órgano que pudiera resultar responsable, o fijar las circunstancias que pudieran ser relevantes en el caso).

Las actuaciones previas se llevarán a cabo de oficio por la Agencia de Protección de Datos bien por:

- Iniciativa propia.
- Como consecuencia de la existencia de una denuncia.
- Por la petición razonada de otro órgano.

Las actuaciones previas tendrán una duración máxima de doce meses a contar desde que la denuncia o petición razonada fuera puesta en conocimiento de la Agencia de Protección de Datos o, de no existir estas, desde que el director de la Agencia de Protección de Datos acordase la realización de dichas actuaciones.

El ejercicio de las funciones inspectoras será llevado a cabo por el personal del área de la inspección de datos, pero existen excepciones, en la que el director de la Agencia podrá designar para la realización de las actuaciones a funcionarios de la Agencia no habilitados para el desempeño de las mismas o funcionarios que no presten sus funciones en la Agencia, siempre y cuando reúnan las condiciones de idoneidad y especialización necesarias para la realización de tales actuaciones.

Los inspectores podrán recabar cuantas informaciones sean necesarias para cumplir con su cometido. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas, etc.

También se podrán realizar visitas de inspección por parte de los inspectores en los locales o sedes del inspeccionado o en su propio domicilio o donde se encuentren ubicados los ficheros.

Los inspectores deben ser autorizados por el director de la Agencia de Protección de datos, dicha autorización debe indicar:

- La habilitación del inspector autorizado.
- La identificación de la persona u órgano inspeccionado.

Las inspecciones concluirán con el levantamiento de la correspondiente acta en la que deberán constar las actuaciones practicadas durante la visita o visitas de inspección.

El acta se emitirá por duplicado y será firmada por los inspectores actuantes y por el inspeccionado que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente. Se le entregará al inspeccionado uno de los originales.

Una vez que han finalizado las actuaciones previas, el director de la Agencia de Protección de Datos decidirá si existen razones para imputar la comisión de una infracción. En el caso de que así sea se dictará acuerdo de inicio de procedimiento sancionador o de infracción de las administraciones públicas. En el supuesto de que no existan indicios que motiven la iniciación de un procedimiento sancionador, el director de la Agencia de Protección de Datos dictará resolución de archivo que notificará al inspeccionado y al denunciante en su caso.

El acuerdo de inicio del procedimiento sancionador deberá contener:

a. Identificación de la persona o personas presuntamente responsables.
b. Una descripción de los hechos imputados.
c. Indicación de que el órgano competente para resolver el procedimiento es el director de la Agencia de Protección de Datos.
d. Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.
e. Designación de instructor o en su caso secretario, indicando el régimen de recusación de los mismos.
f. Indicación expresa del derecho que el responsable tiene a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.
g. Indicar las medidas de carácter provisional que pudieran acordarse.

Nota

El plazo para dictar una resolución será el que determinen las normas del procedimiento sancionador y se computará desde la fecha en que se produce el acuerdo de inicio hasta la notificación de la resolución sancionadora. Una vez que haya finalizado el plazo sin que se dicte resolución se producirá la caducidad del procedimiento y el archivo de las actuaciones.

4.5. Prescripción

La prescripción se refleja en el art. 47 de la LOPD, tanto para las infracciones como para las sanciones.

En cuanto a las infracciones se distingue entre:

- Infracción leve, prescribe al año.
- Infracción grave, prescribe a los dos años.
- Infracción muy grave, prescribe a los tres años.

Se interrumpirá por:

- La iniciación del procedimiento sancionador.
- Si esta iniciación es con conocimiento del interesado.

Se reanudará el plazo de prescripción:

- Si el expediente sancionador estuviera paralizado más de seis meses.
- Por causas no imputables al presunto infractor.

Respecto a las sanciones, estas prescriben:

- A los tres años si se ha impuesto una infracción muy grave.
- A los dos años si se ha impuesto una infracción grave.
- Al año si se ha impuesto una infracción leve.

El plazo de prescripción comenzará a contar desde el día siguiente al que adquiera firmeza la resolución que impone la sanción, es decir, desde el día siguiente a la fecha que lleve la resolución. El plazo de prescripción se interrumpirá por la iniciación del procedimiento por el que se ejecuta el cobro de la sanción.

5. Casos prácticos

5.1. Caso práctico empresa A

En la empresa de telefonía móvil "LOPD Comunicaciones S.L." los datos tratados pertenecen al nivel de seguridad básico. Por esa razón, según el Real Decreto 1720/2007 habría que establecer las siguientes medidas de seguridad.

Medidas de nivel bajo para los ficheros

Documento de seguridad

El responsable del fichero (Pablo García García) elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Este documento deberá contener, como mínimo, los siguientes aspectos:

- Ámbito de aplicación del documento, con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

- Las medidas que sean necesarias adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes o la reutilización de estos últimos.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

El contenido del documento deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Funciones y obligaciones

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas en el documento de seguridad.

El responsable del fichero (Pablo) adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

En este caso práctico, Pablo informará al personal de cuáles son funciones y obligaciones de forma verbal y por escrito a través de correo electrónico con acuse de recibo de la información. También les remitirá de forma periódica información sobre seguridad a través de circulares cuando así lo requieran las circunstancias.

Las funciones y obligaciones definidas en el documento de seguridad para el ejemplo práctico son las siguientes:

El trabajador deberá:

- Guardar secreto y confidencialidad de la información tratada. Quienes intervienen en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto a los

datos y al deber de guardarlos, obligaciones que continúan incluso después de finalizar las relaciones con el responsable del fichero.

- No vulnerar el deber de secreto respecto a los datos personales tratados será considerado una falta leve, grave o muy grave conforme a lo previsto en el art. 44 de la LOPD, lo cual dará lugar al inicio de acciones disciplinarias, si proceden.
- Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.
- Los sistemas de información, recursos, y la información personal a la que se accede, solo se debe utilizar para las labores estrictamente profesionales que el usuario tiene asignadas.
- Facilitar el derecho de acceso, rectificación y cancelación a los titulares de los datos. Para ello se informará al responsable del fichero, responsable de seguridad o encargado del tratamiento y se recogerá siempre en solicitud escrita.

Registro de incidencias

Creación de un registro donde se haga constar cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos o ficheros.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

José Pérez García encargado de la venta al público ha detectado una anomalía: se ha perdido determinada información laboral.

EMPRESA	**Impreso de notificación de incidencias**
Incidencia Nº: **0000002** (A cumplimentar por Responsable Seguridad)	
Fecha de notificación: **30/05/2012**	
Tipo de incidencia: **Perdida de determinada información laboral**	Fecha y hora en que se produce /detecta * **29/05/2012 a las 12:00 h** (* tachar lo que no proceda)
Descripción detallada de la incidencia: **Mal funcionamiento durante la realización y la custodia de las copias de seguridad. Las copias de seguridad se realizan en un pendrive y por error de un trabajador, dichas copias han sido eliminadas (borradas).**	
Efectos que puede producir: **(En caso de no subsanación o incluso independientemente de ella)** **Se le indica de forma verbal al trabajador que debe de tomar todas las precauciones que sean oportunas para evitar que en un futuro vuelva a tener lugar una incidencia de este tipo y se le pide que realice las copia de seguridad a través de copia diaria en unidad de cinta.**	
Persona(s) a quien(es) se comunica: **Pablo García García (responsable del fichero)**	Persona que realiza la comunicación: **José Pérez García. (Encargado de ventas)** Fdo:
MEDIDAS CORRECTORAS APLICADAS: **Se ha procedido a utilizar otro mecanismo para la realización de las copias de seguridad ya que el método empleado no era muy seguro. Las copias de Seguridad debe realizarse a partir de ahora a través de un mecanismo más seguro. Se realiza una copia diaria unidad cinta. Diaria l-v programada, de manera automática. Se realiza 3:00h.** Fecha **01/06/2012** Hora **10:00 h.**	

Identificación y autenticación

El responsable del fichero se encargará de que exista una relación actualizada de los dos usuarios que por ahora tienen acceso autorizado al sistema de información, y de establecer procedimientos de identificación y autenticación para dicho acceso.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

En este supuesto Pablo, como responsable del fichero, establece las responsabilidades sobre el uso de las contraseñas y comunica las mismas. Los usuarios deben memorizar sus contraseñas o guardarlas en un lugar seguro, donde solo ellos puedan acceder. (Se pueden cifrar las contraseñas).

El sistema de identificación y autenticación que da acceso a los ficheros automatizados dispone de las siguientes características:

- Identificación: nombre del usuario.
- Autenticación: contraseña escogida por el usuario. No debe contener el identificador de usuario como parte de la contraseña. No se debe mostrar en la pantalla mientras se está introduciendo.
- Longitud y contenido de las contraseñas: deben tener una longitud mínima de 6 caracteres y contener letras y números.
- Periodicidad de cambio: el cambio de las contraseñas es cada 365 días.

Control de acceso

Cada uno de los usuarios tendrá acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

Pablo ha establecido que el acceso autorizado a los datos del Fichero_clientes serán los mencionados a continuación:

USUARIO	PERFIL	FICHERO	F. ALTA
María Dolores Jiménez Ruiz	Ventas	Clientes	18/01/2012
José Pérez García	Ventas	Clientes	18/01/2012

Pablo establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados. Por eso se establece que los programas de gestión empleados por la empresa tengan claves para acceder a ellos y evitar así que las personas no autorizadas puedan visualizar dicha información.

Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos conforme a los criterios establecidos por el responsable del fichero.

Gestión de soportes

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados, y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

Los datos referentes al fichero de clientes serán guardados por orden alfabético para su fácil localización en carpetas que estarán etiquetadas con la marca CLI012 en la oficina del "Departamento de Ventas".

Por eso Pablo ha decidido que el inventario de los soportes y documentos se realice de la siguiente manera:

INVENTARIO DE SOPORTES Y DOCUMENTOS				
Identificación	**Tipo**	**Soporte o documento**	**Información contenida**	**Alta**
CLI012	Mixto	Disco duro/archivadores-carpetas	Fichero clientes	22/05/2010

Los soportes que contengan los datos personales de clientes deberán estar almacenados en un lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación:

Personas autorizadas	Lugar de acceso
María Dolores Jiménez Ruiz	Departamento de ventas. (Oficina)
José Pérez García	Departamento de ventas. (Oficina)

La salida de soportes y documentos que contengan datos de carácter personal fuera de los locales en los que está ubicado el fichero únicamente podrá ser autorizada por Pablo (responsable del fichero).

Cuando se proceda al traslado de documentación Pablo deberá tomar las medidas necesarias para evitar la sustracción, pérdida o acceso indebido a la información contenida en el mismo o su posterior recuperación.

En el supuesto de que hubiera que desechar cualquier documento o soporte que contenga datos personales, Pablo procederá a su destrucción o borrado, siempre tomando las medidas necesarias para evitar el acceso a la información contenida en el mismo o su posterior recuperación. Pablo utilizará una destructora para la eliminación de los soportes.

Los soportes que contengan datos personales considerados especialmente sensibles se podrán identificar utilizando sistemas de etiquetado comprensibles que permitan al personal con acceso autorizado identificar su contenido pero dificultando la identificación para el resto de personas.

Copias de respaldo y recuperación

El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.

Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción.

Pablo deberá verificar cada seis meses el correcto funcionamiento y aplicación de los procedimientos de copias de respaldo y de recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos personales no se realizarán con datos reales salvo que se garantice el nivel de seguridad correspondiente al tratamiento realizado (en este caso, medidas de seguridad de nivel básico) y se anote en el documento de seguridad.

Pablo ha decidido que las copias de seguridad de la empresa se realicen de la siguiente manera:

Finalizada la jornada laboral, y cuando los sistemas de información no estén operativos, se ejecutarán los procesos de copias de respaldo (o de seguridad), los cuales están previamente programados de forma diaria. Pablo será la persona encargada de programar los sistemas operativos para generar dichas copia y guardarlas.

Ante la necesidad de la recuperación de datos, el usuario debe comunicarlo al responsable del fichero. Pablo analizará la necesidad de recuperación de los datos y decidirá qué ficheros y datos se deben recuperar, en qué momento, a partir de qué copias de respaldo, y si es necesaria su grabación manual. Pablo deberá autorizar por escrito la ejecución de los procesos de recuperación de ficheros.

Las copias de respaldo y recuperación se realizan de acuerdo al siguiente procedimiento y con la periodicidad que se describe a continuación.

Periodicidad de la copia de seguridad	Diariamente.
Procedimiento para la realización de copia de respaldo	Se copian los ficheros en el disco duro.
Procedimiento de recuperación de los datos	Se restauran los ficheros de la copia de respaldo a su ubicación principal.

5.2. Caso práctico empresa B

Para el segundo ejemplo se va a suponer que la empresa de seguros "LOPD Seguros S.L." aún no ha decidido modificar el fichero de clientes para incorporar la información relativa a la salud. Por tanto, según la naturaleza de los datos que contiene el fichero, se deberían cumplir las medidas de seguridad de nivel básico y medio. Además, la empresa mantiene también un fichero no automatizado con datos personales de los clientes (facturas de reparaciones, partes médicos, etc.).

Llegado el punto de describir las medidas a adoptar, solo se detallarán las de nivel medio de seguridad que deberían ser implantadas para ficheros automatizados y las medidas de nivel básico, medio y alto para el fichero manual.

Medidas de nivel medio para ficheros automatizados

Responsable de seguridad: el responsable del fichero (en este caso Antonio) designará uno o varios responsables de seguridad. Esta designación puede ser única para todos los ficheros o tratamientos de datos o diferenciada según los sistemas de tratamientos utilizados, circunstancia que deberá constar en el documento de seguridad (en concreto designará a María). En ningún caso está designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con el reglamento.

Auditoría: los sistemas de información e instalaciones de tratamientos de datos se someterán a una auditoría interna o externa que verifique el cumplimiento del presente reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años. En este caso, dicha auditoría será llevada a cabo de forma interna por Pedro.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que pueda repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de los dos años señalados anteriormente.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá igualmente incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente (María) que elevará las conclusiones al responsable del fichero (Antonio) para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos o, en su caso, a las autoridades de control de las comunidades autónomas.

Identificación y autenticación

Antonio establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Los usuarios se podrán identificar introduciendo en los sistemas de información el nombre de usuario correspondiente a cada uno y mediante el uso de una contraseña. Se limita la posibilidad de acceso a tres intentos reiterados.

Control de acceso físico

Exclusivamente, el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal (en este caso serán tanto Antonio, como María y Pedro).

Gestión de soportes y documentos

Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita directa o indirectamente conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Igualmente se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y la hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

A continuación se muestra un ejemplo de registro de salida de soportes que se produce en la empresa.

REFORMAS MARAVILLAS S.L	**REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES**
SOPORTE	
Tipo de soporte	Envío de la documentación en carpetas y a través de e-mail.
Contenido	Información contable de la empresa.
ORIGEN Y FINALIDAD	
Finalidad	Realización de las facturas, contabilidad.
Origen	**LOPD Seguros S. L**
FORMA DE ENVÍO	
Medio de envío	Envío de la documentación en carpetas y a través de correo electrónico (una vez al mes o de forma puntual cuando lo requiera la actividad empresarial). En el traslado de la documentación se adoptan las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información.
Remitente	**LOPD Seguros S. L**
AUTORIZACIÓN	
Persona responsable de la recepción	**Pedro Andrés Ruiz González (Asesoría Ruiz González S. L.)**
Cargo\Puesto	Asesor laboral.
Observaciones	
Firma	

Registro de incidencias

En el registro de incidencias deberán consignarse los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de recuperación.

<table>
<tr><td>EMPRESA</td><td colspan="2">Impreso de notificación de incidencias</td></tr>
<tr><td colspan="3">Incidencia Nº: I__5_____I (A cumplimentar por responsable de seguridad)</td></tr>
<tr><td colspan="3">Fecha de notificación: /18/05/2012/</td></tr>
<tr><td colspan="2">Tipo de incidencia:
Pérdida de información referente a los clientes.</td><td>Fecha y hora en que se produce /detecta *
17/05/2012. a las 10:35

(* tachar lo que no proceda)</td></tr>
<tr><td colspan="3">Descripción detallada de la incidencia:

De forma accidental se han borrado archivos que contenían información de los seguros de un listado de clientes por un fallo en el suministro de energía.</td></tr>
<tr><td colspan="3">Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)</td></tr>
<tr><td colspan="3">Recuperación de datos: Procedimiento realizado: Datos restaurados: Datos grabados manualmente:

Pedro establece puntos de restauración del sistema (chkpt).

Persona que ejecutó el proceso: Pedro Jiménez Jiménez
Firma del responsable del fichero: Fdo: Antonio Pérez Pérez</td></tr>
<tr><td colspan="2">Persona(s) a quien(es) se comunica:

Antonio Pérez Pérez</td><td>Persona que realiza la comunicación:

Fdo: Pedro Jiménez Jiménez</td></tr>
<tr><td colspan="2">NOTIFICACIÓN A PERSONAL TÉCNICO:

Fecha Hora</td><td>CORRECCIÓN DE LA ANOMALÍA:

La incidencia se ha subsanado correctamente como se han indicado anteriormente

Fecha 19/05/2012 Hora 12:00</td></tr>
</table>

Continúa en página siguiente >>

<< Viene de página anterior

EMPRESA	Impreso de notificación de incidencias	
¿SE APLICAN MEDIDAS CORRECTORAS? SI ☐ NO ☐		
SEGUIMIENTO	DESCRIPCIÓN:	ACCIONES A REALIZAR:
	COMPROBACIÓN DE LA EFICACIA	REALIZADA POR: Firma y Fecha

Será necesaria la autorización del responsable del fichero (Antonio) para la ejecución de los procedimientos de recuperación de los datos.

Se expone a continuación un modelo de autorización de recuperación de datos:

Autorización para la recuperación de datos

En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en concreto del art. 94 del Real Decreto 1720/2007, se AUTORIZA expresamente en este documento la ejecución de los procedimientos de recuperación de datos a los siguientes usuarios y ficheros:

Usuarios autorizados	Ficheros	Inicio
María López López	Clientes	18/01/2010
Pedro Jiménez Jiménez	Clientes	18/01/2010

Medidas de nivel básico para ficheros no automatizados

Criterios de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información, posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Antonio, el responsable del fichero, deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo siempre y cuando no exista norma aplicable a los mismos.

El archivo de los soportes o documentos se realizará de acuerdo con los siguientes criterios:

La empresa dispone de un archivo inactivo donde se guarda la documentación de otros años relativa a los seguros realizados con la cartera de clientes de la empresa. Están guardados en archivadores clasificados por el nombre de la materia o asunto del que se trata. Se almacena o guarda en una habitación en el sótano del local que dispone de cerradura, al que solo accede el responsable del fichero (Antonio) y el personal autorizado (María y Pedro).

La empresa también dispone de varios archivos en activo, entre ellos cabe destacar la información relativa a los tipos de seguros llevados a cabo con la cartera de clientes de la empresa que se encuentran archivados en carpetas clasificadas por el asunto del que tratan, en un armario con cerradura, en la oficina del departamento de seguros, y la información contable de la empresa como facturas, albaranes, etc., que se encuentra archivada por fechas en carpetas, en un armario con cerradura, en el oficina del departamento de contabilidad.

El traslado de la documentación fuera de la empresa se realizará en carpetas custodiadas por la persona autorizada para ello, de forma que su contenido no sea accesible por las personas no autorizadas.

El desecho de los documentos en soporte papel que contengan datos de carácter general que ya no sean útiles o necesarios se destruirán a través de trituradoras de papel de forma que no sea posible recuperar la información que contenían.

Dispositivos de almacenamiento

Los dispositivos de almacenamiento de documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

El responsable del fichero adoptará medidas que impidan el acceso a personas no autorizadas cuando las características físicas de los dispositivos de almacenamiento no permitan adoptar esta medida. Antonio deberá evitar que terceras personas no autorizadas tengan acceso a datos personales y puedan utilizar o manipular dicha información para fines distintos para los que se destinaron.

Custodia de soportes

La documentación que contenga datos de carácter personal y que no se haya procedido a su archivo por estar en procedimiento de revisión o tramitación deberá ser custodiada por el que se encuentre a cargo de dichos documentos (en este caso María) para evitar que personas no autorizadas accedan al contenido de los mismos.

Medidas de nivel medio para ficheros no automatizados

Responsable de seguridad

El responsable de seguridad (en este caso María), al igual que ocurría en las medidas de seguridad de nivel medio para ficheros automatizados, tiene como función primordial la de controlar las medidas de seguridad que se han establecido para gestionar los datos personales que están regulados en el documento de seguridad.

Auditoría

Los ficheros no automatizados se someterán a una auditoría cada dos años, al igual que ocurría con los ficheros automatizados, para verificar el cumplimiento de las medidas establecidas para la protección de datos regulados en este reglamento. En este supuesto, la persona que ha de realizar la auditoría sería Pedro.

Medidas de seguridad de nivel alto de ficheros no automatizados

Almacenamiento de la información

Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados que contengan datos personales deberán encontrarse en áreas en las que el acceso a los mismos 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 necesario el acceso a documentos contenidos en el fichero. La documentación se encuentra en este supuesto en la oficina del departamento de seguros a la que accede solo el personal autorizado (Antonio, María y Pedro) que son los únicos que disponen de las llaves de la oficina.

Copia o reproducción

Como medida de protección, cuando se realicen copias o la reproducción de documentos contenidos en estos ficheros, estas solo podrán realizarse bajo el control del personal autorizado en el documento de seguridad (en este caso Antonio, María y Pedro), para proteger el contenido de los mismos y evitar un uso distinto al que se le debe dar.

Deberá procederse también a la destrucción de las copias o reproducciones desechadas, de forma que evite el acceso a la información contenida en las mismas. (Se realizará mediante destructora de papel).

Acceso a la documentación

El acceso se realizará a través del personal autorizado (Antonio, María y Pedro) que establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por varios usuarios.

El acceso de personas no autorizadas deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido en el documento de seguridad.

Traslado de documentación

Siempre que se proceda al traslado físico de la documentación contenida en un fichero deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado. La persona que adoptará estas medidas será el responsable del fichero, en este caso Antonio.

Se aplican los tres niveles al fichero no automatizado porque este contiene datos personales que deben estar especialmente protegidos al contener datos relativos a la salud de los clientes, como son los partes médicos mencionados anteriormente.

Dichas medidas son:

- El traslado del soporte fuera de las instalaciones debe realizarse siempre en un maletín o contenedor similar que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.
- En todo momento el maletín o contenedor debe estar controlado y bajo supervisión de la persona que lo custodia.

5.3. Caso práctico empresa C

Este tercer ejemplo muestra las medidas de seguridad que tuvo que adoptar la clínica "LOPD Odontos S.L." antes de producirse el cierre. La clínica tenía dos ficheros automatizados que eran los siguientes: "Ficha de pacientes" (que contenía datos identificativos de los pacientes) y "Datos clínicos" (que contenía la historia clínica del paciente, como enfermedades padecidas, operaciones, tratamientos, etc.). Los datos tratados en el fichero "Ficha de pacientes" son de nivel básico, por lo que se aplicaron las medidas correspondientes a este nivel y para el fichero de "Datos clínicos" se aplicaron las medidas de nivel alto, ya que contenía datos de salud. Además se recuerda que la clínica también mantenía un fichero manual con pruebas diagnósticas de los pacientes. A este fichero no automatizado se le aplicaron las mismas medidas que se vieron en el caso práctico anterior, es decir, medidas del nivel básico, medio, y alto por contener datos personales referentes a la salud de los pacientes.

En cuanto al fichero automatizado "Datos de clientes" se le aplicaron las medidas de seguridad correspondientes a nivel básico, medio y alto. En concreto, se describirán solamente las de nivel alto, ya que las de nivel medio y básico se han visto en los ejemplos anteriores.

Gestión y distribución de soportes

La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles que permitan a los usuarios con acceso autorizado a dichos soportes y documentos identificar su contenido y dificultar la identificación para el resto de personas.

Los soportes se almacenarán de acuerdo a las siguientes normas:

Los datos referentes al fichero de "Datos clínicos" serán guardados por orden alfabético para su mejor localización en carpetas que estarán etiquetadas con la marca CLINI012 en la oficina del odontólogo, y las pruebas clínicas estarán guardadas por el nombre del paciente (alfabéticamente), archivadas en carpetas etiquetadas con la marca Dprueb012, y almacenadas en el archivo de pruebas de la clínica.

INVENTARIO DE SOPORTES Y DOCUMENTOS				
Identificación	**Tipo**	**Soporte o documento**	**Información contenida**	**Alta**
clini012	Mixto	Disco duro/archivadores-carpetas	Fichero datos clínicos	25/05/2010
Dprueb012	Mixto	Disco duro/archivador-carpetas	Fichero pruebas clínicas	25/05/2010

Siempre que exista una distribución de soportes que contengan datos personales altamente protegidos la información que contengan estos soportes deberá mantenerse cifrada. Lo que se pretende con esta medida es garantizar la ininteligibilidad y la no manipulación en el momento en que el soporte se esté transportando.

También se cifrarán los datos que contengan los dispositivos portátiles cuando estos se encuentren fuera de las instalaciones que estén bajo el control del responsable del fichero. Deberá evitarse el tratamiento de datos personales en los dispositivos portátiles cuando no permitan su cifrado y en el caso de que sea estrictamente necesario se hará constar este hecho en el documento de seguridad, exponiendo las causas por las que se lleva a cabo.

Copia de respaldo y recuperación

Las copias de respaldo y recuperación deben ser almacenadas en un lugar de acceso restringido diferente al lugar donde se encuentran los sistemas informáticos y servidores que contienen datos altamente protegidos. El lugar de almacenamiento debe cumplir con las normas del reglamento que les sean aplicables utilizando elementos que garanticen la integridad y recuperación de la información.

Las copias de respaldo y recuperación en la empresa "LOPD Odontos S.L." se almacenan en la sala del archivo histórico, en un armario bajo llave, lugar distinto al área donde se encuentran los sistemas informáticos y servidores que contienen datos altamente protegidos.

Registro de accesos

Cuando un usuario acceda a un sistema que contiene datos personales de nivel alto se deberá realizar un registro en el que se contengan la identificación del usuario que ha accedido, fecha y hora de acceso, fichero al que ha accedido y el tipo de acceso.

Persona que accede	Documento o fichero al que se accede	Fecha	Hora	Tipo de acceso
Fernando Ruiz Ruiz	Fichero pruebas clínicas	20/05/2012	12:00 h	Consulta de pruebas
Marta Luque Luque	Fichero datos clínicos	13/05/2012	10:00 h	Consulta de expedientes

En el caso de que el acceso haya sido autorizado será preciso guardar la información que permita identificar el registro accedido.

El responsable de seguridad debe cumplir con tres funciones:

- Tener el control directo del registro de accesos sin que deba permitir la desactivación ni la manipulación de los mismos.
- Revisar periódicamente las informaciones contenidas en el registro de accesos. El periodo de revisión mínimo está previsto que sea de un mes.
- Elaboración de un informe al menos mensual de las revisiones que se han realizado y de los problemas que se hayan producido.

Telecomunicaciones

Siempre que exista una transmisión de datos personales a través de redes públicas y redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

La empresa "LOPD Odontos" cifra todos los datos enviados a través de redes inalámbricas de comunicaciones electrónicas.